Dr.WEB

vxCube

Administrator Manual

Trademarks

Disclaimer

In no event shall Doctor Web and its resellers or distributors be liable for any errors or omissions, or for any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, or by the use of or inability to use the information contained in this document.

Dr.Web vxCube
Version 1.6.0
Administrator Manual
12/12/2024

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

Website: https://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

We thank all our customers for their support and devotion to Dr.Web products!

Table of Contents

1. Conventions

The following symbols and text conventions are used in this guide:

Convention	Comment
⚠	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

2. About Product

Dr.Web vxCube is a service that analyzes potentially malicious files and generates detailed reports on their behavior in the selected environment.

Dr.Web vxCube uses *hardware virtualization* for the analysis. It allows Dr.Web vxCube to work fast and be invisible to the file you are running.

You can upload a file in a supported format to the analyzer, configure environment on a virtual machine, and influence the analysis process. After the analysis, you will receive a full technical report, as well as a video report showing the file’s behavior in the specified conditions.

2.1. What is Special About Dr.Web vxCube?

Below the specific features of Dr.Web vxCube are listed:

- Virtual machines connect to the internet through a private proxy server. This helps fully analyze the file behavior, especially if it depends on downloading data from the internet.
- The new analyzer works at the *hypervisor* level and does not use any additional software on the host operating system, such as drivers that hook functions. Thus, during the analysis, the sample cannot detect hooks or unhook.
- Events are logged at the hypervisor level—thus, the analyzer cannot be detected.
- It is possible to connect to an analyzed environment via VNC client and influence the analysis process.

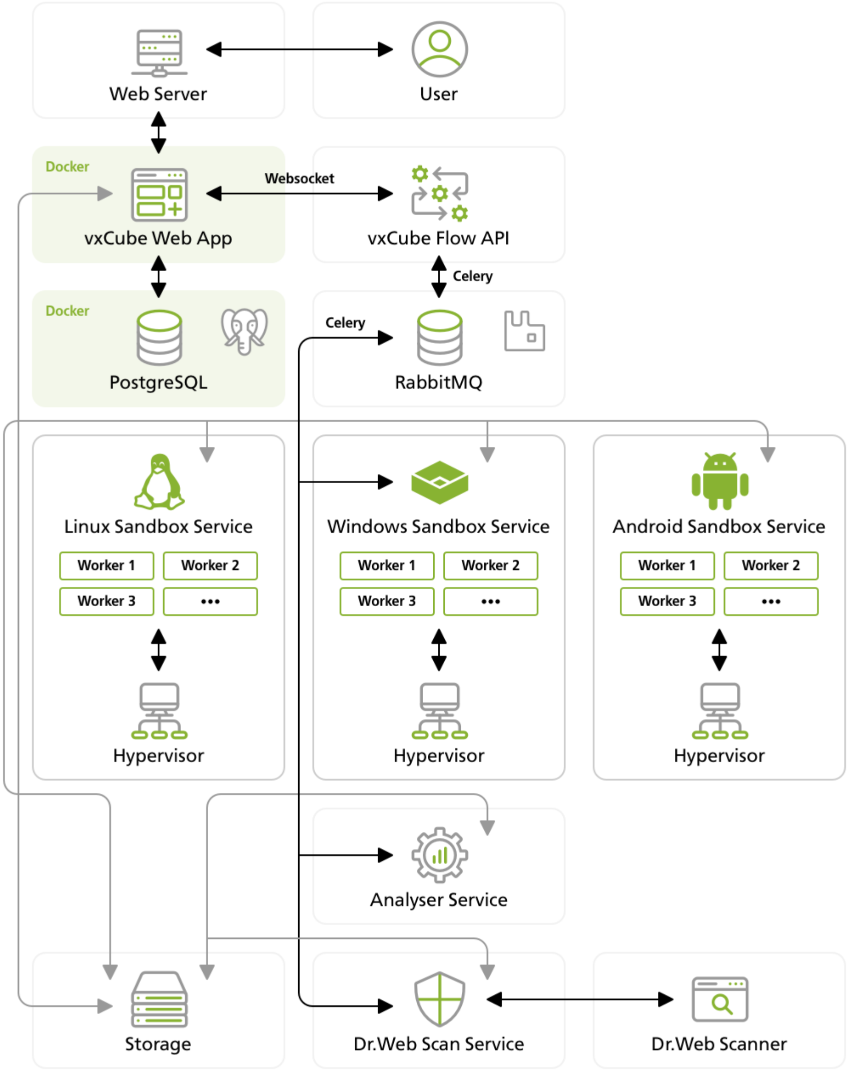
2.2. How to Use Dr.Web vxCube

To scan the suspicious file for threats using Dr.Web vxCube, do the following:

1. Upload a file to be scanned to Dr.Web vxCube.
2. (Optional) Specify additional settings and start the analysis.
3. Review the report that Dr.Web vxCube produced based on the analysis results.

2.3. Under the Hood of Dr.Web vxCube

The analyzer consists of several components and services that interact with each other. The architecture of the product is illustrated in the picture below.



vxCube Web App

The main application, which provides a convenient interface for interacting with a file analysis system. It also supports an API to automate file analysis tasks. It also includes a Python library for convenience.

vxCube Flow API

The component that distributes file analysis tasks among different services. It helps integrate new services into the analysis system.

Windows Sandbox Service

A virtual environment to run files on the Windows OS. This virtual machine is a modified hypervisor that uses built-in function hooks and hardware virtualization technology.

Linux Sandbox Service

A service for dynamic analysis of ELF files. Files are run on a virtual machine with the required architecture and bitness, and all events are logged by a special driver installed on the virtual machine.

> ⚠ If all vxCube components and services are installed on a single server, Linux Sandbox Service’s performance may be affected. That is because virtualization is implemented using software methods. That’s why we recommend that you install each component on a separate server.

Android Sandbox Service (optional)

A virtual environment to run files on the Android OS. A unique implementation of an Android OS image.

Analyser Service

A service that analyzes file behavior recorded on a virtual machine. It assesses the maliciousness and generates descriptions (in a text format, MAEC, or STIX).

Dr.Web Scan Service

A service that scans files and memory dumps created after running a sample.

The components transfer files through the common **Storage** (as illustrated on the picture above), implemented as an FTP server. To store data about users and analysis results, the service uses the *PostgreSQL* database. The *RabbitMQ* message broker transfers tasks between services.

For utmost security, each virtual machine has its own isolated network space and uses a VPN server for internet access. To ensure correct operation of Dr.Web vxCube, VPN server must be configured manually. For more information, see Appendix C. Configuring a separate VPN server.

> ⚠ We recommend that you use a dedicated VPN server because public VPN servers might be configured incorrectly.

2.4. System Requirements

To ensure correct operation of Dr.Web vxCube, your computer should meet the following requirements:

Component	Requirements
Processor (CPU)	Intel CPU with Virtualization Technology: VT-x, EPT, Preempt Timer. Minimum: 16 cores Recommended: 48 cores Optimal: 56 cores
Memory (RAM)	Minimum: 64 GB Recommended: 128 GB Optimal: 256 GB
Drives	Minimum: a 256-GB+ SSD drive Recommended: two 256-GB+ SSD drives Optimal: four 256-GB+ SSD drives To avoid malfunctions, make sure you connect SSD drives via the SATA 3 connector and do not use them in RAID arrays.
Operating System	• Astra Linux 1.7.6 with Linux kernel 5.4 (an OS should be installed on a separate HDD or SSD drive). • Ubuntu 22.04 with Linux kernel 5.15. The amount of SWAP space must be at least 10–50% of RAM.
Integration with MailD	To operate using HTTPS, Dr.Web vxCube requires SSL certificates. Otherwise, the service will not be able to scan emails in the EML format.

For the intended performance of web UI, we recommend that you use:

Parameter	Requirement
Browser	• Google Chrome 60.0 or later. • Mozilla Firefox 55.0 or later. • Safari 11.0 or later. • Opera 47.0 or later. We recommend that you use Google Chrome for Windows XP. We cannot guarantee that Mozilla Firefox will correctly display video on computers that run Windows XP.
Screen resolution	At least 1024x768.
Optional	If you want to manage emulation interactively, make sure that pop-ups are allowed in your browser.

3. Installing Dr.Web vxCube

Before installing Dr.Web vxCube, make sure that a target server meets the system requirements.

Dr.Web vxCube is installed using Ansible Playbook. The Playbooks manage installation of software and environment configuration for several computers at once.

3.1. Preparing for Installation

Once you purchase a license for the service, you will receive the following emails:

- an email that includes links to the product distribution and images of virtual machines where the analysis will be carried out,
- an email with a license key file.

In addition, a Guardant dongle will be sent to you by postal service.

Make sure to do the following before starting the installation:

1. Wipe the SSD drive where you plan to install Dr.Web vxCube components. If it has partitions, delete them.
2. Connect the Guardant dongle to the device where you intend to deploy Dr.Web vxCube. This is required for analyses to run. If you are going to deploy Dr.Web vxCube on several devices, you will need individual Guardant dongles for each of the devices.
3. Download the product distribution, virtual machine images, and the key file from the emails that you received. Unpack the downloaded archives.
4. Put the Dr.Web vxCube license key into `confs/vxcube.key`.
5. Put distribution files and images into the following directories:

- SSL certificates required for connecting with VPN servers and specified in the `vars-user.yml` file (the `openvpn_client_servers` variable) to the `confs/openvpn.crt`, `confs/openvpn.key`, and `confs/openvpn_ca.crt` directories;

> SSL certificates are not supplied with Dr.Web vxCube; you need to obtain them separately.

- the received Windows virtual machine `.tar.gz` images and all `.tar.gz.ver` and `.tar.gz.hash` files to the `vm-images-win directory`;
- the received Android virtual machine `.vdi` images and all `.vdi.hash` and `.vdi.ver` files to the `vm-images-andr directory`;
- the received Linux virtual machine `.tar.gz` images and all `.tar.gz.hash` and `.tar.gz.ver` files to the `vm-images-linux directory`.

⚠ You can also put the virtual machine images into the directories you want. For this, specify the directories in the `vars-default.yml` file (in the `hyperbox_images_repo`, `dimas_images_repo`, and `linuxbox_images_repo` variables).

6. If you want to integrate Dr.Web vxCube with MailD, you need an SSL certificate. If you don't have this, generate it like this:

```
openssl dhparam -out web_dhparam.pem 2048
```

7. If you want Dr.Web vxCube to support the HTTPS protocol, do the following:

- create the `confs/web_ssl.crt` and `confs/web_ssl.key` files;
- create the `confs/web_dhparam.pem` file (if you have skipped step 5).
- in the `vars-default.yml` file, uncomment the following variables: `vxcube_web_ssl_cert`, `vxcube_web_ssl_privkey`, and `vxcube_web_dhparam`.

8. Make sure that all servers where you intend to deploy Dr.Web vxCube components have the following packages installed: `make`, `python3-venv`, and `sshpass`. If not, install them as follows:

```
sudo apt-get install make
sudo apt-get install python3-venv
sudo apt-get install sshpass
```

⚠ When you issue the `make` command, it creates a Python virtual environment and installs packages required to run the appropriate Ansible version. If you use a Python repository other than `pipy.org`, set it in the environment variables, for example:

```
export PIP_INDEX_URL=https://devpi.local
export PIP_TRUSTED_HOST=devpi.local
```

Alternatively, add the following to the run command:

```
PIP_INDEX_URL=https://devpi.local
PIP_TRUSTED_HOST=devpi.local make deploy
```

9. Enable support of `systemd-networkd.socket` as follows:

```
sudo systemctl stop systemd-networkd.service
sudo systemctl enable systemd-networkd.socket
sudo systemctl start systemd-networkd.socket
sudo systemctl start systemd-networkd.service
```

10. (Only if you intend to install Dr.Web vxCube on a computer running Astra Linux) Update to OS Astra Linux 1.7.6. The `/etc/apt/sources.list` file must contain the following repositories:

```
# Extended repository

deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-
extended/ 1.7_x86-64 main contrib non-free
```

```
# Astra 1.7.6 repository

deb http://dl.astralinux.ru/astra/frozen/1.7_x86-
64/1.7.6/repository-main/ 1.7_x86-64 main contrib non-free

deb http://dl.astralinux.ru/astra/frozen/1.7_x86-
64/1.7.6/repository-update/ 1.7_x86-64 main contrib non-free

deb http://dl.astralinux.ru/astra/frozen/1.7_x86-
64/1.7.6/repository-base/ 1.7_x86-64 main contrib non-free
```

11. After updating the repositories, run the following commands:

```
sudo apt update
sudo apt upgrade
```

12. Edit the installation settings. To do this, assign a value for each variable in the `vars-user.yml` file. All the variables in this file must have an assigned value. The detailed description of the variables is given in the file and in the following table below:

The description of variables contained in vars-user.yml

Variable	Description
`vxcube_web_superuser_email`	The email of a Dr.Web vxCube administrator. A user with this email will be created after the web UI is installed.

`vxcube_web_superuser_pass`	An administrator password.
	You can define a password:
	`vxcube_web_superuser_pass: "example_password"`
	Alternatively, it can be automatically generated:
	`vxcube_web_superuser_pass: "{{ lookup('password', 'credentials/vxcube_web_superuser_pass length=10`
	`chars=ascii_letters,digits') }}"`
	The generated password will be saved in the file `credentials/vxcube_web_superuser_pass`.

`hyperbox_ssds`	The list of SSD drives available on the server.
	Example of a variable value for two drives:
	`hyperbox_ssds:`
	`- sdb`
	`- sdc`

`vxcube_os_count`	The maximum number of simultaneously running virtual machines with Windows OS. Keep in mind the technical limitations of the computer when choosing a value for this variable. The optimal value can be calculated by the formula:

Variable	Description
	*<vxcube_os_count> = <number of cores * 1.5> / <number of different OS types>* For example, on a 48-core server running four different operating systems, you can set `vxcube_os_count` to 18.
`vxcube_os_clone_threads`	The number of threads used to clone virtual machines. Keep in mind the technical limitations of the computer when choosing a value for this variable. For example, for two SSD drives and a 48-core CPU, the number of threads must not exceed 15.

`openvpn_client_servers`	The list of VPN servers for routing traffic from virtual machines. You have the option to input several servers in the variable. If the first server stops responding, the next one in the list will be used. Please note that `vxcube-installer` does not deploy a VPN server. To do this, you need to configure a VPN server on your own. See Appendix C. Configuring a separate VPN server.
	Variable value format:
	`openvpn_client_servers:`
	`  - host: xx.xx.xx.xx`
	`    port: 1194`

`vboxnet_vpn_gateway`	The IP address of the gateway inside the VPN network, through which the traffic will be redirected. It is usually the first host in the subnet. For example, if the internal VPN network uses the subnet 10.0.42.0/24, then the gateway IP address will be 10.0.42.1.
`evparser_max_workers_count`	The maximum number of running threads used by the behavior analysis service. Keep in mind the technical limitations of the computer when choosing a value for this variable. We recommend that you set the value equal to `vxcube_os_count`.
`evparser_min_workers_count`	The minimum number of running threads used by the behavior analysis service. The threads will keep running, even if there are no tasks. We recommend that you set the value equal to 20% of `evparser_max_workers_count`.
`evparser_srv_autoscale`	The maximum and minimum possible number of running threads used by the behavior analysis service. Variable value format: `"<max_worker_num>,<min_worker_num>"` Example: `evparser_srv_autoscale: "10,1"`
`drweb_srv_autoscale`	Maximum and minimum number of threads used by the anti-virus for scanning files. Variable value format: "*<max_worker_num>*,*<min_worker_num>*".

Variable	Description
	For example: `drweb_srv_autoscale: "10,1"` We recommend that you set the values the following way: `max_worker_num` equal to `vxcube_os_count`, `min_worker_num` to 20% of `max_worker_num`.
`yara_srv_autoscale`	Maximum and minimum number of threads used by YARA. Variable value format: "<*max_worker_num*>,<*min_worker_num*>". Example: `yara_srv_autoscale: "10,1"` We recommend that you set the values the following way: `max_worker_num` equal to `vxcube_os_count`, `min_worker_num` to 20% of `max_worker_num`.

You may also configure variables in the `vars-default.yml` file. The detailed description of the variables is given in the file and in the following table below:

The description of variables contained in vars-default.yml

Variable	Description
`vxcube_local_hostname`	Name of the host when deploying on local server.
`vxcube_ftp_user`	Login name of an FTP user. It is used for deploying samples on the FTP server. Example: `vxcube_ftp_user: "vxcube_ftp"`
`vxcube_ftp_pass`	A password for the FTP user specified in the `vxcube_ftp_user` variable. By default, a password is randomly generated and stored in the `credentials/vxcube_ftp_pass` file. If a password was previously generated and saved in the `credentials/vxcube_ftp_pass` file, it will be used. Example: `vxcube_ftp_pass: "{{ lookup('password', 'credentials/vxcube_ftp_pass length=10 chars=ascii_letters,digits') }}"`
`vxcube_web_db_pass`	Database password. By default, a password is randomly generated and stored in the `credentials/vxcube_web_db_pass` file. Example: `vxcube_web_db_pass: "{{ lookup('password', 'credentials/vxcube_web_db_pass length=10 chars=ascii_letters,digits') }}"`
`vxcube_web_ssl_cert`	Path to the `.crt` certificate. By default, it is stored at `confs/web_ssl.crt`.

Variable	Description
	Example: `vxcube_web_ssl_cert: "{{ lookup('file', 'confs/web_ssl.crt') }}"`
`vxcube_web_ssl_privkey`	Path to the `.key` private key. By default, it is stored at `confs/web_ssl.key`. Example: `vxcube_web_ssl_privkey: "{{ lookup('file', 'confs/web_ssl.key') }}"`
`vxcube_web_dhparam`	Path to the `.pem` Diffie-Hellman key. By default, it is stored at `confs/web_dhparam.pem`. Example: `vxcube_web_dhparam: "{{ lookup('file', 'confs/web_dhparam.pem') }}"`
`vxcube_web_mail_server`	IP address or domain name of the SMPT server. Example: `vxcube_web_mail_server: "localhost"` By default: `localhost`.
`vxcube_web_recaptcha_site_key`	Website key, which is used for reCAPTCHA. Example: `vxcube_web_recaptcha_site_key: SITE_KEY //<website key>` Values are provided after domain registration on https://www.google.com/recaptcha/admin.
`vxcube_web_recaptcha_secret`	Secret key, which is used for reCAPTCHA. Example: `vxcube_web_recaptcha_secret: SECRET_KEY //<secret key>` Values are provided after domain registration on https://www.google.com/recaptcha/admin.
`vxcube_web_check_exchange_min`	FTP server directory check period in minutes. Possible values: from 1 to 60. Example: `vxcube_web_check_exchange_min: "5"`
`vxcube_web_keep_free_space_percent`	If the value of this variable is lower than the free disk space, old reports will not be deleted. Value is a percentage. Example:

Variable	Description
	`vxcube_web_keep_free_space_percent: "30"`
`vxcube_web_keep_exchange_hours`	Minimum period for storing files if insufficient disk space. Value is in hours. If the variable is set to 0.5, any files created within the last half hour will not be deleted. Example: `vxcube_web_keep_exchange_hours: "0,5"`
`vxcube_web_keep_reports`	Minimum time before an existing report is considered old and will be deleted. Value is in minutes. Example: `vxcube_web_keep_reports: "20m"`
`vxcube_web_reports_clean_period_min`	Frequency at which the task runs to delete old reports. Value is in minutes. Example: `vxcube_web_reports_clean_period_min: "5"`
`vxcube_web_fail_free_space_percent`	Threshold of free disk space where tasks will terminate with an error. Value is a percentage. Example: `vxcube_web_fail_free_space_percent: "5"`
`vxcube_web_local_max_body_size`	An internal variable. Use here the same value as the one given for `vxcube_web_max_body_size` below.
`vxcube_web_local_max_exec_time`	The highest value (in seconds) a user can set for the **Default sample run time**. Example: `vxcube_web_local_max_exec_time: "3600"`
`vxcube_web_max_body_size`	The maximum file size that can be analyzed (in MB). Example: `vxcube_web_max_body_size: "2001"`
`hyperbox_api_rq_username`	Account for RabbitMQ. Example: `hyperbox_api_rq_username: "celery"`
`hyperbox_api_rq_password`	User password specified in `hyperbox_api_rq_username`. By default, a password is randomly generated and stored in `credentials/hyperbox_api_rq_password`. Example:

Variable	Description
	`hyperbox_api_rq_password: "{{ lookup('password', 'credentials/hyperbox_api_rq_password length=10 chars=ascii_letters,digits') }}"`
`hyperbox_api_rq_vhost`	RabbitMQ database name. Example: `hyperbox_api_rq_vhost: "tasks"`
`hyperbox_api_rq_admin_pass`	Administrator password for working with users and database in RabbitMQ. Example: `hyperbox_api_rq_admin_pass: "{{ lookup('password', 'credentials/hyperbox_api_rq_admin_pass length=10 chars=ascii_letters,digits') }}"`
`hyperbox_api_rq_plugins`	List of RabbitMQ plug-ins to be installed. Example: `hyperbox_api_rq_plugins: ["rabbitmq_management"]` The variable is disabled by default.
`hyperbox_key_path`	License key path. Example: `hyperbox_key_path: "confs/vxcube.key"` Default path: `confs/vxcube.key`.
`hyperbox_external_addr`	Address for connecting to a server with virtual machines using VNC. Example: `hyperbox_external_addr: "{{ hostvars[inventory_hostname]['ansible_default_ipv4']['address'] }}"` This variable is required for correct operation of VNC.
`hyperbox_hbsetup`	Used for cloning virtual machines from OVA images. Example: `hyperbox_hbsetup: "false"` Value `True` is used for initial setup and in case of changes in OVA images.
`hyperbox_images_repo`	Path to OVA images of virtual machines. Example: `hyperbox_images_repo: "vm-images-win"` Value of the variable can also be an FTP address in the URI format. Example:

Variable	Description

	`hyperbox_images_repo:`
	`"ftp://user:pass@host:port/path"`

`hyperbox_images`	The list of virtual machines and their specifications. All virtual machines listed here must be located in the image repository specified in `hyperbox_images_repo`.
	Example:
	`hyperbox_images:`
	`  - vm_type: 6.1.7601.17514_x86`
	`    code: Win7x86`
	`    count: "{{ vxcube_os_count }}"`
	`    memory: 1536`
	`    clone_threads: "{{ vxcube_os_clone_threads }}"`
	`    cores: 2`
	`cores` is the number of cores assigned to a VM.

`hyperbox_force_clean_vms`	Forces deletion of all used virtual machines before cloning new ones. Default value: `False`.
`vm_type`	Virtual machine type. Example: `vm_type: 6.1.7601.17514_x86`
`code`	Virtual machine name. Example: `code: Win7x86`
`count`	Number of OS clones for every virtual machine. Example: `count: "{{ vxcube_os_count }}"` By default, the value is taken from the `vxcube_os_count` variable.
`memory`	The amount of RAM allocated for virtual machine at startup. Example: `memory: "1536"`
`clone_threads`	Number of threads used while cloning virtual machines during the installation. Example: `clone_threads: "{{ vxcube_os_clone_threads }}"` By default, the value is taken from the `vxcube_os_clone_threads` variable.
`openvpn_client_crt`	Path to the OpenVPN server certificate. Example:

Variable	Description
	`openvpn_client_crt: "{{ lookup('file', 'confs/openvpn.crt') }}"` Path by default: `confs/openvpn.crt`
`openvpn_client_key`	Path to private key of the OpenVPN server client. Example: `openvpn_client_key: "{{ lookup('file', 'confs/openvpn.key') }}"` Default path: `confs/openvpn.key`
`openvpn_client_ca_crt`	Path to the certificate of the OpenVPN server key certification authority. Example: `openvpn_client_ca_crt: "{{ lookup('file', 'confs/openvpn_ca.crt') }}"` Default path: `confs/openvpn_ca.crt`
`openvpn_client_tls_auth`	The `tls-auth` parameter adds another HMAC signature to SSL/TLS handshake packets, initiating an additional integrity verification. Example: `openvpn_client_tls_auth: "{{ lookup('file', 'confs/openvpn_ta.crt', errors='ignore')| default(omit) }}"`
`openvpn_client_chiper`	The encryption method applied. Example: `openvpn_client_chiper: "AES-128-CBC"`
`vxcube_optional_types_codes`	Optional file types that can be analyzed. Example: `vxcube_optional_types_codes: "moc"` To use the variable, you should install Microsoft Office on images. Disabled by default.
`drweb_srv_se_licence_key`	License key path. Example: `drweb_srv_se_licence_key: "{{ lookup('file', 'confs/vxcube.key') }}"` Default path: `confs/vxcube.key`
`vxcube_web_server_name`	Domain name of the Dr.Web vxCube web interface.

Variable	Description
`vxcube_storage`	Path to the directory containing virtual machines and temporary files created during the analysis. Example: `vxcube_storage: "/var/lib/storage"`
`vxcube_configure_firewall`	A variable that indicates if firewall needs to be configured after installation (true/false).
`evparser_dwschecker_url`	URL to access the link checking service. Available if supported by the license. Example: `evparser_dwschecker_url: "http://hostname/?key=mykey&url={0}&info=1"`
`dimas_external_ip`	Address of a server with virtual machines. Required for the correct operation of VNC. Example: `dimas_external_ip: "{{ hostvars[inventory_hostname]['ansible_default_ipv4']['address'] }}"`
`dimas_vms_setup`	The variable that indicates if virtual machines need to be recloned (true/false).
`vxcube_force_clean_vms`	Deletes virtual machine files.
`dimas_images_repo`	Path to the directory containing VDI images of virtual machines. You can also enter an FTP address in the URI format. Example: `dimas_images_repo: "ftp://user:pass@host:port/path"`
`dimas_tar_repo`	Path to the vboxsdk repository. You can also enter an FTP address in the URI format. Example: `dimas_tar_repo: "ftp://user:pass@host:port/path"`

`dimas_images`	The list of Android-based virtual machines and their specifications.
	All virtual machines listed here must be located in the image repository specified in `dimas_vdi_repo`.
	Example:
	`dimas_images:`
	`  - vm_type: Android7.1`
	`    code: Android7.1`
	`    count: 3`
	`    memory: 4072`
	`    cores: 2`
	`    clone_threads: 3`

Variable	Description

`_vxcube_use_windows_workers: "{{ lookup('ini', 'Windows section=Settings file={{ hyperbox_key_path }}') | bool }}"`
 	
`_vxcube_use_android_workers: "{{ lookup('ini', 'Android section=Settings file={{ hyperbox_key_path }}') | bool }}"`
 	
`_vxcube_use_linux_workers: "{{ lookup('ini', 'Linux section=Settings file={{ hyperbox_key_path }}') | bool }}"`
 	
`vxcube_web_expire_date: "{{ lookup('ini', 'Expires section=Key file={{ hyperbox_key_path }}') }}"`
 	
`vxcube_web_activation_date: "{{ lookup('ini', 'Created section=Key file={{ hyperbox_key_path }}') }}"`
	License information.

`zabbix_agent_required`	The `zabbix_agent_required` variable for optional installation of a Zabbix agent, which allows for real-time monitoring of the state of vxCube components.
	
	Example:
	
	`zabbix_agent_required: "true"`
	`zabbix_agent_server: 192.168.33.30`
	`zabbix_agent_serveractive: 192.168.33.30`
	`zabbix_version: 3.0`
	
	The variables `zabbix_agent_server` and `zabbix_agent_serveractive` must contain the IP address or domain name of the Zabbix server.
	
	For that, you have to install the Zabbix Server on your own.
	
	The `zabbix_version` parameter is optional. If you do not specify it, the latest Zabbix version will be installed to host. If you need an older version, specify it.

Variable	Description
	Example: `zabbix_version: 4.0`, `zabbix_version: 3.4`, or `zabbix_version: 2.2`.
`zabbix_agent_serveractive`	Zabbix server addresses for active monitoring.
`vxcube_web_flask_workers`	The number of running threads of a web application. Example: `vxcube_web_flask_workers: 5`
`vxcube_web_flask_timeout`	The response timeout for the web application. Example: `vxcube_web_flask_timeout: 300`
`linuxbox_vms_setup`	The variable that indicates if virtual machines need to be recloned (true/false). Example: `linuxbox_vms_setup: true`

`linuxbox_images_repo`	Path to the repository that contains VDI images of virtual machines. Value of the variable can also be an FTP address in the URI format.
	Example:
	`linuxbox_images_repo: "ftp://user:pass@host:port/path"`
	or
	`linuxbox_images_repo: "vm-images-linux"`

`linuxbox_images`	The list of Linux virtual machines and their specifications. All virtual machines listed here must be located in the image repository specified in `linuxbox_vdi_repo`.
	Example:
	`linuxbox_images:`
	`  - vm_type: intel64_astra_ce_2.12`
	`    code: intel64_astra_ce_2.12`
	`    count: 1`

`linuxbox_force_clean_vms`	Forces deletion of all used virtual machines before cloning new ones. Default value: `False`.

3.2. Installing on a Local Server

To install all Dr.Web vxCube components on a local server, use the following command:

```
$ make install
```

After that, Ansible will request the current user password to install components from the `inventory-local.yml` on a server. The password will be requested by `BECOME password:`.

Configuration performance depends on device specifications and might vary on different devices. You need to consider this when setting it up in `vars-user.yml`.

3.3. Installing on a Remote Server or a Group of Servers

To install Dr.Web vxCube on one server or several servers with the same configuration (number of cores, drives, etc.)

1. Enter the server addresses for each component in the `inventory.yml` file.
   Only the variables `hyperbox_hosts`, `hyperbox_api_host`, `evparser_hosts`, `drweb_srv_hosts`, `dimas_hosts`, `linuxbox_hosts` и `yara_hosts` can take on a set of server addresses as a value.
   Components corresponding to those variables carry the main load during file analysis and support scale-out for processing large amounts of files uploaded to Dr.Web vxCube.

   > ⚠ To avoid freezing of the web UI, we recommend that you deploy `vxcube_web_host` and each individual analyzer (`hyperbox_hosts`, `hyperbox_api_host`, `evparser_hosts`, `drweb_srv_hosts`, `dimas_hosts`, `linuxbox_hosts`, `yara_hosts`) on individual nodes.

2. To install vxCube on several servers, specify the drives to be used for installation in the `hyperbox_hosts` variable in the `inventory.yml` file, for example:

```
hyperbox_hosts:
      hosts:
        192.168.1.10:
          hyperbox_ssds: [ "sda" ]
        192.168.1.11:
          hyperbox_ssds: [ "sda", "sdb", "sdc", "sdd"]
```

3. To access the servers, specify a user name and a path to its private key in the values `ansible_user` and `ansible_ssh_private_key_file` in the `inventory.yml` file.

This user must be able to run commands as the superuser without entering a password. To create such a user on multiple servers simultaneously, use the command:

```
$ make prepare
```

Running the command will create a user on all servers specified in `inventory.yml` and save a private authorization key as a file (default path: `credentials/ssh/id_rsa`).

4. To start Dr.Web vxCube installation using the `inventory.yml` file, run the command:

```
$ make deploy
```

To install Dr.Web vxCube on several servers with varying configurations (number of cores, drives, etc.)

1. Enter the server addresses for each component in the `inventory.yml` file.
   Only the variables `hyperbox_hosts`, `hyperbox_api_host`, `evparser_hosts`, `drweb_srv_hosts`, `dimas_hosts`, `linuxbox_hosts` и `yara_hosts` can take on a set of server addresses as a value.
   Components corresponding to those variables carry the main load during file analysis and support scale-out for processing large amounts of files uploaded to Dr.Web vxCube.

   To avoid freezing of the web UI, we recommend that you deploy `vxcube_web_host` and each individual analyzer (`hyperbox_hosts`, `hyperbox_api_host`, `evparser_hosts`, `drweb_srv_hosts`, `dimas_hosts`, `yara_hosts`) on individual nodes.

2. Specify the drives to be used for installation in the `hyperbox_hosts` variable in the `inventory.yml` file, for example:

```
hyperbox_hosts:
      hosts:
        192.168.1.10:
          hyperbox_ssds: [ "sda" ]
        192.168.1.11:
          hyperbox_ssds: [ "sda", "sdb", "sdc", "sdd"]
```

3. To access the servers, specify a user name and a path to its private key in the values `ansible_user` and `ansible_ssh_private_key_file` in the `inventory.yml` file.
   This user must be able to run commands as the superuser without entering a password. To create such a user on multiple servers simultaneously, use the command:

```
$ make prepare
```

Running the command will create a user on all servers specified in `inventory.yml` and save a private authorization key as a file (default path: `credentials/ssh/id_rsa`).

4. For each node, place an individual openvpn certificate (`.crt`, `.key`) in the `confs` directory, for example: `192.168.1.10.crt`, `192.168.1.20.crt`, `192.168.2.10.key`, `192.168.2.20.key`.
5. In the `vars-default.yml` configuration file, set values for the variables `openvpn_client_crt` and `openvpn_client_key`, for example:

```
openvpn_client_crt: "{{ lookup('file', 'confs/
{{ inventory_hostname }}.crt') }}"
openvpn_client_key: "{{ lookup('file', 'confs/
{{ inventory_hostname }}.key') }}"
```

6. In the root directory of the installation archive, create the `host_vars` directory and create an individual YML file with deployment settings for each server, for example: `192.168.1.10.yml` и `192.168.2.20.yml`.
7. Enter the settings in the YML files:
   a. Enter the Ansible user name and password, for example:

```
ansible_user: test_ansible_user
ansible_ssh_pass: test_ansible_user_pass
ansible_become_password: test_ansible_user_pass
```

   b. Enter the directory where you will be cloning VM images to, for example:

```
hyperbox_ssds: [ "sda" ]
```

   c. Enter the configurations of VMs, for example:

```
hyperbox_images:
  - vm_type: 6.1.7601.17514_x86
    code: Win7x86
    count: 2
    clone_threads: 2
    params:
      memory: 2112
      cores: 2

  - vm_type: 6.1.7601.17514_x64
    code: Win7x64
    count: 2
    clone_threads: 2
    params:
      memory: 2112
      cores: 2

linuxbox_images:
  - vm_type: intel64_astra_se_1.7.2
```

```
    code: intel64_astra_se_1.7.2
    count: 1

  - vm_type: intel64_astra_ce_2.12
    code: intel64_astra_ce_2.12
    count: 1

dimas_images:
  - vm_type: Android7.1
    code: Android7.1
    count: 3
    memory: 4072
    cores: 2
    clone_threads: 3
```

Variables from `vars-default.yml` are higher priority for deployment than variables from YML files in the `host_vars` directory. To redefine their values, comment out the matching variables in `vars-default.yml`.

For example, if we create the file `host_vars/192.168.1.10.yml` and redefine the `hyperbox_ssds` variable as `hyperbox_ssds: [ "sda" ]`, then we have to comment this variable out in the `vars-default.yml` file.

8. To start Dr.Web vxCube installation using the `inventory.yml` file, run the command:

```
$ make deploy
```

For more information about the `inventory.yml` file, refer to the Ansible documentation.

3.4. Updating Settings

If you need to update settings after installing Dr.Web vxCube, restart the installer with the option `hyperbox_hbsetup: false`. This will prevent redeploying virtual machines and will significantly speed up the installation.

You can also change some of the settings manually on the server.

SSL certificate renewal

To renew the SSL certificate

1. Add new files in the following paths:
   - `/etc/nginx/ssl/vxcube.crt`,
   - `/etc/nginx/ssl/vxcube.key`.
2. Reload the web server:

```
sudo systemctl reload nginx
```

Updating the VPN agent settings

To change a server IP address

1. Open file `/etc/openvpn/client.conf`.
2. Specify a new address in parameter `remote "New IP address" 1194`.

To renew the VPN server access certificates

1. Add new files in the following paths:
   - `/etc/openvpn/client.crt`,
   - `/etc/openvpn/client.key`,
   - `/etc/openvpn/ca.crt`.

To change an IP address of the VPN gateway

1. Open the file `/etc/vbox/config.json`.
2. Specify the new IP address of the VPN: `"vpn_gateway": "IP address of VPN gateway"`.

After making all the changes, restart the OpenVPN and Sandbox services:

```
sudo systemctl restart openvpn vboxsvc vboxapi
```

Updating the network interface settings

By default, the network interface settings are transferred through the DHCP protocol.

To change settings

1. Open the file `/etc/netplan/01-netcfg.yaml`.
2. Specify new settings.
3. Run `netplan apply` to apply changes.
4. Reload server.

3.5. List of vxCube Services

The table below contains a full list of services installed with vxCube (except for those that are part of OS Astra Linux 1.7.3) with paths to their event logs.

Service	Path to log file or command to view log	Description
Infrastructure services		
nginx.service	`/var/log/nginx`	A high performance web server and a reverse proxy server
openvpn.service	`/var/log/openvpn`	OpenVPN service
openvpn@client.service	`sudo journalctl -u openvpn@client.service`	OpenVPN connection to client
proftpd.service	`/var/log/proftpd`	Starts ProFTPD daemon
containerd.service	`sudo journalctl -u containerd.service`	containerd container runtime
docker.service	`sudo journalctl -u docker.service`	Docker Application Container Engine
rabbitmq-server.service	`/var/log/rabbitmq/`	RabbitMQ Messaging Server
General virtualization services		
vboxdrv.service	`sudo journalctl -u vboxdrv.service`	VirtualBox Linux kernel module
vboxnet.service	`sudo journalctl -u vboxnet.service`	VirtualBox Network Service
vboxsvc.service	`sudo journalctl -u vboxsvc.service`	VirtualBox Service
vboxapi.service	`sudo journalctl -u vboxapi.service`	VirtualBox API Service
vboxautostart-service.service	`sudo journalctl -u vboxautostart-service.service`	VirtualBox autostart service
vboxballoonctrl-service.service	`sudo journalctl -u vboxballoonctrl-service.service`	VirtualBox watchdog daemon
vboxweb-service.service	`sudo journalctl -u vboxweb-service.service`	VirtualBox web service API
Windows virtualization services		
hyperbox_<*>_vxcube.service,	`/var/log/hyperbox/`	Celery Worker for hyperbox_<*>_vxcube 1,3, where <*> stands for the name of a Windows image supplied with the installer, such as

Service	Path to log file or command to view log	Description
where <*> stands for the name of a supplied Windows image, such as hyperbox_win10x64_1903_vxcube.service		`win7x86`, `win10x64_1903`, `win7x64`, `winxpx86` (there can be several such services)
hbcheck.service	`sudo journalctl -u hbcheck.service`	Hyperbox check
Android virtualization services		
dimas_<*>vxcube.service, where <*> stands for the name of a supplied Android image, such as dimas_android4.3_vxcube.service	`/var/log/dimas`	Celery Worker Dimas для dimas_<*>_vxcube 1,1, where <*> stands for the name of an Android image supplied with the installer, such as `android4.3`, `android7.1` (there can be several such services)
dimasnet.service	`sudo journalctl -u dimasnet.service`	dimasnet vboxifs init oneshot service
vboxapi_android.service	`/var/log/dimas/vboxapi`	Android VirtualBox API Service
System, network tools		
binfmt-support.service	`sudo journalctl -u binfmt-support.service`	Enables support for additional executable binary formats
loadcpufreq.service	`sudo journalctl -u loadcpufreq.service`	Loads kernel modules needed to enable CPUFreq scaling
cpufrequtils.service	`sudo journalctl -u cpufrequtils.service`	Sets CPUFreq kernel parameters
netfilter-persistent.service	`sudo journalctl -u netfilter-persistent.service`	netfilter persistent configuration
isc-dhcp-server.service	`sudo journalctl -u isc-dhcp-server.service`	ISC DHCP IPv4 server
Analyzer service		
evparser.service	`/var/log/evparser`	EvParser service
vxCube Flow API service		

Service	Path to log file or command to view log	Description
vxcube-flow-api.service	`/var/log/vxcube-flow-api`	HyperboxAPI
vxCube services run in Docker containers		
vxcube-web	`/var/log/vxcube/testing`	vxCube web interface Path to docker-compose file: `/var/lib/vxcube/active/docker-compose.yml`
vxcube-redis	In the directory where docker-compose files are stored: `sudo docker-compose logs`	Path to docker-compose file: `/var/lib/vxcube/active/docker-compose.yml`
vxcube-postgres	In the directory where docker-compose files are stored: `sudo docker-compose logs`	Path to docker-compose file: `/var/lib/vxcube/active/docker-compose.yml`
yara-service	`/var/log/yara_service`	Path to docker-compose file: `/etc/yara_service/docker-compose.yml`
drweb-service_drweb-srv_1	`/var/log/drweb`	Path to docker-compose file: `/etc/drweb-service/docker-compose.yml`
drweb-service_drweb-se_1	In the directory where docker-compose files are stored: `sudo docker-compose logs`	Path to docker-compose file: `/etc/drweb-service/docker-compose.yml`

To view real-time logs, use the command `tail -f` <*path to log file*>.

If you use the `jourtnalctl` and `docker-compose logs` commands to view logs, follow the logs in real time using the `-f` option.

To collect logs for the technical support team, you can also use the following script:

```
if [ "$EUID" -ne 0 ]
  then echo "Please run as root"
  exit
fi
rm -rf support.tar.gz support.tar
set -x
ifconfig > ifconfig.log
journalctl -b > journal.log
tar -P -cf
```

```
support.tar /var/log/drweb /var/log/evparser /var/log/vxcube/testing /var/log/
nginx /var/log/hyperbox /var/log/openvpn /var/log/proftpd ifconfig.log
journal.log /var/lib/hyperbox/hbsetup.log
find "/var/lib/hyperbox/VirtualBox VMs/" -type d -name "Logs" -exec tar -P -
rvf support.tar {} \;
rm -rf ifconfig.log
rm -rf journal.log
gzip support.tar
set +x
```

To restart services that run in Docker containers

1. Go to the directory where the respective docker-compose files are saved.
2. Run commands to restart the service.

For the file `/var/lib/vxcube/active/docker-compose.yml`:

```
cd /var/lib/vxcube/active/

sudo docker-compose down

sudo docker-compose up -d
```

For the file `/etc/yara_service/docker-compose.yml`:

```
cd /etc/yara-service

sudo docker-compose down

sudo docker-compose up -d
```

Для `/etc/drweb-service/docker-compose.yml`:

```
cd /etc/drweb-service

sudo docker-compose down

sudo docker-compose up -d
```

⚠ To monitor the state of vxCube components, you can optionally install a Zabbix agent.

4. How to Update Dr.Web vxCube

You can update your installed Dr.Web vxCube service whenever a new version of the distribution and virtual machine images becomes available.

To do this, follow the steps below:

1. Download a product distributive and images to your computer. Unpack the archives. Unpack the distribution into the directory where you will run the installer.

> ⚠ We do not recommend unpacking the distribution in the directory where the previous version of the service is located. Choose another directory.

2. Put the Dr.Web vxCube license key into `confs/vxcube.key` of the unpacked distribution.
3. Put distribution files and images into the following directories:

- SSL certificates required for connecting with VPN servers and specified in the `vars-user.yml` file (the `openvpn_client_servers` variable) to the `confs/openvpn.crt`, `confs/openvpn.key`, and `confs/openvpn_ca.crt` directories;

> ⚠ SSL certificates are not supplied with Dr.Web vxCube; you need to obtain them separately.

- the received Windows virtual machine `.tar.gz` images and all `.tar.gz.ver` and `.tar.gz.hash` files to the `vm-images-win directory`;
- the received Android virtual machine `.vdi` images and all `.vdi.hash` and `.vdi.ver` files to the `vm-images-andr directory`;
- the received Linux virtual machine `.tar.gz` images and all `.tar.gz.hash` and `.tar.gz.ver` files to the `vm-images-linux directory`.

> ⚠ You can also put the virtual machine images into the directories you want. For this, specify the directories in the `vars-default.yml` file (in the `hyperbox_images_repo`, `dimas_images_repo`, and `linuxbox_images_repo` variables).

4. If you want Dr.Web vxCube to support the HTTPS protocol, do the following:

- create the `confs/web_ssl.crt` and `confs/web_ssl.key` files;
- create the `confs/web_dhparam.pem` file (if you have skipped step 5).
- in the `vars-default.yml` file, uncomment the following variables: `vxcube_web_ssl_cert`, `vxcube_web_ssl_privkey`, and `vxcube_web_dhparam`.

5. Update to OS Astra Linux 1.7.6. The file `/etc/apt/sources.list` must contain the following repositories:

```
# Extended repository
```

```
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free

# Astra 1.7.6 repository

deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-main/ 1.7_x86-64 main contrib non-free

deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-update/ 1.7_x86-64 main contrib non-free

deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-base/ 1.7_x86-64 main contrib non-free
```

6. After updating the repositories, run the following commands:

   ```
   sudo apt update
   sudo apt upgrade
   ```

7. Edit the installation settings. To do this, assign a value for each variable in the `vars-user.yml` file. All the variables in this file must have an assigned value. The detailed description of the variables is given in the file and in the Description of variables contained in vars-user.yml table.

   You may also configure variables in the `vars-default.yml` file. The detailed description of the variables is given in the file and in the Description of variables contained in vars-default.yml table.

8. Copy the `hyperbox_api_rq_password`, `vxcube_ftp_pass`, and `vxcube_web_db_pass` files from the `/credentials` directory where the previous version of Dr.Web vxCube was installed to `/credentials` of the latest version.

9. Run the commands to disable the old EvParser service:

   ```
   sudo systemctl stop evparser.service
   sudo systemctl disable evparser.service
   ```

Once you have completed all steps above, you could begin installing the service on a local server or on a remote server.

5. Signing in and out of Dr.Web vxCube

Signing in to Dr.Web vxCube

Before you start working with Dr.Web vxCube, make sure that your computer meets the system requirements.

To sign in to Dr.Web vxCube

1. Go to https://<*server IP*> or https://<*server domain name*>.
2. Enter your login information, which is the email address. You can find it in the `vxcube_web_superuser_email` variable, in the `vars-user.yml` file.
3. Enter your password. You can find it in the `vxcube_web_superuser_pass` variable, in the `vars-user.yml` file. If the variable has no assigned value, that means the password was generated automatically and stored in the `vxcube_web_superuser_pass` file in the `credentials` directory.

The first time you sign in, you will be prompted to accept the License Agreement.

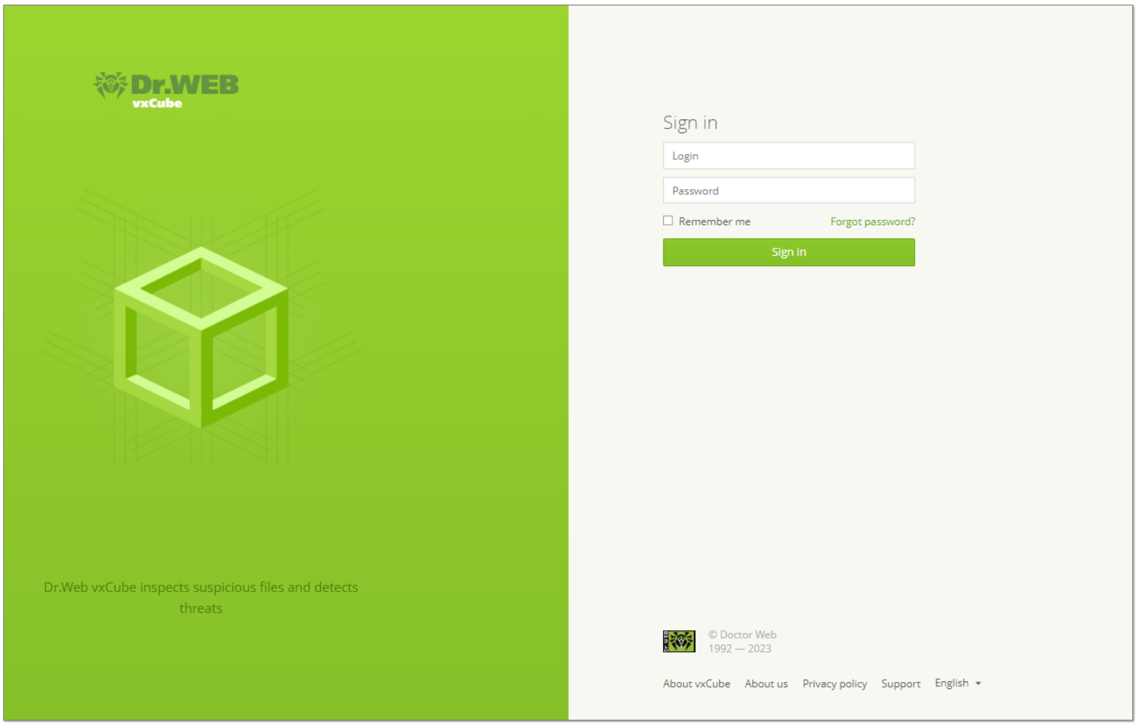


Figure 1. Dr.Web vxCube sign-in page

Signing out of your Dr.Web vxCube account

To sign out of your Dr.Web vxCube account, in the top right-hand corner of the main screen click 👤 **Profile > Sign out**.

6. Settings

You can change an interface language of Dr.Web vxCube (currently supports Russian and English), set default file analysis settings, and manage your API keys and password.

6.1. Changing an Interface Language

Dr.Web vxCube is available in English and Russian. By default, Dr.Web vxCube display language matches the language preferences of your browser.

To change your display language

1. Scroll down the page.
2. Click the language selection menu at the bottom of the page.
3. Select English or Russian in the drop-down.

6.2. Default Analysis Settings

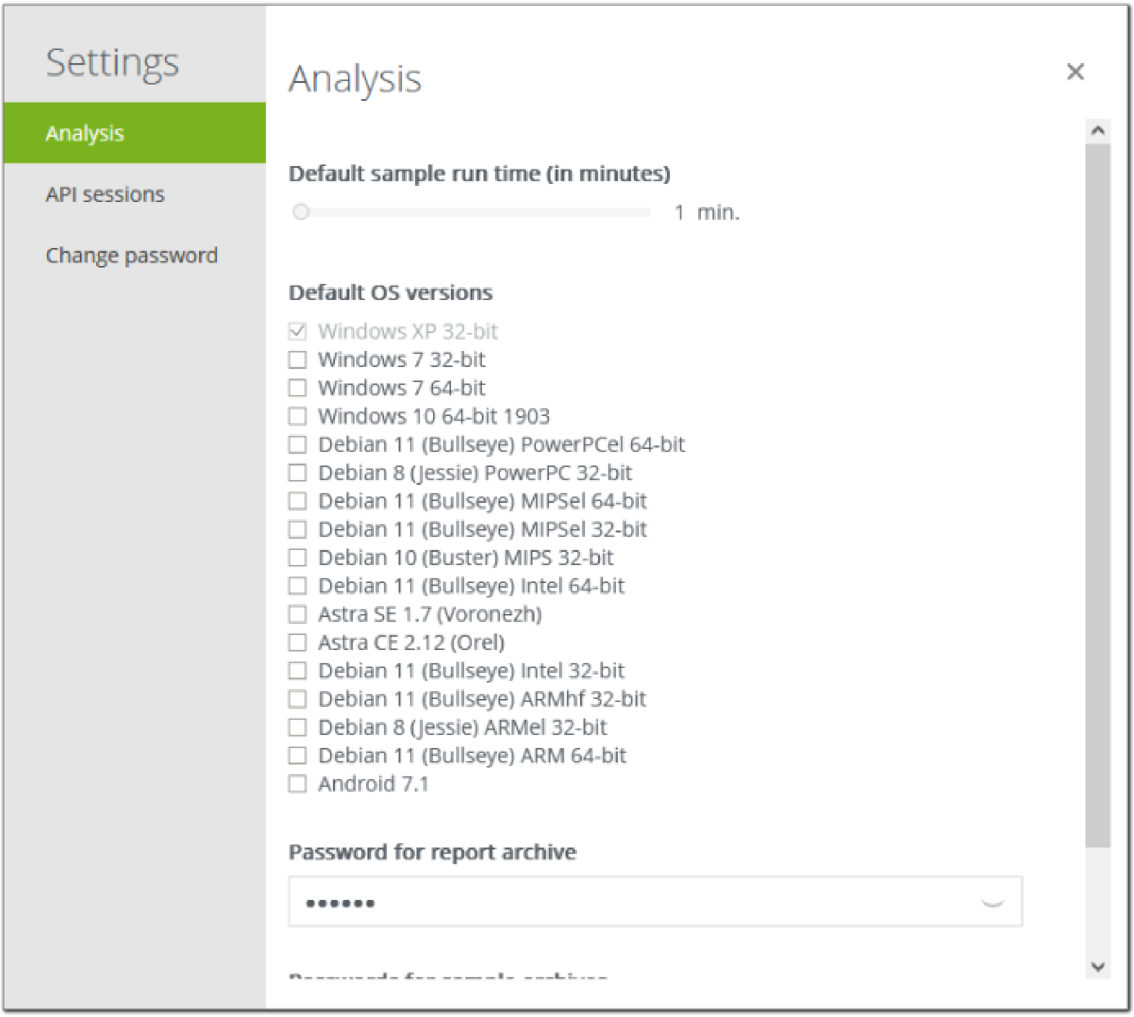
You can specify the default analysis settings such as sample run time on the virtual machine, OS versions to analyze on and the optional password for the report archive (if no password is set, the archive is sent without it).

In the **Passwords for sample archives** field, you can input passwords that will be used to analyze a password-protected archive.

⚠ In case a report archive is not password-protected, your local machine’s anti-virus can scan it and potentially detect it as malware, particularly if the report includes alloc function dumps.

To specify the default analysis settings

1. In the top right-hand corner of the main page, click 👤 **Profile > Settings**.
2. On the left, select the **Analysis** tab.
3. Specify the default settings for file analysis.



Analysis

Default sample run time (in minutes)

○ 1 min.

Default OS versions

☑ Windows XP 32-bit
☐ Windows 7 32-bit
☐ Windows 7 64-bit
☐ Windows 10 64-bit 1903
☐ Debian 11 (Bullseye) PowerPCel 64-bit
☐ Debian 8 (Jessie) PowerPC 32-bit
☐ Debian 11 (Bullseye) MIPSel 64-bit
☐ Debian 11 (Bullseye) MIPSel 32-bit
☐ Debian 10 (Buster) MIPS 32-bit
☐ Debian 11 (Bullseye) Intel 64-bit
☐ Astra SE 1.7 (Voronezh)
☐ Astra CE 2.12 (Orel)
☐ Debian 11 (Bullseye) Intel 32-bit
☐ Debian 11 (Bullseye) ARMhf 32-bit
☐ Debian 8 (Jessie) ARMel 32-bit
☐ Debian 11 (Bullseye) ARM 64-bit
☐ Android 7.1

Password for report archive

••••••

Figure 2. Settings

6.3. Managing a Password

If you have forgotten your Dr.Web vxCube password, you can reset it. You can also change your password if it has been compromised.

6.3.1. How to Change a Password

To change your password

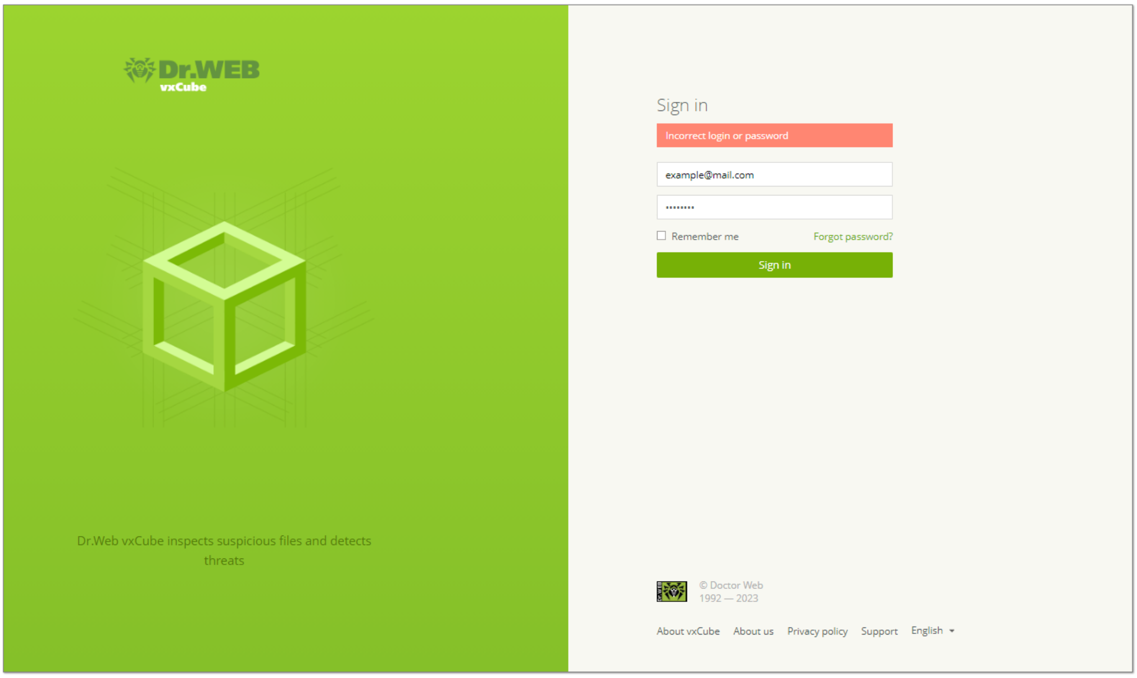
1. In the top right-hand corner of the main page, click **Profile > Settings**.
2. On the left, select the **Change password** tab.
3. Enter your current password, then enter the new one twice and click **Save**.

6.3.2. How to Reset a Password

Dr.Web vxCube uses email for password reset. Make sure that there is a configured SMTP server to support this feature. You can also set a different SMTP server in the `vxcube_web_mail_server` value of the `vars-default.yml` file.

To reset your password

1. On the Dr.Web vxCube login page, click **Forgot password?**.



Incorrect login or password

example@mail.com

••••••••

☐ Remember me

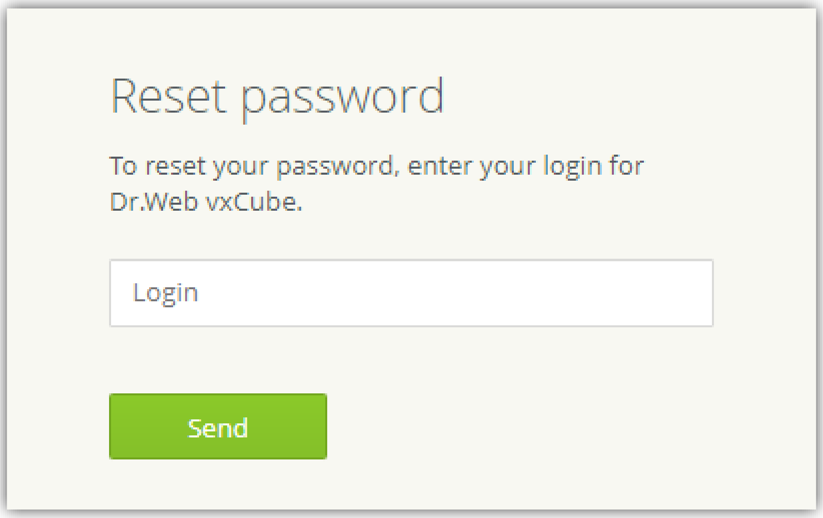
Dr.Web vxCube inspects suspicious files and detects threats

© Doctor Web 1992 — 2023

Figure 3. Failed to sign in to Dr.Web vxCube

2. On the **Reset password** page specify email address you used for registering in Dr.Web vxCube.
3. Select the **I’m not a robot** check box. It is only required if the CAPTCHA was enabled during the installation of Dr.Web vxCube.
4. Click **Send**.

   On this address, you will receive an email with a link for resetting your password. If you do not receive the email within 10 minutes, check the Spam folder or contact the server administrator.



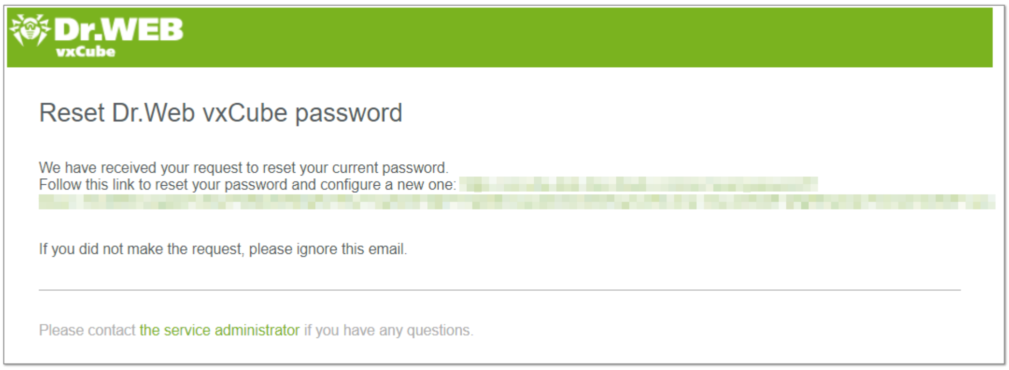
Reset password

To reset your password, enter your login for Dr.Web vxCube.

Figure 4. Requesting a password reset

5. Open the email you have received.
6. Follow the link to reset your password.

   You will be redirected to Dr.Web vxCube.



Reset Dr.Web vxCube password

We have received your request to reset your current password.
Follow this link to reset your password and configure a new one:

If you did not make the request, please ignore this email.

Please contact the service administrator if you have any questions.

Figure 5. Confirming the request to reset your password

7. Type in your new password and confirm it.
8. Click **Create**.

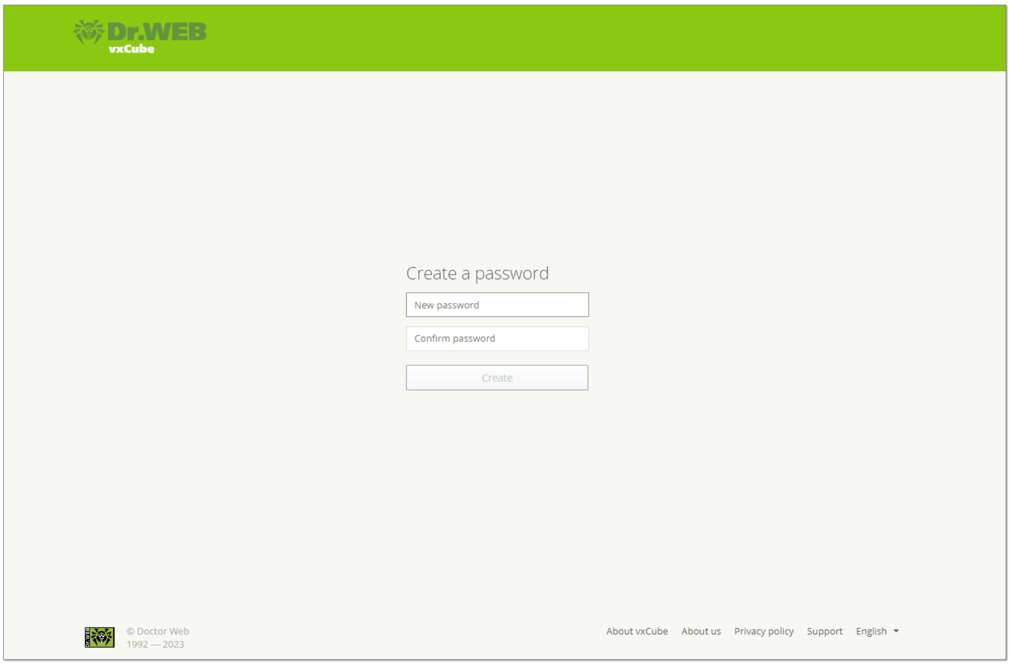


Figure 6. Creating a password

7. Licensing

To use Dr.Web vxCube, you need to purchase a license. When buying a license, you can select the options that best fit your needs:

- The platforms files can be analyzed at
- The license term

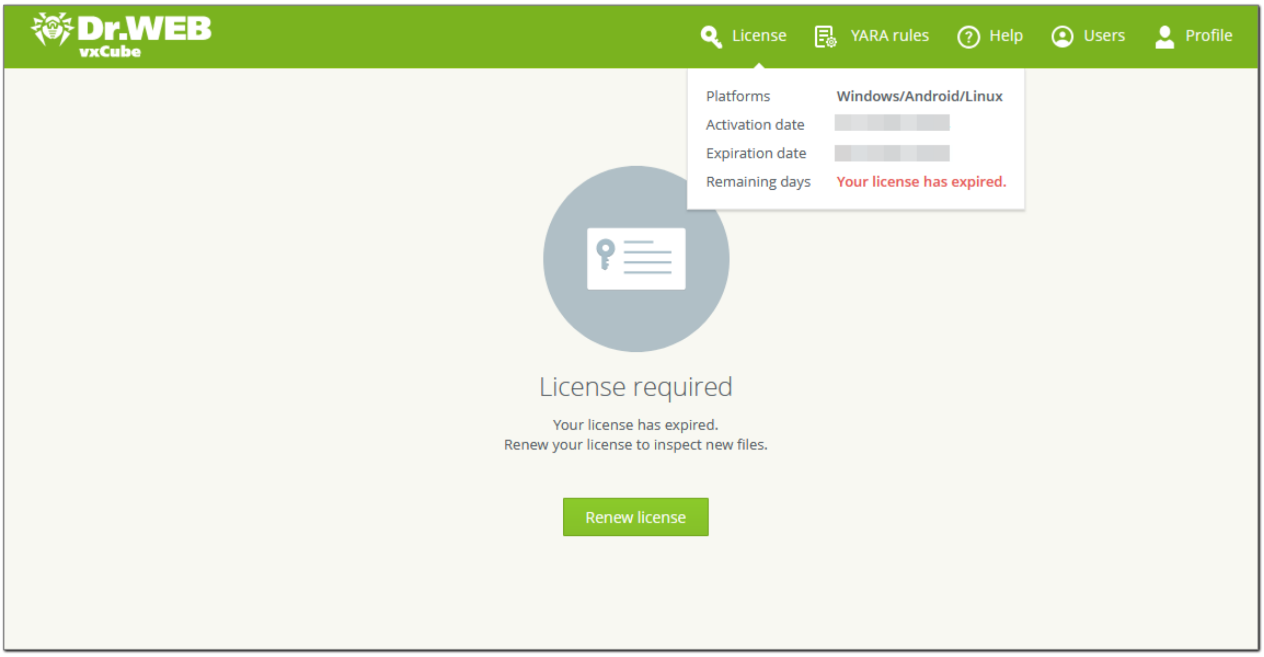
Once your license expires, you cannot upload the files for analysis on the service. However, you still can do the following:

- Sign in to Dr.Web vxCube
- View reports on the files analyzed earlier
- Download archives that contained analysis reports

To restore full Dr.Web vxCube functionality, renew the license.

Renewal of a license

When your license expires, a notification appears on the Dr.Web vxCube main page.



Platforms Windows/Android/Linux
Activation date
Expiration date
Remaining days Your license has expired.

License required

Your license has expired.
Renew your license to inspect new files.

When your license expires, a notification appears on the main screen. To restore full functionality of Dr.Web vxCube, click **Renew license**. You will be directed to the license purchasing page on the Doctor Web website where you can request the new license key file. Then, manually update the license following the instructions provided below.

To update the vxCube license manually

1. Change the name of your new key file, `drweb32.key`, to `vxcube.key` and save it to the `/etc/vbox/vxcube.key` directory, replacing the file that was already there.
2. Edit the license configuration file for vxcube-web as follows:
   a) In the `/opt/vxcube/config/default.yml` file, replace the `activation_date` and `expire_date` field values to the `Created` and `Expires` field values from your key file.

      Please note that you should edit the file volume-mounted on the host of the Docker container, not the file within the Docker container.

   b) Restart the vxcube-web service using the following commands:

```
cd /var/lib/vxcube/active

sudo docker-compose down

sudo docker-compose up -d
```

To update the scanning service (drweb-service) license manually

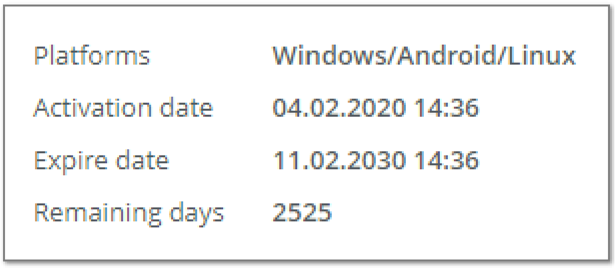
1. Save the new license file in the `/etc/drweb-service/drweb32.key` directory on the host of the Docker container (not within the container itself).
2. Restart the service using the following commands:

```
cd /etc/drweb-service

sudo docker-compose down

sudo docker-compose up -d
```

Information about the current license

To view your license details, click **License** at the top of the Dr.Web vxCube main page. The window with the following details opens:

- The platforms files can be analyzed at (Windows, Android, Linux)
- The number of days left until the license expires
- The date and time when the license was activated
- The date and time of the license expiry



Platforms	Windows/Android/Linux
Activation date	04.02.2020 14:36
Expire date	11.02.2030 14:36
Remaining days	2525

Figure 7. License details

8. YARA Rules

Using YARA rules you can identify and classify malware samples: a rule triggers when the condition within it is met. The condition can refer to the specific file contents, behavior, or location. YARA rules can include strings, boolean expressions, wildcards, regular expressions, special operators, and many other features. For more information about YARA rules, go to official YARA documentation.

YARA rules used in Dr.Web vxCube have some special capabilities:

- In the `meta` rule section, the required `maliciousness` field is added. This field is used to specify a maliciousness type that will be added to the report if the rule triggers
- Using the exclusive dr_sandbox module, you can create rules triggered when specific behavior for a file is detected on a virtual machine.

All the YARA rules in Dr.Web vxCube are divided into two categories: *system* rules and *user* rules. System rules are created by the Dr.Web vxCube developers and used in file analysis by default. You can’t view or edit the contents of system rules, as well as delete them, but you have the option to disable these rules that are not needed. Additionally, you can create your own (user) rules. User rules can be edited, disabled, or deleted.

8.1. How to Create a YARA Rule

All the YARA rules in Dr.Web vxCube follow the standard format:

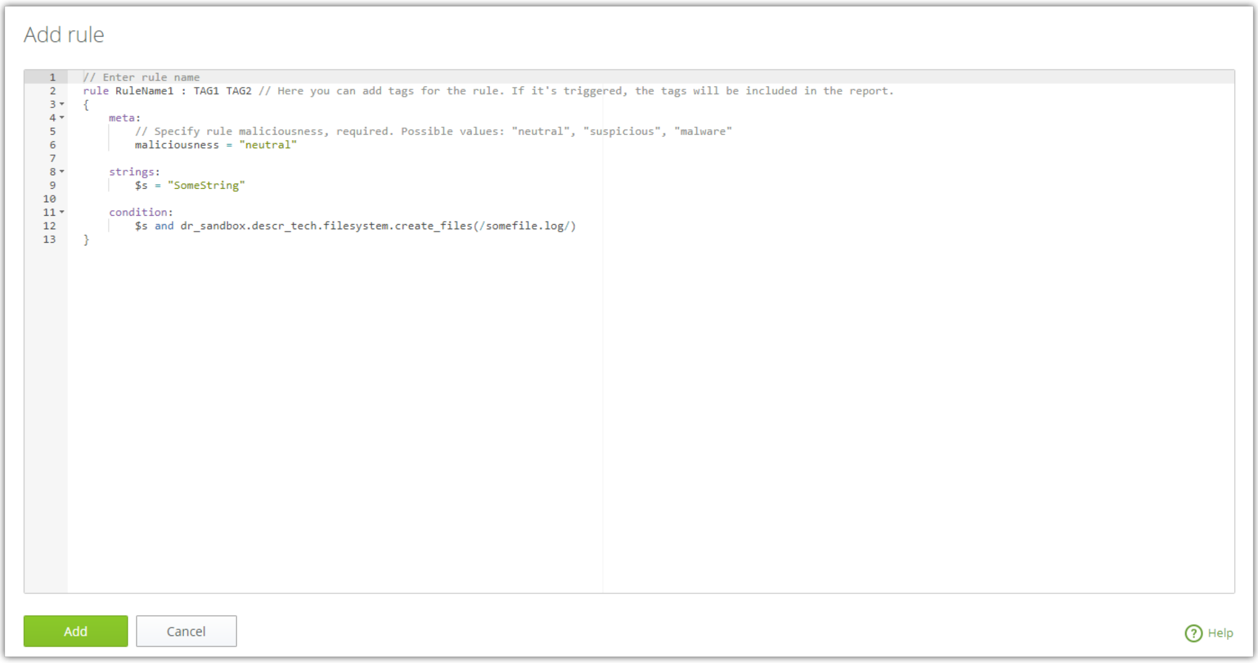
```
rule RuleName1 : TAG1 TAG2
{
    meta:
        maliciousness = "neutral"

    strings:
        $s = "SomeString"

    condition:
        $s
}
```

Every rule begins with the keyword `rule` followed by a rule name that should be entered using latin letters, digits, or underscore. Then, after a colon, you could specify tags. They will be included in the report if this rule is triggered during the file analysis. The rule body can contain three sections:

- The required `meta` section specifies the maliciousness type (the `maliciousness` field) that will be set for the file if the rule is triggered. The possible values for the field: `maliciousness`: `neutral`, `suspicious`, `malware`.
- In the required `condition` section, a condition is set. If the condition is met, the rule will be triggered.
- In the optional `strings` section, the strings that used in the rule are specified.

To create a YARA rule

1. At the top of the Dr.Web vxCube main page, click **YARA rules**.
2. Click ⊕ **Add**. The window containing a rule example code appears.
3. Edit the code to include the rule options you want.
4. Click **Add**.



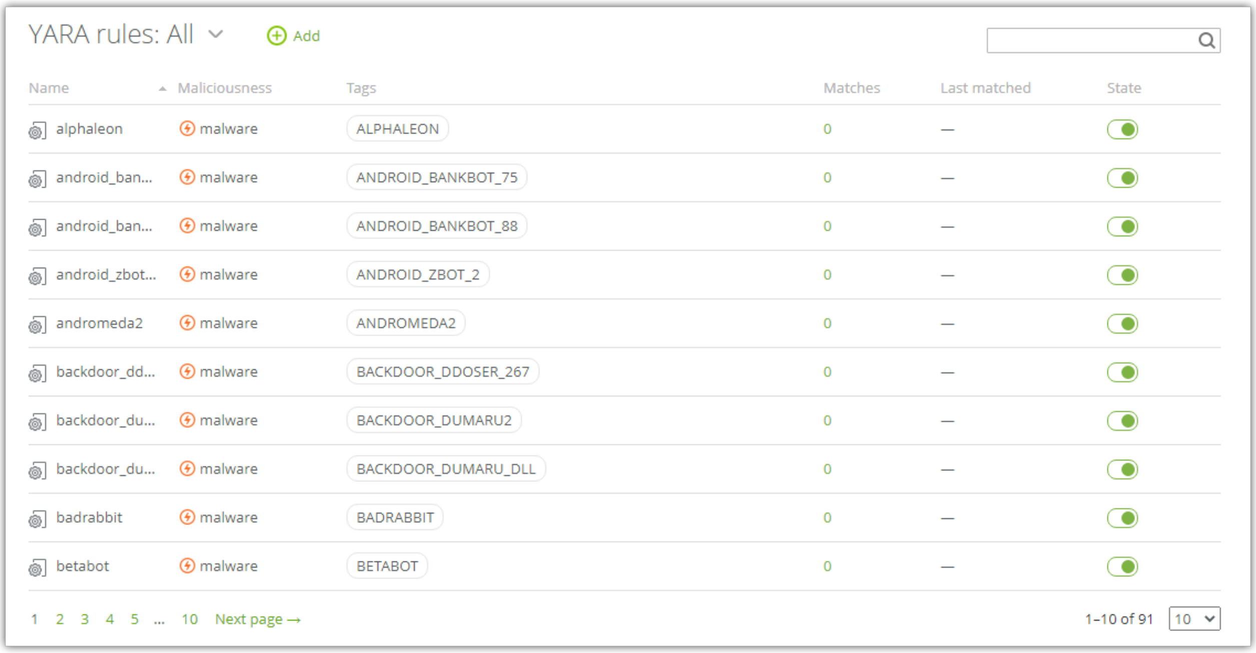
```
// Enter rule name
rule RuleName1 : TAG1 TAG2 // Here you can add tags for the rule. If it's triggered, the tags will be included in the report.
{
    meta:
        // Specify rule maliciousness, required. Possible values: "neutral", "suspicious", "malware"
        maliciousness = "neutral"

    strings:
        $s = "SomeString"

    condition:
        $s and dr_sandbox.descr_tech.filesystem.create_files(/somefile.log/)
}
```

Figure 8. Add rule window

8.2. How to Manage YARA Rules

Click **YARA rules** at the top of the Dr.Web vxCube main page to see all YARA rules available for your account. The YARA rule list that opens includes the following information for each rule:

- The rule type (👤 for user rules and ⚙ for system rules).
- **Name:** The rule name.
- **Maliciousness:** The maliciousness level specified in the rule.
- **Tags:** Tags specified in the rule.
- **Matches:** The total amount of matches for the particular rule.
- **Last matched:** The date when the rule was last triggered. If the trigger occurred today, the time will be shown instead of the date.
- **State:** The current state of the rule (enabled/disabled).



YARA rules: All ⌄ ⊕ Add

Name ▲	Maliciousness	Tags	Matches	Last matched	State
alphaleon	malware	ALPHALEON	0	—	●
android_ban...	malware	ANDROID_BANKBOT_75	0	—	●
android_ban...	malware	ANDROID_BANKBOT_88	0	—	●
android_zbot...	malware	ANDROID_ZBOT_2	0	—	●
andromeda2	malware	ANDROMEDA2	0	—	●
backdoor_dd...	malware	BACKDOOR_DDOSER_267	0	—	●
backdoor_du...	malware	BACKDOOR_DUMARU2	0	—	●
backdoor_du...	malware	BACKDOOR_DUMARU_DLL	0	—	●
badrabbit	malware	BADRABBIT	0	—	●
betabot	malware	BETABOT	0	—	●

1 2 3 4 5 ... 10 Next page → 1–10 of 91 10

Figure 9. The list of YARA rules

In the list of YARA rules, you can:

- Search for rules by their names and tags
- Filter rules by type (system/user)
- Sort rules
- View information about rule matches (the name of the file that the rule was triggered on, the date of triggering, OS)
- Edit, delete, and enable/disable rules

To search for a rule

- To find specific rule(s), type their name or tags (or a portion of them) in the search box located at the top right of the rule list.

To filter rules by type

- Next to the header of the rule list, click ⌄ and choose the filter option: **YARA rules: All**, **YARA rules: System**, or **YARA rules: User**.

To sort rules

- Click the header of the column you want to sort by. At the left of the header ▲ or ▼ will appear. To change the sorting direction, click the header again.

To view information about the rule matches

- In the **Matches** column, click the number of matches for the required rule. The page of reports on matches for this rule opens.

To edit a rule

- Hover over the row of the rule and click ✎ on the right.

To delete a rule

- Hover over the row of the rule and click 🗑 on the right.

To disable or enable a rule

- In the row of the rule, turn the ⬤ switcher on or off.

To set the number of rules displayed per page

- At the bottom right, select the required value (10, 25, 50, or 100) from the drop-down.

8.3. The Rule Matches

You can view information about all the matches of the particular YARA rule. To do this:

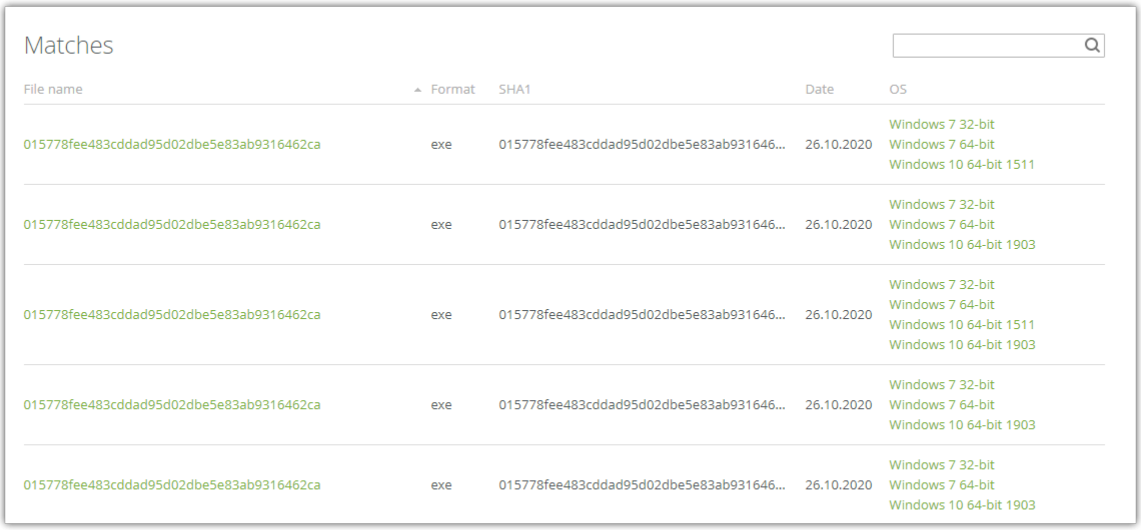
1. At the top of the Dr.Web vxCube main page, click **YARA rules**.
2. In the **Matches** column for the required rule, click the number.

The full list of matches for this rule opens. For each match, the following information is displayed:

- **File name:** The name of the file that the match occurred on.
- **Format:** The format of the file that the match occurred on.
- **SHA1:** The hash of the file.
- **Date:** The date when the match was occurred.
- **OS:** The list of operating systems that the analysis has been done for.

From the rule match report, you can go to the analysis report related to the particular match:

- To go to the report main page, click the file name in the corresponding row.
- To go to the report page for the specific platform, click the OS name in the corresponding row.



Matches

File name	Format	SHA1	Date	OS
015778fee483cddad95d02dbe5e83ab9316462ca	exe	015778fee483cddad95d02dbe5e83ab931646...	26.10.2020	Windows 7 32-bit Windows 7 64-bit Windows 10 64-bit 1511
015778fee483cddad95d02dbe5e83ab9316462ca	exe	015778fee483cddad95d02dbe5e83ab931646...	26.10.2020	Windows 7 32-bit Windows 7 64-bit Windows 10 64-bit 1903
015778fee483cddad95d02dbe5e83ab9316462ca	exe	015778fee483cddad95d02dbe5e83ab931646...	26.10.2020	Windows 7 32-bit Windows 7 64-bit Windows 10 64-bit 1511 Windows 10 64-bit 1903
015778fee483cddad95d02dbe5e83ab9316462ca	exe	015778fee483cddad95d02dbe5e83ab931646...	26.10.2020	Windows 7 32-bit Windows 7 64-bit Windows 10 64-bit 1903
015778fee483cddad95d02dbe5e83ab9316462ca	exe	015778fee483cddad95d02dbe5e83ab931646...	26.10.2020	Windows 7 32-bit Windows 7 64-bit Windows 10 64-bit 1903

Figure 10. Report on YARA rule matches

8.4. The dr_sandbox Module

The dr_sandbox module is an exclusive YARA module of Doctor Web. With dr_sandbox, you can create rules based on the following information:

- File behavior on a virtual machine
- Types of created files (`src`, `dump`, `drop`, `alloc` etc.)
- Details regarding detected threats
- The name of the analyzed file

The rule example that includes the `connect_to` function of dr_sandbox:

```
rule bad_file
{
    condition:
        dr_sandbox.descr_tech.network.connect_to(/http:\/\/someplace\.badsite\.com/)
}
```

You can find the full list of the dr_sandbox module functions in Appendix B. Functions of dr_sandbox module.

9. Analyzing Files

To analyze a file

1. Make sure Dr.Web vxCube supports the format of the file you want to analyze.
2. Browse for the file you want to check and upload it to the application.

   If Dr.Web vxCube cannot identify the file format automatically, you will be able to select it manually.
3. Select an environment for the analysis—an operating system version or an application version.

   You can select multiple OS versions or application versions.
4. (Optionally) Specify additional settings for analyzing the file.
5. Click **Analyze**.

> ⚠ Files can be also analyzed using API.

Analysis

When you start the analysis, one or several virtual machines with pre-installed software will be run. The number of virtual machines depends on the number of OS versions or application versions you have selected.

All events related to file behavior on a virtual machine are monitored to detect any suspicious activity. All processes on a guest OS are logged to the API Log. The analyzer uses a list of rules to categorize these processes.

The Dr.Web vxCube analyzer interacts with a *hypervisor* and does not use any additional software in the guest operating system (for example, drivers that hook functions). Thus, during analysis, the sample cannot detect or remove hooks.

Virtual machines connect to the internet through a dedicated proxy server. This helps fully analyze the virus behavior, especially if its functioning depends on downloading data from the internet.

In order to log events, Dr.Web vxCube interacts with a hypervisor, not with virtual machines. It means the analyzer cannot be detected.

You can connect to a virtual machine through a VNC (Virtual Network Computing) client and influence the analysis. Note that this can only be done when the virtual machine is operating.

Once the analysis is complete, you will receive a detailed report and be able to review the history of previously analyzed files.

Sometimes analysis of the same file may have different results if the file behavior depends on external conditions, for example, current date or availability of remote resources.

Additionally, results of analysis using VNC may differ from those obtained without VNC if the analyzed file uses an injection method unknown to Dr.Web vxCube, or the control is transferred to processes indirectly.

9.1. Supported Formats

Dr.Web vxCube supports the following formats:

File type	File format
Windows executable files	CPL, DLL, EXE, MSI, NATIVE APP, SYS
Android packages	APK
Microsoft Office documents	MHT, RTF, DOC, DOCX, DOCM, DOTM, DOTX, WPS, XLL, XLS, XLSX, XLSM, XLSB, XLAM, XTLX, XTLM, SLK, IQY, PPT, PPTX, PPTM, PPSX, PPSM, SLDX, SLDM, PPA, PPAM, THMX, POTX, POTM, XML, ACCDB, PUB, ODT, ODS, ODP
Acrobat Reader files	PDF
Java executable files	CLASS, JAR
Script files	BAT, JS, JSE, PL, PS1, PY, SCT, SH, VBE, VBS, WSF, XSL
*nix executable files	ELF
Other	7Z, ACE, ARJ, BZ2, CAB, CHM, DOCKER, EML, GZ, HTA, LNK, MOF, RAR, TAR, XZ, ZIP

Files with the ZIP, ARJ, XZ, ACE, TAR, BZ2, CAB, GZ, RAR, 7Z, or EML extensions can only be uploaded for analysis using API.

The file size cannot exceed 1000 MB.

File processing

For different formats, Dr.Web vxCube uses different ways of file processing and running.

If you choose a Microsoft Office, Acrobat Reader, or Java file for analysis, you will be prompted to select an app version to run the file instead of an OS version. For example, for a PDF file, you will need to choose between three versions of Acrobat Reader: 10.1, 11.0, or 15.10.

File formats and methods to launch them

File format	Launching
EXE	*%sample%*
DLL	regsvr32 /s *%sample%*
CPL	rundll32 shell32.dll, Control_RunDLL "*%sample%*"
SYS	sc create *%random_name%* type= kernel start= demand error= ignore binpath= "*%sample%*" DisplayName= *%random_name%* sc start *%random_name%*
NATIVE APP	rtlrun *%sample%*
MSI	msiexec.exe /i *%sample%*
MHT	winword *%sample%*
XML	msoxmled.exe
RTF, DOC, DOCX, DOCM, DOTM, DOTX, WPS, ODT	winword.exe
XLS, XLSX, XLSM, XLSB, XLAM, XTLX, XTLM, SLK, IQY, ODS	excel.exe
PPT, PPTX, PPTM, PPSX, PPSM, SLDX, SLDM, PPA, PPAM, THMX, POTX, POTM, ODP	powerpnt.exe
ACCDB	msaccess.exe
PUB	mspub.exe
PDF	acrord32.exe
JAR	javaw -jar *%sample%*
CLASS	java *%sample%*
JS, VBS, WSF, JSE, VBE	wscript /b /nologo *%sample%*
PS1	powershell -file *%sample%*

File format	Launching
BAT	cmd /c *%sample%*
SCT	regsvr32.exe /s /i:*%sample%* scrobj.dll
XSL	wmic printjob get /format:"*%sample%*"
MOF	mofcomp *%sample%*
LNK, HTA	*%sample%*
CHM	hh.exe
XLL	excel.exe *%sample%*
ELF	*%sample%*
SH	bash *%sample%*
PY	python *%sample%*
PL	perl *%sample%*
DOCKER	docker load -i *%sample%* docker run *%image_id%*

%sample% is the name of the analyzed file on a virtual machine.

%random_name% is a randomly given name.

9.2. Uploading Files to be Analyzed

To upload a file for analysis

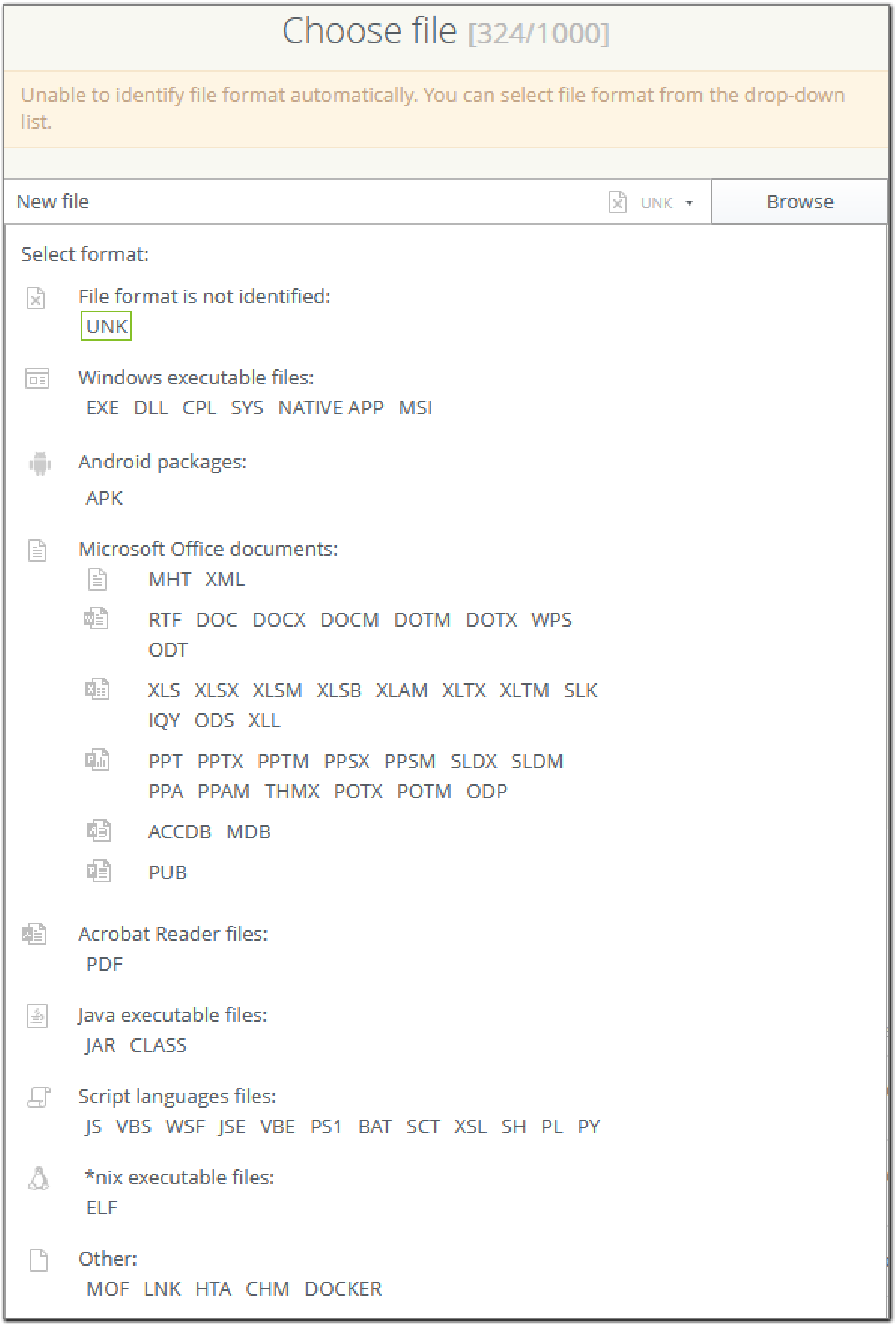
1. On the Dr.Web vxCube main page, click the **Browse** button or the file-select field. Select a file you want to analyze.

   You can also drag a file into the file-select field.

   The uploaded file format is detected automatically by its content.

   If the format is not identified (UNK), you will see the **Unable to identify file format** message. In this case, you can select the file format manually.

   ⚠ The MOF, JS, VBS, WSF, JSE, VBE, PS1, and BAT file formats may be identified incorrectly. For these files, it’s recommended that you select format manually.



Choose file [324/1000]

Unable to identify file format automatically. You can select file format from the drop-down list.

New file UNK ▾ Browse

Select format:

File format is not identified:
UNK

Windows executable files:
EXE DLL CPL SYS NATIVE APP MSI

Android packages:
APK

Microsoft Office documents:
MHT XML
RTF DOC DOCX DOCM DOTM DOTX WPS ODT
XLS XLSX XLSM XLSB XLAM XLTX XLTM SLK IQY ODS XLL
PPT PPTX PPTM PPSX PPSM SLDX SLDM PPA PPAM THMX POTX POTM ODP
ACCDB MDB
PUB

Acrobat Reader files:
PDF

Java executable files:
JAR CLASS

Script languages files:
JS VBS WSF JSE VBE PS1 BAT SCT XSL SH PL PY

*nix executable files:
ELF

Other:
MOF LNK HTA CHM DOCKER

Figure 11. Selecting file format manually

To select a file format manually, click drop-down arrow and select the corresponding format.

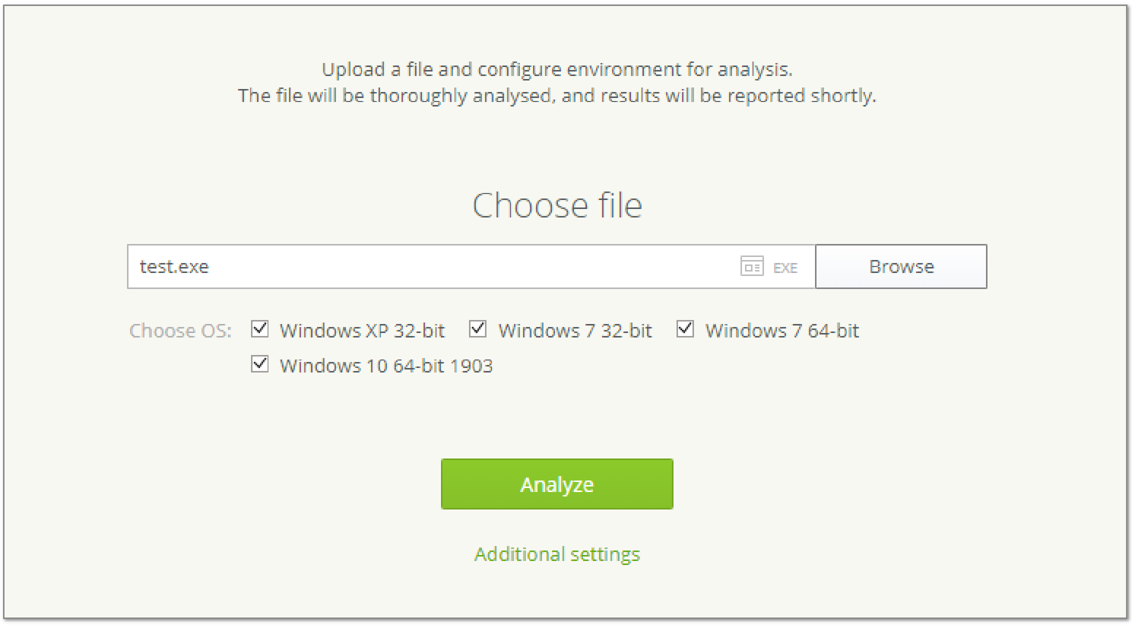
Make sure you have selected a correct file format. Otherwise, analysis results may be inaccurate.

2. Choose an operating system or an application version for running the file and specify additional settings if necessary.

You can select multiple OS versions or application versions: then multiple virtual machines will be launched. For example, if you select two Windows OS versions to analyze an executable file (.exe), Dr.Web vxCube will run two VMs.

3. Click **Analyze** to start checking the file.

You can run analysis of multiple files one by one. Click **Back** at the top of the page and then choose another file. The ⁛ icon displays progress of each analysis.



Upload a file and configure environment for analysis.
The file will be thoroughly analysed, and results will be reported shortly.

Choose file

test.exe EXE | Browse

Choose OS: ☑ Windows XP 32-bit ☑ Windows 7 32-bit ☑ Windows 7 64-bit
☑ Windows 10 64-bit 1903

Analyze

Additional settings

Figure 12. Uploading a file for analysis

9.3. Additional Settings

- **Sample name**

  Use this option if you want to submit the file for analysis under a different name. The original file won’t be overridden.

- **Use VNC**

  The use of VNC client is convenient if you choose more than one operating system and you want to influence the process on each of them.

  To activate the function, select the **Use VNC** check box. When you start the analysis, new browser tabs open automatically. Tabs are connected to the corresponding virtual machines via the VNC client. At the top of each tab, a progress bar is displayed. The bar shows the completion percentage and the current state of the analysis.

  Although new tabs open immediately, it can take some time to connect to virtual machines.

> ⚠ If you have not selected this option in **Additional settings** and have already started the analysis, click **Use VNC** on the analysis page. VNC client will open in a new tab.

- **Monitor all processes if VNC is used**

  By default, this setting is disabled and the report only includes the processes engaged in malicious activity.

- **Show MITM traffic**

  Select this check box if you want Dr.Web vxCube to parse encrypted traffic. This option is limited to Windows platforms. Once the analysis is done, you can view the decrypted traffic. To do this:

  1. Open the report page generated as a result of the analysis.
  2. Click zip **Download archive**.
  3. Unzip the archive. If prompted, input the password specified in the **Password for report archive** field in Settings. The default password is `vxcube`.
  4. Locate the `network.pcapng` file in the unpacked archive and upload it into a network packet analyzer like Wireshark.

- **Sample run time**

  The default sample run time in Dr.Web vxCube is 1 minute. You can adjust this value for the particular file if required. For example, you can increase the value if a file needs more time to show suspicious behavior. To do this, move the slider to the right.

- **Total size limit for drops**

  By default, the total size for files created during the analysis is limited to 64 MB. You can increase it to 512 MB.

- **Specify a command to run the file**

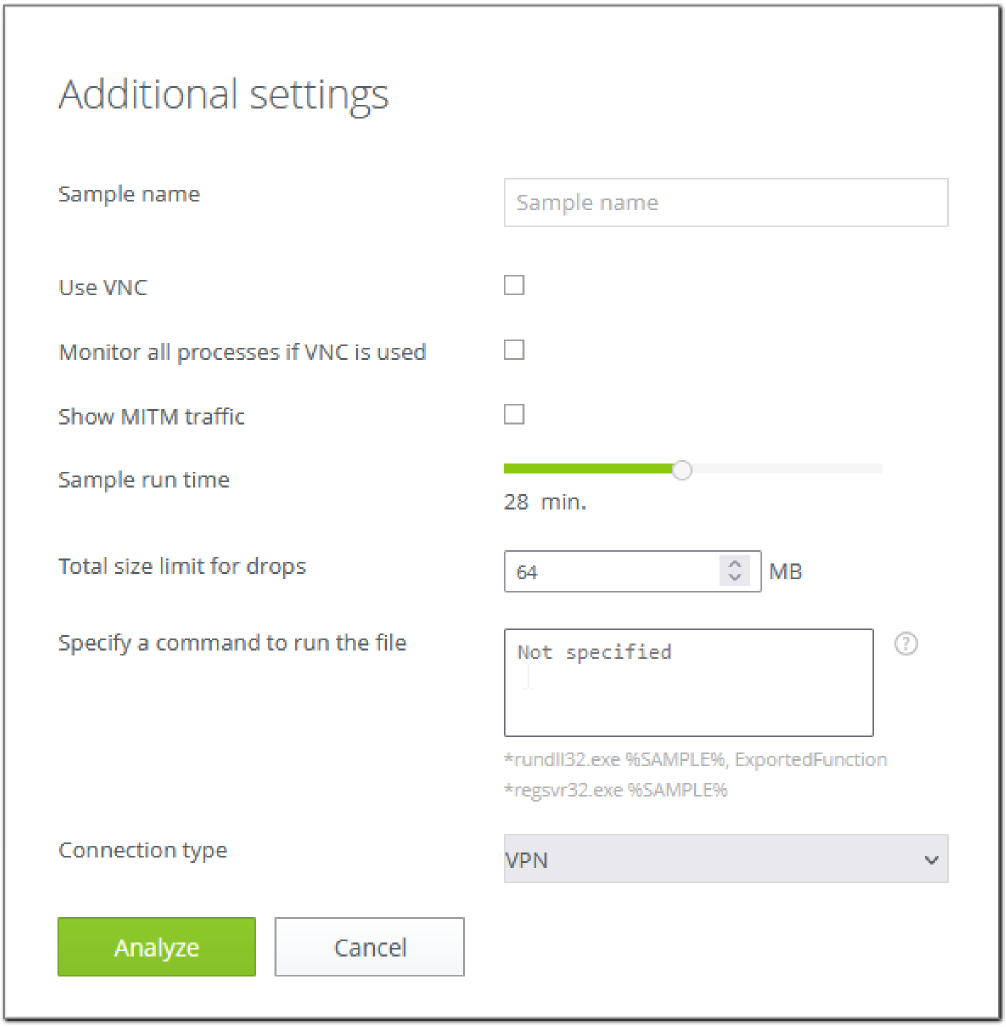
  This option allows you to set a specific command to run the file analysis. You can use any application from the standard Windows pack as a command, for example, `rundll32.exe`, `regsvr32.exe`, `notepad.exe`, etc. To use the command, specify it in the **Specify a command to run the file** field.

  You can specify a full path to the file using the special `%SAMPLE%` parameter.

  You can use this option if you need to run an executable file by calling an exported function. For example, `rundll32 %SAMPLE%, ExportedFunction`.

- **Connection type**

  VPN is used by default. For some connection types, you can specify a proxy server address and authorization parameters. Only TCP connections are proxied. Traffic of the other protocols is transferred through the default VPN server. To redirect UDP traffic, select the **Redirect UDP** check box.



Additional settings

Sample name: Sample name

Use VNC □

Monitor all processes if VNC is used □

Show MITM traffic □

Sample run time: 28 min.

Total size limit for drops: 64 MB

Specify a command to run the file: Not specified

*rundll32.exe %SAMPLE%, ExportedFunction

*regsvr32.exe %SAMPLE%

Connection type: VPN

Figure 13. Additional settings

After specifying additional settings

- Click **Analyze** to start analyzing the file.
- Click **Cancel** to reset settings and close the window.

> Additional settings are only applied to the current file. If you close the **Additional settings** window or select another file, you will have to configure the settings again.

10. Reports

Information obtained during the analysis is recorded in a report. Then you can open or download the report.

10.1. Opening a Report

To open a report

- If you keep the analysis page open, the report opens automatically once the analysis is done.
- If you had left the page before the analysis was completed, select the file you were analyzing in the **History** section on the Dr.Web vxCube main page.

10.2. Downloading a Report

On the report page, you can use the download buttons to:

Download an original file.

Download a ZIP archive with the report. The default password for the archive is **vxcube**.

Download a report in either HTML or PDF format.

Download a PCAP file.

To download a report

1. At the top of the report page, select a platform.
2. Click **Download report** to open the **Report parameters** window.
3. Select a report format: HTML or PDF.
4. Select the sections you need to include in the report. The **API log** and **Intents** sections may contain thousands of records; you can filter the records by the degree of danger.
5. Click **Download report**.

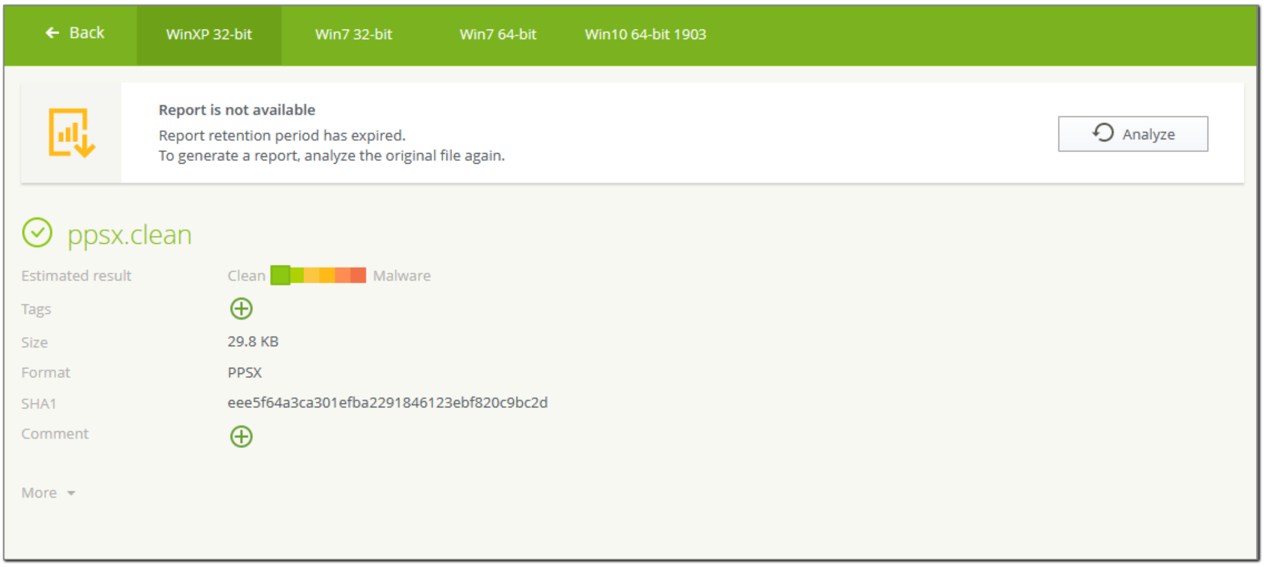
⚠ The **Intents** table is only present in reports for Android packages.

10.3. The Retention Period of Reports

The guaranteed period for keeping reports is set in the `vxcube_web_keep_reports` variable (the default value is 20 minutes). Once this period is over, a report could be removed from the server.

Once the report is removed, only the general information will remain on the report page, with a notification about the report's expiration at the top.

To generate the report again, restart the analysis. To do so, click **Analyze** on the report page.



Report is not available

Report retention period has expired.
To generate a report, analyze the original file again.

ppsx.clean

Estimated result	Clean 🟩🟩🟨🟧🟥 Malware
Tags	⊕
Size	29.8 KB
Format	PPSX
SHA1	eee5f64a3ca301efba2291846123ebf820c9bc2d
Comment	⊕

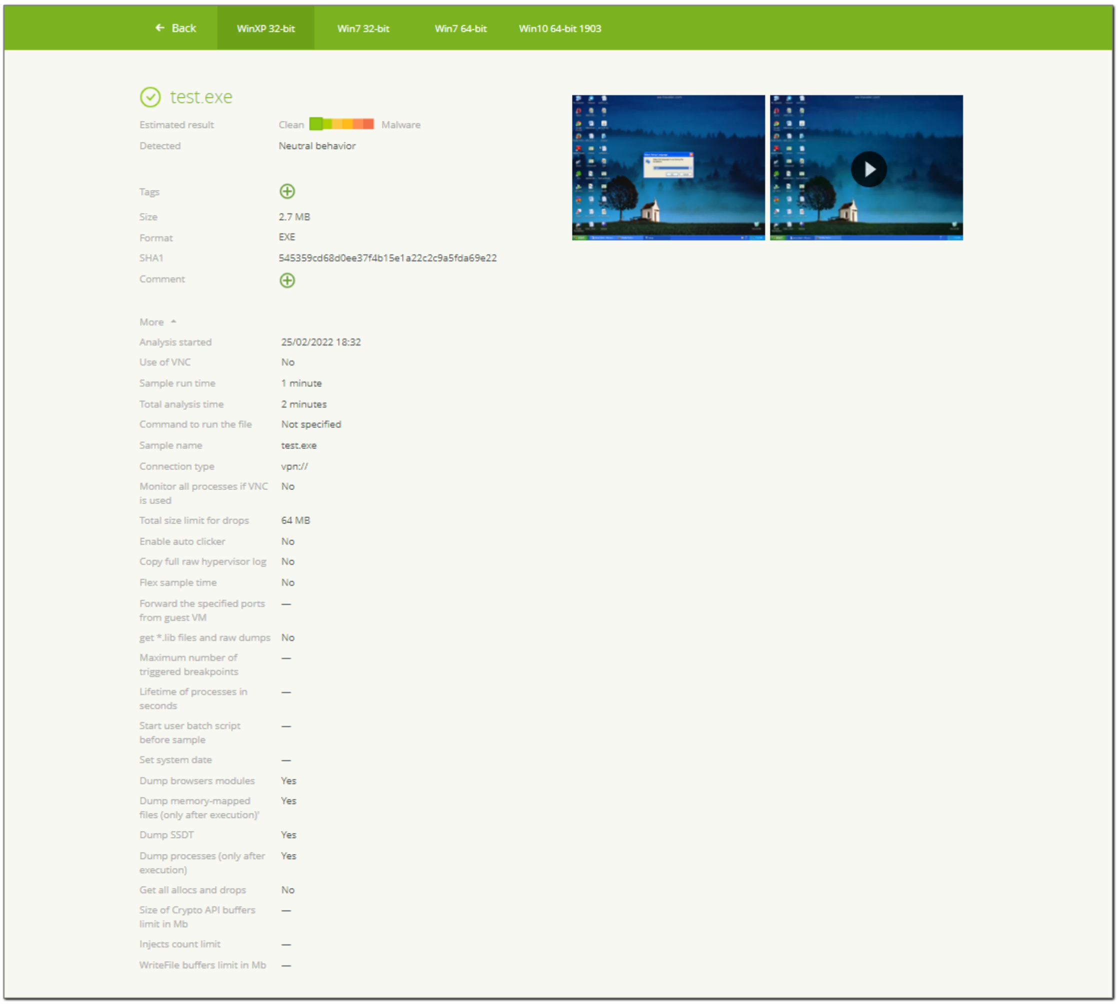
Figure 14. Notification about the report's expiration

10.4. The Report Structure

A report is divided into two parts: general information and main part.

General information consists of two sections: *basic details* and *more details*. Basic details provide a sample size, a sample format, an estimated analysis result, and other basic information. In the More details section you can find information such as a sample name, analysis start date and time, and total analysis time. Here you can also view the additional options, which are set for the analysis. You can explore these options, change them if needed and re-analyze the sample.

Main part can include the following sections: *Manifest*, *Behavior and YARA rules*, *Process graph*, *Description*, *Files and dumps*, *Phone calls and SMS*, *API Log and intents*, and *Network activity map*. The sections that are included in the list can differ based on a sample file format. For example, some of these sections are specific for reports of Android package analyses.



test.exe

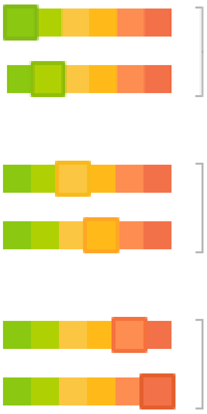
Estimated result	Clean 🟩🟨🟧🟥 Malware
Detected	Neutral behavior
Tags	⊕
Size	2.7 MB
Format	EXE
SHA1	545359cd68d0ee37f4b15e1a22c2c9a5fda69e22
Comment	⊕

More ▴

Analysis started	25/02/2022 18:32
Use of VNC	No
Sample run time	1 minute
Total analysis time	2 minutes
Command to run the file	Not specified
Sample name	test.exe
Connection type	vpn://
Monitor all processes if VNC is used	No
Total size limit for drops	64 MB
Enable auto clicker	No
Copy full raw hypervisor log	No
Flex sample time	No
Forward the specified ports from guest VM	—
get *.lib files and raw dumps	No
Maximum number of triggered breakpoints	—
Lifetime of processes in seconds	—
Start user batch script before sample	—
Set system date	—
Dump browsers modules	Yes
Dump memory-mapped files (only after execution)'	Yes
Dump SSDT	Yes
Dump processes (only after execution)	Yes
Get all allocs and drops	No
Size of Crypto API buffers limit in Mb	—
Injects count limit	—
WriteFile buffers limit in Mb	—

Figure 15. Report structure

10.4.1. General Information

Item	Description
Estimated result	Overall assessment of possible maliciousness.  Clean file Suspicious file Malware
Detected	Brief information on the file behavior and detected threats.

Item	Description
Tags	Tags added by a user or by a triggered YARA rule.
Size	File size.
Format	File format.
SHA1	File hash.
Comment	In this field, you can put any additional information you may need. There is a limit of 200 characters for a comment.
More	
Analysis started	Date and time the analysis started. It is counted from the moment the file was launched on a virtual machine.
Use of VNC	Use of the VNC client during the analysis (yes/no).
Sample run time	Sample run time that was specified in the additional settings of analysis.
Total analysis time	Total duration of file analysis.
Command to run the file	The command specified in the additional settings to run the file you are analyzing.
Sample name	The name of the file that was sent for analysis. More...
Connection type	The type of the connection. More...
Monitor all processes if VNC is used	Monitor all processes if VNC is used (yes/no). More...
Total size limit for drops	The limit on the total size of files generated during analysis. More...
Enable auto clicker	Enable auto clicker (yes/no).
Copy full raw hypervisor log	Copy full raw hypervisor log (yes/no).
Flex sample time	Use flex sample time (yes/no).
Forward the specified ports from guest VM	Forward the specified ports from guest VM. Example: `2343, 4353:tcp`.
Get `*.lib` files and raw dumps	Get `*.lib` files and raw dumps (yes/no).

Item	Description
Maximum number of triggered breakpoints	Set the maximum number of triggered breakpoints.
Lifetime of processes in seconds	Set the lifetime of processes. Example: `notepad.exe,35,winword.exe,20`.
Start user batch script before sample	Start a user batch script before running the sample.
Set system date	Set a system date on VM on which the analysis is performed. Example: `17.03.2022`.
Dump browser modules	Dump browser modules (yes/no).
Dump memory-mapped files (only after execution)	Dump memory-mapped files (only after execution) (yes/no).
Dump SSDT	Dump SSDT (yes/no).
Dump processes (only after execution)	Dump processes (yes/no).
Get all allocs and drops	Get all allocs and drops (yes/no).
Size of Crypto API buffers limit in MB	Set size of Crypto API buffers limit in MB. Example: `512`.
Injects count limit	Set a limit for injects. Example: `100`.
WriteFile buffers limit in MB	Set WriteFile buffers limit in MB. Example: `256`.

To the right from the general information part, there is a screenshot and a video report about the file’s behavior when it was run in a guest operating system.

10.4.2. Main Part

The main part may contain the following sections, depending on the sample format.

Section	Android packages (optional)	Other formats
Manifest	+	–
Behavior and YARA rules	+	+

Section	Android packages (optional)	Other formats
Process graph	–	+
Description	+	+
Files and dumps	+	+
Phone calls and SMS	+	–
API log and intents	+	**API log** only
Network activity map	+	+

10.4.2.1. Manifest (optional)

⚠ The section appears in reports for Android packages only.

The section contains the following information from the `AndroidManifest.xml` file:

Component	Comment
Package	Application package name.
Application name	Application name that appears to the user.
Version code	Internal version number.
Version name	Name and/or number of the version that appears to the user.
Permissions	Permissions that are requested by the application for its operation.

The section also contains the following components that are declared in the manifest: activities, broadcast receivers, and services.

10.4.2.2. Behavior and YARA rules

The section contains two tables: **Behavior** and **YARA rules**. To open a table, click its name.

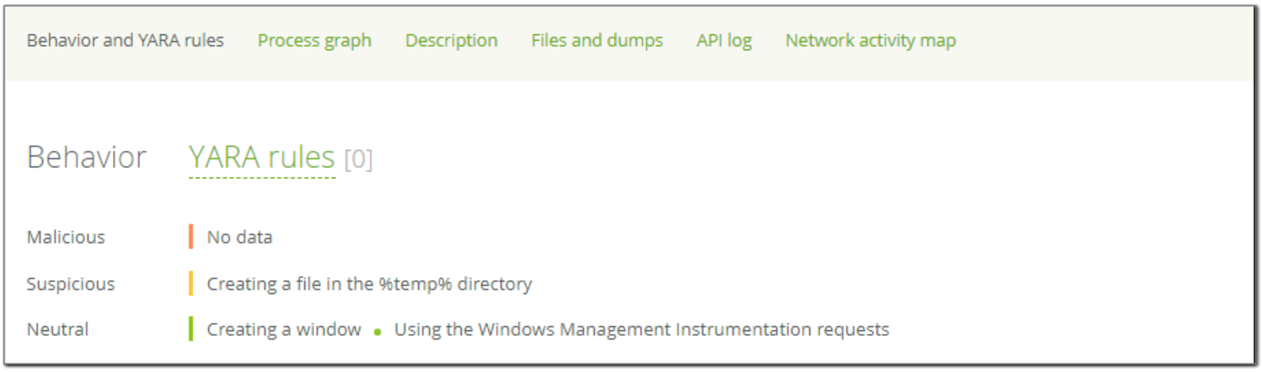
Behavior

The section contains a brief description on file behavior.

Dr.Web vxCube records all actions registered on a virtual machine throughout the analysis and categorizes them depending on how harmful they may be.

Dr.Web vxCube defines 3 categories of file behavior:

- Malicious
- Suspicious
- Neutral



Behavior YARA rules [0]

Malicious	No data
Suspicious	Creating a file in the %temp% directory
Neutral	Creating a window • Using the Windows Management Instrumentation requests

Figure 16. Reports on file behavior and YARA rules triggers

YARA Rules

The section contains information on YARA rule matches. The number of rules triggered during the analysis is displayed to the right from the table name.

The table displays information about the analysis results, tags, and triggered rule names.

To learn more about a rule, click its name.

To sort table columns in ascending or descending order, click the column titles.

10.4.2.3. Process Graph

⚠ The section is absent in reports for Android packages.

The section contains information about suspicious processes registered on a virtual machine. The data is represented as an interactive graph with an explanatory unit for each process.

To open the graph in a new tab, click the **Process graph** title. To zoom in or zoom out, click + or −. You can also zoom in by double-clicking the graph.

Conventions

Convention	Comment
■■■■■	Process or resource maliciousness. Measured on a scale from 0 to 100: ■ Less than 20. ■ Less than 40. ■ Less than 60. ■ Less than 80. ■ Less than 100.
▭	Process. The unit color corresponds to the process maliciousness.
☁ ☁☁ ☁☁☁	Network resource with remote access. The cloud color corresponds to the resource maliciousness. The protocol level and the IP address of the remote resource are displayed inside the cloud. 2 clouds are displayed if a process connects to the resource 2–5 times. 3 clouds are displayed if a process connects to the resource 6 times or more. In these cases, a number of connections is also displayed inside the cloud.
⌽	Sample. The sign is used to mark the first running process.
⚡	Known threat that is contained in the Dr.Web virus databases. The sign is used to mark a process if a threat is detected in its dump.
⚙	Known threat that is contained in the Dr.Web virus databases and that is detected in a dump of a loaded module. The sign is used to mark a process that a malicious module is loaded into. If threats are detected in both process and module dumps, the process is marked only with the ⚡ sign.
→	Process creation.
⇢	Injection into another process.
⇢	Web query.
⇢	RPC request.

Description

Click a process unit to show the information about a process in the description part.

Process parameters

Parameter	Description
PID	Process unique ID.
Full path	The path in which the process is run.
Run parameters	Special parameters for the process running. Optional field.
Behavior	The rules corresponding to tags about suspicious behavior of a process.
View the process activity	A link to the API log. Data in the log is filtered by process. To learn more about this feature, refer to API Log.
Download the dump file	Link for downloading the dump of the process.

Network resource parameters

Parameter	Description
Address	IP address of the network resource.
Port	Port number.

Protocol level	Protocol level of the OSI network model used for data transferring:
	• **Transport**
	• **Application**
	⚠ If the analyzer fails to determine the application level protocol, the following information will be displayed in this field:
	`Application: UNK`
	`Unknown data: {16,03,01,00,41,45…06,00,13,00,00,63,01,00}`

Query	This field is displayed if **Protocol level** is determined as **Application: DNS**.
URL	This field is displayed if **Protocol level** is determined as **Application: HTTP**.

10.4.2.4. Description

This section contains information about suspicious activity of a file, including objects, connections, etc. The data is grouped into categories and subcategories, depending on file behavior. The list of categories and subcategories is given below.

Enabling autorun and distribution

- Modifies the listed registry keys.
- Creates or modifies the listed files.
- Sets a service to autorun.
- Creates the listed services.
- Changes the listed executable system files.
- Replaces the listed executable system files.
- Replaces system binary files.
- Replaces system binary files using a symbolic link.
- Infects the listed executable files.
- Creates the following files on removable media.
- Modifies master boot record (MBR).
- Creates or modifies files to ensure autorun:
    - in /init.d;
    - in /router;
    - in /cron;
    - on desktop;
    - in other folders.
- Creates or modifies files to ensure autorun using symbolic links:
    - in /cron.
- Creates or modifies symbolic links to ensure autorun:
    - in /init.d;
    - on desktop;
    - in other folders.

Malicious functions

- Bypasses firewall, removes, or modifies the listed registry keys.
- To complicate detection of its presence in the operating system:
    - Forces the system to hide from view:
        - hidden files;
        - file extensions.
    - Blocks execution of the listed system utilities:

    - Command Prompt (CMD);
    - Windows Task Manager (Taskmgr);
    - Registry Editor (RegEdit).
    - Windows Firewall.
    - System Updates (Windows Update).
    - Windows Security Center.
    - System Anti-virus (Windows Defender).
  - Blocks the following features:
    - System Restore (SR);
    - Windows File Protection (WFP);
    - User Account Control (UAC);
    - System File Checker (SFC);
    - Windows Security Center.
    - Windows Support Center (Action Center).
  - Changes the listed system preferences:
    - changes the DNS server;
    - disables taskbar notifications.
  - removes shadow copies of volumes;
  - adds anti-virus exceptions using the listed registry keys.
- Creates and executes the listed processes:
  - creates and executes files (an exploit);
  - creates and loads libraries (an exploit);
  - downloads and executes files.
- Executes the listed processes.
- Injects code into the listed processes:
  - listed system processes;
  - listed user processes;
  - a large number of user processes.
- Installs hooks to intercept notifications:
  - About keystrokes:
    - Handler for all processes;
    - Handler for the listed processes.
- Terminates or attempts to terminate:
  - processes;
  - listed system processes;

  - listed user processes;
  - a large number of user processes.
  - processes of traffic analysis and program running applications;
  - processes by name.
- Searches for registry branches where third-party applications store passwords.
- Executes WMI operations.
- Registers a file system filter driver.
- Searches for the listed windows to:
  - bypass different anti-viruses;
  - bypass the Windows File Protection system;
  - detect analytics tools;
  - detect applications and games;
  - detect virtual machines.
- Creates an onion service.
- Loads the listed drivers.
- Hooks the following functions in the System Service Descriptor Table (SSDT):
  - a handler.
- Restores hooked functions in the System Service Descriptor Table (SSDT).
- Brute forces passwords of OS accounts.
- Performs a bruteforce attack in the network.
- Disables AMSI.
- Changes firewall settings.
- Changes router settings.
- Stops critical services.
- Manages services.
- Blocks through firewall:
  - SSH;
  - telnet;
  - standard web service ports.
- Modifies the listed settings of Windows Explorer.
- Modifies the listed settings of Windows Internet Explorer.
- Affects processes:
  - hides the listed processes;
  - traces processes;
  - injects itself in processes.

- Forces autorun for removable media.
- Sets a new unauthorized home page for Internet Explorer.
- Attempts to shut down Windows OS.
- Sends SMS.
- Executes the code of detectable threats.
- Downloads detectable threats from the internet.
- Sends contacts saved on the device to a remote server.
- Sends data on incoming SMS to a remote server.
- Overlays the interface preventing access to it.
- Sets a lock screen password.
- Prompts to install a third-party application.
- Hides its icon from screen.
- Ends incoming phone calls.
- Muffles incoming phone calls.
- Intercepts incoming SMS and terminates the process of their transmission to handlers of other apps.
- Deactivates a device administrator.
- Removes user data.
- Threat detection based on machine learning.
- Contains typical banking trojan/virus code.
- Contains typical locker code.
- Loads the listed detectable threats to be executed.
- Downloads the listed detectable threats from the internet.
- Launches a large number of processes.

File system changes

- Creates the listed files.
- Appends the “hidden” attribute to the listed files.
- Deletes the listed files.
- Sets a written file as executable.
- Sets a file as executable.
- Deletes a file.
- Deletes a system binary file.
- Creates or modifies symbolic links.
- Writes to system directory:
    - files;

  - symbolic links.
- Writes to system subdirectory:
  - files;
  - symbolic links.
- Writes to temporary directory:
  - files;
  - symbolic links.
- Creates directories:
  - in system subdirectory;
  - in system directory;
  - in temporary subdirectory;
  - in temporary directory;
  - in other directories.
- Removes directories:
  - in system directory;
  - in system subdirectory;
  - in temporary subdirectory;
  - in other directories.
- Moves the listed system files.
- Moves the listed files.
- Replaces the listed executable files.
- Modifies the HOSTS file.
- Replaces the HOSTS file.
- Moves itself.
- Deletes itself.
- Creates files.
- Changes access rights:
  - for a file;
  - for a written file.
- Changes owner:
  - for a file;
  - for a written file.
- Locks files.
- Changes the time when the file was created, accessed, or modified.
- Mounts file systems.

- Unmounts file systems.
- Creates files and demands payment for file decoding (Trojan.Encoder).
- Changes a large amount of user data (Trojan.Encoder).
- Changes file extensions in user data (Trojan.Encoder).
- Sets permissions to execute files.
- Adds an exclusion to Microsoft Defender.

Network activity

- Connects to a network resource.
- Opens a port.
- Sends data to a server.
- Receives data from a server.
- Accesses SSH.
- Connects to server through:
  - HTTP;
  - IRC.
- TCP:
  - HTTP GET requests;
  - HTTP POST requests;
  - HTTP HEAD requests;
  - HTTP PATCH requests;
  - HTTP PUT requests;
  - HTTP DELETE requests;
  - HTTP OPTIONS requests;
  - HTTP TRACE requests;
  - unknown HTTP requests.
- UDP:
  - DNS requests.

Miscellaneous

- Adds a root certificate.
- Disables certificate.
- Collects information:
  - on the OS;
  - on the CPU;
  - on the RAM;
  - on the network activity.

- Changes value of the AutoConfigURL parameter as follows.
- Substitutes an application name.
- Searches for the listed windows.
- Creates and executes files.
- File protected with the Themida packer by Oreans Technologies.
- Uses NTFS alternate data streams.
- Loads the listed drivers.
- Unloads the kernel module.
- Sets kernel module to autorun.
- Executes shell scripts.
- Runs as daemon.
- Compiles source code.
- Reads information from /proc/kallsyms.
- Loads dynamic libraries.
- Makes phone calls.
- Uses data encryption algorithms.
- Uses data decryption algorithms.
- Uses elevated privileges.
- Uses administrator rights.
- Gains root access.
- Accesses the ITelephony private interface.
- Uses libraries to hide executable bytecode.
- Can send SMS automatically.
- Accesses audio/video recording interfaces.
- Records audio/video.
- Accesses camera interface.
- Changes volume and vibration settings.
- Accesses location of the device.
- Accesses network information.
- Gets information about the device (phone number, IMEI, etc.).
- Gets information about APN settings.
- Gets information about active device administrators.
- Gets information about installed apps.
- Gets information about running apps.
- Gets information about accounts linked with the device.

- Adds tasks to the System Scheduler.
- Displays its windows over windows of other apps.
- Processes information from SMS.
- Gets information about incoming/outgoing phone calls.
- Gets information about sent/received SMS.
- Gets information about phone contacts.
- Enables/disables all cameras.
- Manages Wi-Fi connectivity.
- Checks for anti-virus applications.
- Intercepts notifications.
- Requests permission to display system alert windows.
- Sample from Google Play Store.
- Restarts the analyzed sample.

10.4.2.5. Files and Dumps

The section contains two tables: **Created files** and **Dumps**. The number of objects detected during the analysis is displayed to the right from the table name.

To open a table, click its name.

To sort table columns in ascending or descending order, click the column titles.

To download a file from the table, click **Download the file** ⤓. If Dr.Web vxCube has not collected the file due to resource constraints, you are not able to download the file. In this case the ⊘ icon is displayed.

Created files

The table contains information about files created during the analysis. The table displays a path, hash, and name of a detected threat.

Dumps

The table contains information about the following objects:

- Dumps.
- Injections.
- Memory blocks that are allocated by the running sample. Memory allocations may contain traces of malicious activity.

The table displays a file name, hash, unique number of a process (PID), and name of the detected threat.

> ⚠ The name of the detected threat is displayed only if it is in the Dr.Web database.

10.4.2.6. Phone Calls and SMS (optional)

> ⚠ The section appears in reports for Android packages only.

The section contains information about outgoing phone calls and SMS messages, that have been made by the analyzed application. The table contains receivers' phone numbers and message texts.

10.4.2.7. API Log and Intents

The section contains two tables: **API log** and **Intents**.

> ⚠ The **Intents** table appears in reports for Android packages only.

The number of objects detected during the analysis is displayed to the right from the table name.

To open a table, click its name.

To sort table columns in ascending or descending order, click the column titles.

To filter the data by maliciousness, click one of the colors in the ■ ■ ■ ■ ■ scale. The filter includes the upper level of maliciousness into the previous one.

API Log

The **API log** table contains information about all events that occurred on the virtual machine while the file was running. The **API log** table contains structured data from the Process graph section.

Click **Open API Log in a New Tab** to open this section in a new browser tab.

Parameter	Comment
Time	Time of the process. Counted from the moment the file analysis started.
Process	The full path to the process in the host operating system.
Event	An event which occurs while the file is running. It corresponds to the commonly used API functions.
Arguments	Arguments of the events. They indicate special conditions for executing events.

Intents

The **Intents** table contains the intents that were sent by the analyzed application to start components of other applications.

Parameter	Comment
Time	Time of the action. Counted from the moment the file analysis started.
Data	Data to perform the action upon.
Action	Name of action to perform.
Transaction	Transaction defining a type of component to start: • START_ACTIVITY—starting an activity. • START_SERVICE—starting a service. • BROADCAST_INTENT—delivering a broadcast.
Component name	Component that receives the intent.

10.4.2.8. Network Activity Map

The section contains information about data that was sent by a file and where it was transferred. The connections are marked on an interactive map. For more information on each connection, refer to the table below the map.

Parameter	Description
Protocol	Protocol that is used for the connection.
Address	Address for connection.
Application-level data	DNS request, URL request, or unknown data.

You can sort the **Protocol** and **Address** columns in ascending or descending order. To do this, click the header of the column you want to sort by. At the left of the header ▲ or ▼ will appear. To change the sorting direction, click the header again.

> ⚠ By default, the map will only show connections that are initiated by the sample itself. To include connections initiated by you through the VNC client, select the **Monitor all processes if VNC is used** check box in the additional settings before starting the analysis.

10.5. History

History contains information about file analyses that have been performed before. The history section is located on the Dr.Web vxCube main page below the file uploading section.

History allows you to:

- Search for a string, filter and sort entries.
- Check the progress of the ongoing analysis.
- View, delete, and download reports of analyzed files.

History management

To set a number of entries displayed on one page

- Click the drop-down menu below the table.

To sort entries

- Click the corresponding column title.

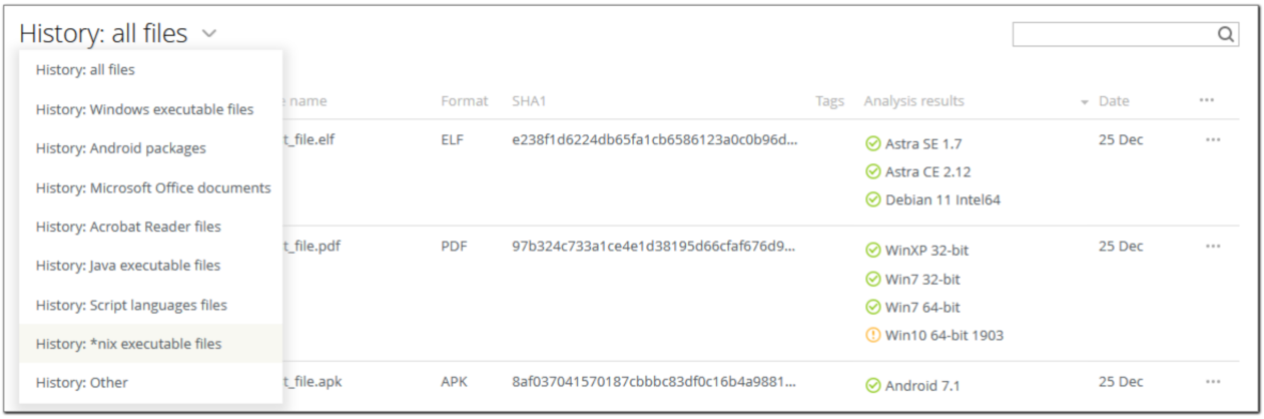
  You can sort entries by user login, file name, or date.

To filter entries

- Type a string into the search box. You can search across all table columns.
- Click **History** to filter by file type.

To select which columns to display

- Click ··· in the right corner of the table.
- Select the columns you want to display.



History: all files

- History: all files
- History: Windows executable files
- History: Android packages
- History: Microsoft Office documents
- History: Acrobat Reader files
- History: Java executable files
- History: Script languages files
- History: *nix executable files
- History: Other

name	Format	SHA1	Tags	Analysis results	Date	···
t_file.elf	ELF	e238f1d6224db65fa1cb6586123a0c0b96d...		✓ Astra SE 1.7 ✓ Astra CE 2.12 ✓ Debian 11 Intel64	25 Dec	···
t_file.pdf	PDF	97b324c733a1ce4e1d38195d66cfaf676d9...		✓ WinXP 32-bit ✓ Win7 32-bit ✓ Win7 64-bit ! Win10 64-bit 1903	25 Dec	···
t_file.apk	APK	8af037041570187cbbbc83df0c16b4a9881...		✓ Android 7.1	25 Dec	···

Figure 17. Selecting file type

To open a page with analysis report

- Click the corresponding file name.

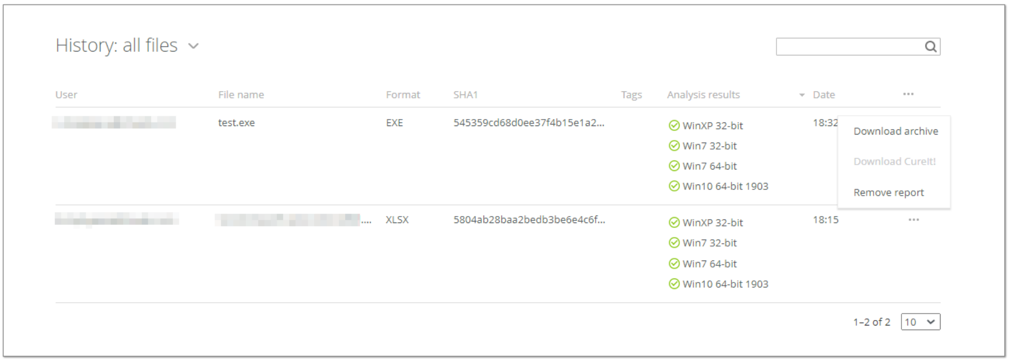
To download analysis report

- Hover over the ••• icon corresponding to the required file and select **Download archive**.

  The detailed report will be downloaded as a ZIP archive.

To remove analysis report

- Hover over the ••• icon corresponding to the required file and select **Remove report**.



History: all files

User	File name	Format	SHA1	Tags	Analysis results	Date	···
[redacted]	test.exe	EXE	545359cd68d0ee37f4b15e1a2...		✓ WinXP 32-bit ✓ Win7 32-bit ✓ Win7 64-bit ✓ Win10 64-bit 1903	18:32	
[redacted]	[redacted]....	XLSX	5804ab28baa2bedb3be6e4c6f...		✓ WinXP 32-bit ✓ Win7 32-bit ✓ Win7 64-bit ✓ Win10 64-bit 1903	18:15	···

Figure 18. Actions available in the History section

10.6. Tags

To make it easier to work with reports, use special classification labels, *tags*. You can add tags in two ways:

- When adding a YARA rule. Then, if this particular rule is triggered during the analysis, the report will automatically have the specified tags added to it.
- Manually added to the generated report. To do this:

  1. Click ⊕ in the **Tag** section of the report.

2. Enter a tag name using letters, digits, or underscore.

3. Click +.

11. API

Dr.Web vxCube API allows you to:

- Automatically analyze files
- Analyze more files in less time
- Automatically sort results

We recommend you to use our Dr.Web vxCube API Client as it simplifies the interaction with vxCube. With this API client, you won't need to generate queries manually for actions like sending samples for analysis, receiving the analysis results, or downloading reports.

Currently, Dr.Web vxCube API v2.0 is used. This version only supports the JSON format. Use the following base URL address for all your API requests:

```
https://<IP address/domain name of the server>/api-2.0/
```

11.1. Authentication

Every API request to Dr.Web vxCube service should be authenticated using an API key. The key serves as a user ID or access key to the service, much like a login and password on a web interface. To authenticate, add an `Authorization` header with an API key to your API request.

Example request

```
curl -X GET https://<IP address/domain name of the server>/api-2.0/analyses/60e21c98-
7c2a-4112-81b5-a577f6cdf4db \
-H "Content-Type: application/json" \
-H "Authorization: api-key aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee"
```

You can create an API key on the service's web interface or by sending an API request.

11.2. Managing API Keys

You can create new API keys, view, or delete existing ones.

At most, you can have 10 API keys. If you have reached the limit, but want to add another key, start by deleting one or more existing keys.

To create an API key on the service's web interface

1. In the top right-hand corner of the main page, click 👤 **Profile > Settings**.
2. On the left, select the **API sessions** tab.

3. In the **New key** field, enter the key name, then click + . The key appears in the **Existing keys** list.
4. If you want to copy the newly created key, click ⧉ on the right of it.

To create an API key by sending an API request

- Send the POST login request.

To view your existing API keys

1. In the top right-hand corner of the main page, click 👤 **Profile** > **Settings**.
2. On the left, select the **API sessions** tab.
3. You can find the API keys you have in the **Existing keys** list.

> ⚠ If you've already had an API key, you can retrieve this by sending the API request POST login.

To delete an API key

1. In the top right-hand corner of the main page, click 👤 **Profile** > **Settings**.
2. On the left, select the **API sessions** tab.
3. In the **Existing keys** list, click 🗑 on the right of the key.

> ⚠ You can undo the deletion of the API key. To do this, click **Restore** on the right of API key deletion info. But if you close the **Settings** window, the **Restore** button will disappear and the API key will be permanently deleted.

11.3. Endpoints

11.3.1. analyses

Use the endpoint to manage analyses.

DELETE analyses/<analysis_id:uuid>

Description	**Parameters**	**Result**
Delete analysis.	—	Analysis is deleted, code 204.

GET analyses

Description	Result
Get data about analyses.	List of Analysis objects.

Parameters

Parameter	Type	Description	Required
`count`	integer	Number of returning objects, 1...100. To get more objects, use several requests and the `offset` parameter. By default, `count=10`.	No
`offset`	integer	Offset, 0...+∞. By default, `offset=0`.	No
`format_group_name`	string	Filter by file type.	No

GET analyses/<analysis_id:uuid>

Description	Parameters	Result
Get detailed information about analysis.	—	Analysis object.

Usage example

GET analyses/<analysis_id:uuid>/archive

Description	Parameters	Result
Download the archive with analysis results.	—	Archive that contains analysis results on all tasks.

Usage example

GET analyses/<analysis_id:uuid>/sample

Description	Parameters	Result
Download sample.	—	Sample.

POST analyses

Description	Result
Start the file analysis.	Analysis object.

Parameters

Parameter	Type	Description	Required
`analysis_time`	integer	Sample run time in seconds, from 30 to 300. By default, `analysis_time=60`.	No
`convert_video`	boolean	Convert video while the analysis is ongoing.	No
`copylog`	boolean	Copy full raw hypervisor log.	No
`crypto_api_limit`	integer	Crypto API buffers limit in MB.	No
`custom_cmd`	string/null	Command to run the sample.	No
`drop_size_limit`	integer	Total size limit for created files.	No
`dump_browsers`	string	Dump browser modules.	No
`dump_mapped`	boolean	Dump memory-mapped files (only after execution).	No
`dump_processes`	boolean	Dump processes (only after execution).	No
`dump_size_limit`	integer	Maximum size of collectable drops.	No
`dump_ssdt`	boolean	Dump SSDT.	No
`flex_time`	boolean	Sample flex time.	No
`format_name`	string	File format.	Yes if the format is not identified automatically
`forwards`	array [string]/null	Forward the specified ports from guest VM.	No
`generate_cureit`	boolean	Generate the Dr.Web CureIt! utility for neutralizing threats in the original file and in all files created during the analysis.	No

Parameter	Type	Description	Required
get_lib	boolean	Get *.lib files and raw dumps.	No
injects_limit	integer	Injects count limit.	No
monkey_clicker	boolean	Enable auto clicker.	No
net	string	Command to redirect virtual machine network traffic according to specified settings. • VPN = vpn:// (used by default if the net parameter is not specified) • TOR = tor:// • Socks4 = socks4://host:port • Socks5 = socks5://[login:password@]host:port?parameters • Shadowsocks = shadowsocks://[login:password@]host:port?parameters Possible values for parameters: udp—UDP protocol behavior (udp=on redirects all UDP traffic, udp=off does not redirect traffic); login:password—proxy server authorization parameters (optional for Socks5, required for Shadowsocks).	No
no_clean	boolean	Get all allocs and drops.	No
optional_count	integer/null	Maximum number of triggered breakpoints.	No
platforms	array [string]/null	Platforms to run the sample.	No
proc_lifetime	string/null	Lifetime of processes in seconds. Example: 'notepad.exe,35,winword.exe,20	No
sample_id	integer	Sample ID.	Yes
set_date	string	Set system date (format: 17.03.2022).	No
write_file_limit	integer	WriteFile buffers limit in MB.	No

Usage example

POST analyses/<analysis_id:uuid>/restart

Description	Parameters	Result
Restart all deleted or failed tasks of the specified analysis.	—	Restart of deleted or failed tasks.

11.3.2. formats

Use the endpoint to get data about supported formats.

GET formats

Description	Parameters	Result
Get a list of formats supported by Dr.Web vxCube.	—	List of Format objects.

11.3.3. login

Use the endpoint to get one of the existing API keys or to create a new one. You can have a maximum of 10 API keys.

POST login

Description	Result

Get API key.	`{`
	`  "new_key": <true or false>`
	`  "api_key": "<API key>"`
	`  "start_date": "<date>"`
	`  "name": <key name>`
	`}`

Parameters

Parameter	Type	Description	Required
`login`	string	User login.	Yes
`password`	string	User password.	Yes

Parameter	Type	Description	Required
`new_key`	boolean	Determines whether to create a new API key or to get one of the created earlier. By default `new_key=false`. If you have not got any API keys created, you do not have to specify the parameter—API key will be created anyway.	No
`name`	string	The name that will be used to describe this API key.	No

Usage example

11.3.4. platforms

Use the endpoint to get data about supported platforms.

GET platforms

Description	Parameters	Result
Get a list of supported platforms.	—	List of Platform objects.

Supported platforms

The following table lists the supported platforms for the various file formats.

File format	Supported platforms
EXE, DLL, CPL, SYS, Native App, MSI, JS, VBS, WSF, JSE, VBE, PS1, BAT, SCT, XSL, MOF, LNK, HTA, CHM, CDF, EML, ZIP, ARJ, XZ, TAR, BZ2, CAB, GZ, RAR, 7Z	winxpx86, win7x86, win7x64, win10x64_1511, win10x64_1903
ACCDB, DOC, DOCM, DOCX, DOTM, DOTX, IQY, MDB, MHT, ODP, ODS, ODT, POTM, POTX, PPA, PPAM, PPSM, PPSX, PPT, PPTM, PPTX, PUB, RTF, SLDM, SLDX, SLK, THMX, XLAM, XLL, XLS, XLSB, XLSM, XLSX, XLTM, XLTX, XML, WPS	office_xp, office_7_32, office_7_64, office_10_64_1511, office_10_64_1903
PDF	acrobat_xp_10, acrobat_7_32_11, acrobat_7_64_15, acrobat_10_64_1511_15, acrobat_10_64_1903_15
JAR, CLASS	java_xp, java_7_32, java_7_64, java_10_64_1511, java_10_64_1903

File format	Supported platforms
SH, PY, PL, EL, DOCKER	arm64_debian_bullseye, armel32_debian_jessie, armhf32_debian_bullseye, intel32_debian_bullseye, intel64_astra_ce_2.12, intel64_astra_se_1.7.2, intel64_debian_bullseye, mips32_debian_buster, mipsel32_debian_bullseye, mipsel64_debian_bullseye, ppc32_debian_jessie, ppcel64_debian_bullseye
APK	android4.3, android7.1

11.3.5. samples

Use the endpoint to manage samples.

GET samples

Description	Result
Get a list of samples that were uploaded earlier.	List of Sample objects.

Parameters

Parameter	Type	Description	Required
`count`	integer	Number of returning objects, 1...100. To get more objects, use several requests and the `offset` parameter. By default, `count=10`.	No
`offset`	integer	Offset, 0...+∞. By default, `offset=0`.	No
`md5`	string	Filter by MD5.	No
`sha1`	string	Filter by SHA1.	No
`sha256`	string	Filter by SHA256.	No
`format_name`	string	Filter by file format.	No
`format_group_name`	string	Filter by file type.	No

GET samples/<sample_id:number>

Description	Parameters	Result
Get data about the file that was uploaded earlier.	—	Sample object.

GET samples/<sample_id:number>/analyses

Description	Parameters	Result
Get data about the file analyses.	—	Analysis object.

POST samples

Description	Result
Upload a sample to the Dr.Web vxCube server.	Sample object.

Parameters

Parameter	Type	Description	Required
`file`	string	The sample that needs to be uploaded to the server. Specify a full filepath preceded by the `@` symbol.	Yes
`password`	string	The password for the uploaded archive. The password can be 1 to 25 characters long.	No

Usage example

11.3.6. sessions

Use the endpoint to manage sessions.

DELETE sessions/<api_key:string>

Description	Parameters	Result
Delete the session with the specified API key.	—	Session is deleted, code 204.

GET sessions

Description	Parameters	Result
Get a list of all open sessions.	—	List of Session objects.

11.3.7. tasks

Use the endpoint to manage analysis tasks and report data.

GET tasks/<task_id:number>

Description	Parameters	Result
Get data about the task.	—	Task object.

GET tasks/<task_id:number>/archive

Description	Parameters	Result
Download archive with analysis results.	—	Archive with analysis results.

GET tasks/<task_id:number>/sample

Description	Parameters	Result
Download sample.	—	Sample.

GET tasks/<task_id:number>/report

Description	Parameters	Result
Download one-page HTML report.	—	One-page HTML report.

GET tasks/<task_id:number>/graph

Description	Parameters	Result
Download SVG graph.	—	SVG graph.

GET tasks/<task_id:number>/dumps

Description	Result

Get data from the Dumps table.	{
	    "total_count": <*number*>,
	    "items": <*list of* Dump *objects*>
	}

Parameters

Parameter	Type	Description	Required
`count`	integer	Number of returning objects, 1...100. To get more objects, use several requests and the `offset` parameter. By default, `count=10`.	No
`offset`	integer	Offset, 0...+∞. By default, `offset=0`.	No
`search`	string	Pattern for string searching.	No

GET tasks/<task_id:number>/drops

Description	Result

Get data from the Created files table.	{
	    "total_count": <*number*>,
	    "items": <*list of* Drop *objects*>
	}

Parameters

Parameter	Type	Description	Required
`count`	integer	Number of returning objects, 1...100. To get more objects, use several requests and the `offset` parameter. By default, `count=10`.	No
`offset`	integer	Offset, 0...+∞. By default, `offset=0`.	No
`search`	string	Pattern for string searching.	No

GET tasks/<task_id:number>/networks

Description	Result

Get data from the Network activity map table.	`{`
	`"total_count":` *<number>*`,`
	`"items":` *<list of Connection objects>*
	`}`

Parameters

Parameter	Type	Description	Required
`count`	integer	Number of returning objects, 1...100. To get more objects, use several requests and the `offset` parameter. By default, `count=10`.	No
`offset`	integer	Offset, 0...+∞. By default, `offset=0`.	No

GET tasks/<task_id:number>/api_log

Description	Result

Get data from the API log table.	`{`
	`"total_count":` *<number>*`,`
	`"items":` *<list of APIEvent objects>*
	`}`

Parameters

Parameter	Type	Description	Required
`count`	integer	Number of returning objects, 1...100. To get more objects, use several requests and the `offset` parameter. By default, `count=10`.	No
`offset`	integer	Offset, 0...+∞. By default, `offset=0`.	No
`search`	string	Pattern for string searching.	No

GET tasks/<task_id:number>/intents (optional)

Description	Result

Get data from the Intents table. The endpoint is used for tasks started on Android.	{
	"total_count": *<number>*,
	"items": *<list of Intent objects>*
	}

Parameters

Parameter	Type	Description	Required
`count`	integer	Number of returning objects, 1...100. To get more objects, use several requests and the `offset` parameter. By default, `count=10`.	No
`offset`	integer	Offset, 0...+∞. By default, `offset=0`.	No
`search`	string	Pattern for string searching.	No

GET tasks/<task_id:number>/phone_actions (optional)

Description	Result

Get data from the Phone calls and SMS table. The endpoint is used for tasks started on Android.	{
	"total_count": *<number>*,
	"items": *<list of Call and Message objects>*
	}

Parameters

Parameter	Type	Description	Required
`count`	integer	Number of returning objects, 1...100. To get more objects, use several requests and the `offset` parameter. By default, `count=10`.	No
`offset`	integer	Offset, 0...+∞. By default, `offset=0`.	No
`search`	string	Pattern for string searching.	No

GET tasks/<task_id:number>/archive_storage

Description	Parameters	Result

Get a list of files and directories in the archive, or download a file or a directory from the archive.	`path` (string)—path, optional	If `path` is not specified:
		`{`
		`"folders":` *<list of folders in the archive>*`,`
		`"files":` *<list of files in the archive>*
		`}`
		If `path` is specified, file or archive of the folder

Usage example

POST tasks/<task_id:number>/restart

Description	Parameters	Result
Restart the deleted or failed task.	—	Restart of the deleted or failed task.

11.3.8. ws/progress

To connect over the WebSocket protocol and get data about the analysis progress in real time, in the request, specify the following JSON object as a string:

```
{"analysis_id": <ID>}
```

In response, you receive the JSON object:

```
{'message': '<message>', 'progress': <progress>, 'task_id': <ID>}
```

11.4. Objects

11.4.1. Analysis

The **Analysis** object contains general analysis information and a list of Task objects.

Structure

Key	Type	Description
`id`	UUID	Task UUID.
`sha1`	string	SHA1 hash.
`sample_id`	integer	Sample ID.
`size`	integer	File size in bytes.
`format_name`	string/null	File format. Matches the Sample.format_name format, if the format was not specified explicitly when starting the file analysis.
`start_date`	string (datetime.iso8601)	Date and time the analysis started.
`user_name`	string	User login.
`tasks`	array [Task]	List of tasks. Corresponds to the selected platforms.

Examples

If you request a certain analysis by its ID, in response, you receive the **Analysis** object where the `tasks` key is a list of TaskFinished or TaskProcessing objects:

```
{
  "id": 1629b17b-fd44-46e6-97a2-1310c1f050a4,
  "sample_id": 6248,
  "size": 3242863,
  "sha1": "8c81eb1b6a87e30656d479968eca969bc59bdeb3",
  "start_date": "2018-12-12T11:29:44.645968+00:00",
  "user_name": "name_example",
  "format_name": "rtf",
  "tasks": [
    {
      "end_date": "2018-12-12T11:33:37.490050+00:00",
      "platform_code": "winxpx86",
      "maliciousness": 100,
      "id": 16916,
      "status": "successful",
      "start_date": "2018-12-12T11:29:44.645968+00:00",
      "rules": {
        "neutral": [
          "Searching for the window",
          "Creating a window",
          "DNS request",
          "Sending an HTTP GET request"
        "suspicious": [
          "Connection attempt by exploiting the app vulnerability"
        ]
      },
      "detects": [
        "behavior",
        "files_dumps"
        ],
      "verdict": "malware2"
    },
    {
      "end_date": "2018-12-12T11:33:47.716867+00:00",
      "platform_code": "win7x86",
      "maliciousness": 100,
      "id": 16917,
      "status": "successful",
      "start_date": "2018-12-12T11:29:44.645968+00:00",
      "rules": {
        "neutral": [
          "Creating a window",
          "DNS request",
          "Sending an HTTP GET request",
          "Creating a process from a recently created file",
          "Launching a process"
        ],
        "suspicious": [
          "Connection attempt by exploiting the app vulnerability"
        ]
      },
      "detects": [
        "behavior",
        "files_dumps"
        ],
      "verdict": "malware2"
    },
    {
      "end_date": "2018-12-12T11:34:08.229276+00:00",
      "platform_code": "win7x64",
      "maliciousness": 100,
      "id": 16918,
      "status": "successful",
      "start_date": "2018-12-12T11:29:44.645968+00:00",
      "rules": {
        "neutral": [
          "Creating a window",
          "DNS request",
          "Sending an HTTP GET request",
          "Creating a file in the %temp% directory",
          "Launching a process",
          "Launching the default Windows debugger (dwwin.exe)"
        ],
        "suspicious": [
          "Connection attempt by exploiting the app vulnerability"
        ]
      },
      "detects": [
        "behavior",
        "files_dumps"
        ],
      "verdict": "malware2"
    },
    {
      "end_date": "2018-12-12T11:35:11.553665+00:00",
      "platform_code": "win10x64_1903",
      "maliciousness": 100,
      "id": 16919,
      "status": "successful",
      "start_date": "2018-12-12T11:29:44.645968+00:00",
      "rules": {
        "neutral": [
          "Creating a window",
          "Sending an HTTP GET request"
        ],
        "suspicious": [
          "Connection attempt by exploiting the app vulnerability"
        ]
      },
      "detects": [
        "behavior",
        "files_dumps"
        ],
      "verdict": "malware2"
    }
  ]
}
```

If you request a list of analyses using the GET analyses method, in response, you receive a list of **Analysis** objects, each contains the `tasks` key—a list of TaskBasic objects:

```
{
    "id": 1629b17b-fd44-46e6-97a2-1310c1f050a4,
    "sample_id": 6248,
    "size": 3242863,
    "sha1": "8c81eb1b6a87e32152d439965eca944bc59bdeb3",
    "start_date": "2018-12-12T11:29:44.645968+00:00",
    "user_name": "name_example",
    "format_name": "rtf",
    "tasks": [
      {
        "end_date": "2018-12-12T11:33:37.490050+00:00",
        "platform_code": "winxpx86",
        "maliciousness": 100,
        "id": 16916,
        "status": "successful",
        "start_date": "2018-12-12T11:29:44.645968+00:00"
      },
      {
        "end_date": "2018-12-12T11:33:47.716867+00:00",
        "platform_code": "win7x86",
        "maliciousness": 100,
        "id": 16917,
        "status": "successful",
        "start_date": "2018-12-12T11:29:44.645968+00:00"
      },
      {
        "end_date": "2018-12-12T11:34:08.229276+00:00",
        "platform_code": "win7x64",
        "maliciousness": 100,
        "id": 16918,
        "status": "successful",
        "start_date": "2018-12-12T11:29:44.645968+00:00"
      },
      {
        "end_date": "2018-12-12T11:35:11.553665+00:00",
        "platform_code": "win10x64_1903",
        "maliciousness": 100,
        "id": 16919,
        "status": "successful",
        "start_date": "2018-12-12T11:29:44.645968+00:00"
      }
    ]
  }
```

11.4.2. APIEvent

The **APIEvent** object contains data about an event that occurred while the sample was running.

Structure

Key	Type	Description
`process`	string	The full path to the process in the host operating system.
`rules`	object	List of triggered rules.
`arguments`	string	Arguments of the event. They indicate special conditions for executing events.
`maliciousness`	integer	Maliciousness, from 0 to 100.
`event`	string	An event which occurs while the file is running. It corresponds to the commonly used API functions.
`timestamp`	integer	Event timestamp. Counted from the moment the file analysis started.

Example

```
{
  "process": "<CURRENT_DIR>\\example.exe:1432:2432",
  "rules": {
    "neutral": [
      "Connection attempt"
    ]
  },
  "arguments": "To '125.251.199.120':540",
  "maliciousness": 0,
  "event": "ConnectNet",
  "timestamp": 9
}
```

11.4.3. Call (optional)

The **Call** object contains data about an outgoing phone call. The object is used only in results of Android app analysis.

Structure

Key	Type	Description
`type`	string	Always `call`.
`number`	string	Phone number the call was made to.

Example

```
{
  "type": "call",
  "number": "667206"
}
```

11.4.4. Connection

The **Connection** object contains data about a network connection.

Structure

Key	Type	Description
`port`	integer	Port number.
`host`	string	Host name or IP address.
`country`	object	Country.
`app`	string	Application-level data.
`protocol`	string	Protocol that is used for the connection.
`ip`	string	Host IP address.

Example

```
{
  "port": 31,
  "host": "<IP address>",
  "country": {
    "name": "China",
    "code3": "CHN"
  },
  "app": "{70,69,6e,67}",
  "protocol": "TCP/IP",
  "ip": "<IP address>"
}
```

11.4.5. Dump

The **Dump** object contains data about a potentially malicious dump of a process.

Structure

Key	Type	Description
`archive_path`	string	Path to the file in the report archive.
`name`	string	File name.
`sha1`	string	SHA1 hash.
`detect`	string	Threat name.
`pid`	integer	Process identifier.

Example

```
{
  "archive_path": "dumps/4_89432000_a71a8d8316cb3bc.4.38.6.ndmp",
  "name": "a71a8d8316cb3bc",
  "sha1": "8f11bc1fb9ac4444472213e0ae91bc166493f0ab",
  "detect": "Trojan.Necurs.5",
  "pid": 4
}
```

11.4.6. Drop

The **Drop** object contains data about a file created during the analysis.

Structure

Key	Type	Description
`archive_path`	string	Path to the file in the report archive.
`sha1`	string	SHA1 hash.
`detect`	string	Threat name.
`path`	string	Path to the created file.

Example

```
{
  "archive_path": "drops/d##vault.hta(0)",
  "sha1": "392b84af9ede8fc70a29f02131e9ae91ef88c809",
  "detect": "JS.DownLoader.994",
  "path": "D:\\vault.hta"
}
```

11.4.7. Format

The **Format** object contains data about a file format.

Structure

Key	Type	Description
`name`	string	The name of the file format.
`group_name`	string	The name of the file type. Possible values: • `apk`: Android packages. • `arf`: Acrobat Reader files. • `ja`: Java executable files. • `js`: script files. • `moc`: Microsoft Office documents. • `other`: other types. • `uef`: *nix executable files. • `wef`: Windows executable files.
`platforms`	array [Platform.code]	The list of platforms.

Example

```
{
   "name": "exe",
   "group_name": "wef",
   "platforms": [
     "winxpx86",
     "win7x86",
     "win7x64",
     "win10x64_1903"
   ]
}
```

11.4.8. Intent (optional)

The **Intent** object contains data about an intent. The object is used only in results of Android app analysis.

Structure

Key	Type	Description
`cn`	string	Component that receives the intent.
`action`	string	Name of action to perform.
`data`	string	Data to perform the action upon.
`transaction`	string	Transaction defining a type of component to start: • START_ACTIVITY—starting an activity. • START_SERVICE—starting a service. • BROADCAST_INTENT—delivering a broadcast.
`maliciousness`	integer	Maliciousness, from 0 to 100.
`rules`	object	List of triggered rules.
`timestamp`	integer	Timestamp. Counted from the moment the file analysis started.

Example

```
{
  "cn": null,
  "action": "android.app.action.ADD_DEVICE_ADMIN",
  "data": null,
  "transaction": "START_ACTIVITY",
  "maliciousness": 69,
  "rules": {
    "suspicious": [
      "Using device administration features"
    ]
  },
  "timestamp": 0
}
```

11.4.9. Message (optional)

The **Message** object contains data about an outgoing SMS message. The object is only used in the results of Android app analysis.

Structure

Key	Type	Description
type	string	Always message
number	string	Phone number the message was sent to.
text	string	Text of the message.

Example

```
{
  "type": "message",
  "number": "000",
  "text": "Balance"
}
```

11.4.10. Platform

The **Platform** object contains data about an OS platform and, in some cases, about an application for running the sample.

Structure

Key	Type	Description
code	string	Short name of the platform.
name	string	App name or OS platform.
os_code	string	OS platform.

Example

```
{
    "code": "office_7_32",
    "name": "Microsoft Office 2010",
    "os_code": "Windows 7 32-bit"
}
```

11.4.11. Sample

The **Sample** object contains data about an original file uploaded for analysis.

Structure

Key	Type	Description
`id`	integer	Sample ID.
`name`	string	File name.
`format_name`	string	File format. It is identified by Dr.Web vxCube automatically. File format determines the command for file running if the command is not specified explicitly when starting the file analysis.
`is_x64`	boolean	Determines the bitness of the platform for file running. It is `null` if the file is not executable.
`md5`	string	MD5 hash.
`sha1`	string	SHA1 hash.
`sha256`	string	SHA256 hash.
`size`	integer	File size in bytes.
`upload_date`	string	Date and time the file was uploaded.
`platforms`	array [Platform.code]	List of supported platforms for file running.

Example

```
{
  "id": 42,
  "name": "sample.exe",
  "format_name": "sys",
  "is_x64": null,
  "md5": "a0b0f87193b79ac1db32f251f2f5e5b2",
  "sha1": "e54639e9d81680d0acc154d42ae7350ed481b848",
  "sha256": "51133e7e4d52b94e3360ac1866b76bf2b2bca056492bcf93de3c37d6b0c07104",
  "size": 1897856,
  "upload_date": "2018-07-31T11:42:36.873274+00:00"
  "platforms": [
    "winxpx86",
    "win7x86",
    "win7x64",
    "win10x64_1903"
  ]
}
```

11.4.12. Session

The **Session** object contains data about a session.

Structure

Key	Type	Description
`api_key`	string	API key.
`start_date`	string	Date and time the session was started.

Example

```
{
    "api_key": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
    "start_date": "2018-12-20T08:55:35.158344+00:00"
}
```

11.4.13. Task

The **Task** object contains data about a task. **Task** is a file analysis on a single platform. Task can contain a various set of keys: **TaskBasic**, **TaskFinished**, or **TaskProcessing**.

TaskBasic

The **TaskBasic** object contains general information about a task. Such an object with the basic set of keys is used in a list of Analysis objects.

Structure

Key	Type	Description
`id`	integer	Task ID.
`status`	string	Task status. Available values: `in queue`, `failed`, `processing`, `deleted`, `successful`.
`platform_code`	string	Platform.code.
`start_date`	string (datetime.iso8601)	Date and time the task was started.
`end_date`	string/null (datetime.iso8601)	Date and time the task was completed.
`maliciousness`	integer/null	Maliciousness, from 0 to 100.

Example

```
{
    "id": 20,
    "status": "failed",
    "platform_code": "winxpx86",
    "start_date": "2018-07-30T16:54:07.156371",
    "end_date": "2018-07-30T16:55:07.156371",
    "maliciousness": null
}
```

TaskFinished

The **TaskFinished** object contains the keys of the **TaskBasic** object and analysis results for the specified platform.

Structure

Key		Type	Description
`detects`		string[]	A list of detected threats. The list can include the following strings: `yara`: a YARA rule has triggered; `behavior`: malicious or suspicious behavior for a file has been detected; `files_dumps`: the threats have been detected in created files or/and memory dumps.
`end_date`		string/null (datetime.iso8601)	Date and time the task was completed.
`id`		integer	Task ID.
`maliciousness`		integer/null	Maliciousness, from 0 to 100.
`platform_code`		string	Platform.code.
`rules`		object/null	List of triggered rules.
	`malicious`	string[]	List of rules that have been triggered due to malicious activity of the sample.
	`neutral`	string[]	List of rules that have been triggered due to neutral activity of the sample.
	`suspicious`	string[]	List of rules that have been triggered due to suspicious activity of the sample.
`sample_detect`		string/null	Name of the threat detected using signature databases.

Key		Type	Description
start_date		string (datetime.iso8601)	Date and time the task was started.
status		string	The current status of the task. Available values: in queue, failed, processing, deleted, successful.
tags		string[]	The list of tags retrieved from the triggered YARA rules.
verdict		string	Overall result of the file maliciousness corresponding to one of three categories. The higher number corresponds to the higher level of the maliciousness probability. Available values: none, clean1, clean2, suspicious1, suspicious2, malware1, malware2.
yara_rules		object[]	List of triggered YARA rules.
	name	string	The name of the YARA rule
	rule_type	string	The type of the YARA rule. Available values: user (a user-defined rule) and system (a system-defined rule).
	severity	string	The file behavior category. When adding a YARA rule, you should specify the behavior category that will be assigned to the sample if the YARA rule is triggered. The specified category appears in the severity field. Available values: neutral, suspicious, malware. More about adding a YARA rule...

Example

```
{
  "id": 16916,
  "status": "successful",
  "maliciousness": 100,
  "platform_code": "winxpx86",
  "start_date": "2018-12-12T11:29:44.645968+00:00",
  "end_date": "2018-12-12T11:33:37.490050+00:00",
  "verdict": "malware2",
  "rules": null,
  "detects": [
     "files_dumps"
   ],
  "platform_code": "win7x64"
}
```

TaskProcessing

TaskFinished contains the keys of the **TaskBasic** object and data about the analysis process.

Structure

Key	Type	Description
`end_date`	string	Date and time the task was completed.
`id`	integer	Task ID.
`maliciousness`	integer/null	Maliciousness, from 0 to 100.
`message`	string/null	Message about the task progress.
`platform_code`	string	Platform.code.
`progress`	integer	Task progress, in percent.
`start_date`	string (datetime.iso8601)	Date and time the task was started.
`status`	string	The current status of the task. Available values: `in queue`, `failed`, `processing`, `deleted`, `successful`.

Example

```
{
  "id": 18656,
  "status": "processing",
  "maliciousness": null,
  "platform_code": "win7x86",
  "start_date": "2019-02-07T09:39:11.517117+00:00",
  "end_date": null,
  "message": "Waiting while the file is running (60 sec)…",
  "progress": 19
}
```

11.5. Examples

This section provides examples of how to work with Dr.Web vxCube using an API.

You will learn how to:

- Get an API key
- Upload a sample to the Dr.Web vxCube server
- Start the analysis
- Get information about the analysis

- Download the report

11.5.1. Get an API Key

To get an API key, send the POST login request with the login and password:

Get API key created earlier

To get one of the created API keys, specify the parameter value `new_key: false` or just do not specify the parameter:

```
curl -X POST https://<IP address/domain name of the server>/api-2.0/login \
-H "Content-Type: application/json" \
-d "{\"login\":\"example@drweb.com\", \"password\":\"secret_password\"}"
```

You receive a response with the API key (the API key is required to be specified in the header of each subsequent request):

```
{
    "new_key": false,
    "api_key": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
    "start_date": "2019-02-08T04:08:15.162342+00:00"
}
```

Create API key

To create a new API key, specify the parameter value `new_key: true` (if you have not got any API keys created, you do not have to specify the parameter—API key will be created anyway):

```
curl -X POST https://<IP address/domain name of the server>/api-2.0/login \
-H "Content-Type: application/json" \
-d "{\"login\":\"example@drweb.com\", \"password\":\"secret_password\", \"new_key\":
true, \"name\":\"example_name_api\"}"
```

You receive a response with the API key (the API key is required to be specified in the header of each subsequent request):

```
{
   "new_key": true,
   "api_key": "bbbbbbbb-cccc-dddd-eeee-ffffffffffff",
   "start_date": "2019-03-08T04:08:15.162342+00:00",
   "name": "example_name_api"
}
```

11.5.2. Upload a Sample to the Dr.Web vxCube Server

To upload a sample to the server, send the POST samples request:

```
curl -X POST https://<IP address/domain name of the server>/api-2.0/samples \
-F "file=@testfile.pdf" \
-F "password="vxcube"" \
-H "Authorization: api-key aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee"
```

In response, you receive the Sample object that contains data about the uploaded file including the file format identified automatically and a list of supported platforms. Use the received data for the further file analysis.

Response:

```
{
    "id": 6784,
    "size": 10881846,
    "name": "testfile.pdf",
    "is_x64": null,
    "format_name": "pdf",
    "upload_date": "2019-02-08T04:08:15.162343+00:00",
    "md5": "34fb8ae3c01653985085ee7e2f749ea5",
    "sha1": "00a610100a3516f4d0daa33e7de317d2ddb6c2c6",
    "sha256": "11bd131be00cbe1c43b4444ec4300dc7651805ea36393b1cca1675983dc275bc",
    "platforms": [
        "acrobat_xp_10",
        "acrobat_7_32_11",
        "acrobat_7_64_15",
        "acrobat_10_64_15"
    ]
}
```

11.5.3. Start the Analysis

To start the analysis of a sample, send the POST analyses request:

```
curl -X POST https://<IP address/domain name of the server>/api-2.0/analyses \
-H "Content-Type: application/json" \
-H "Authorization: api-key aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee" \
-d "{\"sample_id\":\"6784\", \"platforms\":[\"acrobat_7_32_11\", \"acrobat_7_64_15\"]}"
```

In the request, the uploaded file ID and the list of platforms are specified. The values are taken from the response for the previous request.

To start the analysis of a sample using network traffic redirection, send the POST analyses request:

```
curl -X POST https://<IP address/domain name of the server>/api-2.0/analyses \
-H "Content-Type: application/json" \
-H "Authorization: api-key aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee" \
-d "{\"sample_id\":\"6784\", \"platforms\":[\"acrobat_7_32_11\", \"acrobat_7_64_15\",
\"net\": \"socks5://username:password@<proxyaddress>:1080?udp=on\"}"]}"
```

In response, you receive the Analysis object that contains general analysis information:

```
{
    "id": 6260,
    "sample_id": 6784,
    "size": 10881846,
    "sha1": "00a610100a3516f4d0daa33e7de317d2ddb6c2c6",
    "start_date": "2019-02-08T04:08:15.162343+00:00",
    "format_name": "pdf",
    "user_name": "example@drweb.com",
    "tasks": [{
        "message": null,
        "end_date": null,
        "platform_code": "acrobat_7_64_15",
        "maliciousness": null,
        "progress": 0,
        "id": 18676,
        "status": "in queue",
        "start_date": "2019-02-08T04:08:15.643122+00:00"
    }, {
        "message": null,
        "end_date": null,
        "platform_code": "acrobat_7_32_11",
        "maliciousness": null,
        "progress": 0,
        "id": 18675,
        "status": "in queue",
        "start_date": "2019-02-08T04:08:15.632924+00:00"
    }]
}
```

11.5.4. Get Information About the Analysis

To get detailed information about analysis, wait for the analysis to finish, and then send the GET analyses/<analysis_id:uuid> request. In the request, specify the analysis ID:

```
curl -X GET https://<IP address/domain name of the server>/api-2.0/analyses/60e21c98-
7c2a-4112-81b5-a577f6cdf4db \
-H "Content-Type: application/json" \
-H "Authorization: api-key aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee"
```

In response, you receive the Analysis object:

```
{
    "id": "111ba12c5-d330-40eb-b988-fa16402ee111",
    "sha1": "9e92e9408afdf75fc3dea5e457cb0c70728f74ce",
    "sample_id": 77236,
    "size": 156160,
    "format_name": "dll",
    "start_date": "2024-02-13T14:28:08.871359",
    "user_name": "test@test.com",
    "tasks": [
        {
            "id": 235182,
            "status": "successful",
            "platform_code": "win10x64_2004",
            "start_date": "2024-02-13T14:28:09.135345",
            "end_date": "2024-02-13T14:30:46.776797",
            "maliciousness": 94,
            "verdict": "malware2",
            "detects": [
                "yara"
            ],
            "sample_detect": null,
            "rules": {
                "neutral": [
                    "Creating synchronization primitives",
                    "Searching for synchronization primitives"
                ]
            },
            "yara_rules": [
                {
                    "name": "gozi3",
                    "severity": "malware",
                    "rule_type": "system"
                },
                {
                    "name": "gozi",
                    "severity": "malware",
                    "rule_type": "system"
                }
            ],
            "tags": [
                "GOZI3",
                "GOZI"
            ]
        }
    ]
}
```

11.5.5. Download a Report

To download an archived analysis report, send the GET analyses/<analysis_id:uuid>/archive:

```
curl -X GET https://<IP address/domain name of the server>/api-2.0/analyses/40e2fc98-
1c2a-4112-81b5-a57df2cd22db/archive \
-H "Content-Type: application/json" \
-H "Authorization: api-key aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee" \
-o <output_archive>
```

To download one of the report files, send the GET tasks/<task_id:number>/archive_storage request. A request example for downloading the PCAP file:

```
curl -X GET https://<IP address/domain name of the server>/api-
2.0/tasks/18681/archive_storage \
-H "Content-Type: application/json" \
-H "Authorization: api-key aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee" \
-d "{\"path\": \"network.pcap\"}" \
-o some_file
```

12. Managing Users

To open a page with a user list

- At the top of the Dr.Web vxCube main page, click **Users**.

You can view the user accounts in a table. The following details are shown for every user:

- User login
- Account type (administrator or user)
- Status (active or blocked)
- Number of uploaded files
- Date the user was added

To set a number of entries displayed on one page

- Click the drop-down menu below the table.

To sort entries by any column

- Click the corresponding column title.

To reverse the order, click the title once again.

To filter entries

- Type a string into the search box. You can search across all table columns.

Additional options

An admin user can add, delete, edit, block, or unblock users.

To add a new user

1. On the **Users** page, select ⊕ **Add**.
2. Enter the user credentials and click **Add**.

To edit user credentials

1. In the user list, go to the right of the user, then click ··· > **Edit**.
2. Make the changes and click **Apply**.

To delete a user

1. In the user list, go to the right of the user, then click ··· > **Delete**.

2. Confirm deleting the user.

To block a user

1. In the user list, go to the right of the user, then click ••• > **Block**.
2. Confirm blocking the user.

To unblock a user

1. In the user list, go to the right of the user, then click ••• > **Unblock**.
2. Confirm unblocking the user.

13. Uninstalling Dr.Web vxCube

To remove all vxCube components from the server in case of installation errors, you can use a script. Run it on every node where you have vxCube components installed.

> If you run the uninstallation script on the host of `vxcube_web_host`, it will remove the vxcube-web database, including all previous scan results, created users, and all other data.

Uninstallation Keeping Windows VMs

To save time on re-installation, pass the `keepvm` argument when running the script. It will keep the information on all cloned virtual machines on hosts with Windows analyzers (`hyperbox_hosts`).

Then you will be able to restart the installer with the option hyperbox_hbsetup: false (the flag that indicates if VMs need to be recloned) and avoid having to clone the machines again.

Running a Script

To run a script

1. Save the contents below to the file `clean.sh`.
2. To run it, use the command `sudo bash clean.sh`.

```
clear
echo 'Warning! This uninstallation script will completely remove all data and services associated with vxCube installation, including the database, scan results, created users, integration settings, etc.'
while true; do
    read -p "Continue uninstallation? (yes/no) " yn
    case $yn in
        [Yy]* ) echo go clean; break;;
        [Nn]* ) exit;;
        * ) echo "Needs response Yes or No.";;
    esac
done

set -x
```

```
# docker services
docker container stop $(docker container ls -aq)
docker system prune -a --volumes -f
docker image prune -a -f
systemctl stop docker
rm -rf /etc/docker
apt purge -y docker-ce
apt purge -y docker.io
rm -rf /etc/systemd/system/multi-user.target.wants/containerd.service
# docker vxcube web
rm -rf /var/lib/vxcube
rm -rf /opt/vxcube
rm -rf /var/log/vxcube
userdel -f -r vxcube
# docker yara
rm -rf /etc/yara_service /var/log/yara_service
# docker drweb
rm -rf /etc/drweb-service /var/log/drweb

# vxcube-flow-api
systemctl stop vxcube-flow-api
systemctl disable vxcube-flow-api
rm -rf /var/lib/vxcube-flow-api /var/log/vxcube-flow-api /etc/vxcube-flow-api
rm -rf /etc/apt/sources.list.d/*
rm -rf /etc/systemd/system/vxcube-flow-api.service
rm -rf /etc/systemd/system/multi-user.target.wants/vxcube-flow-api.service
userdel -f -r hyperbox-api

# linuxbox
systemctl stop linuxbox-routes
systemctl stop linuxbox_rpc
systemctl disable linuxbox-routes
systemctl disable linuxbox_rpc
rm -rf /etc/systemd/system/linuxbox-routes.service
rm -rf /etc/systemd/system/linuxbox_rpc.service
/var/lib/linuxbox/routes_reset.sh
rm -rf /var/lib/linuxbox
rm -rf /var/lib/storage/linuxbox-*
rm -rf /etc/linuxbox
apt purge -y qemu*

# dimas
systemctl stop dimas_android7.1_vxcube
systemctl stop dimasnet
systemctl disable dimas_android7.1_vxcube
systemctl disable vboxapi_android
rm -rf /etc/systemd/system/dimas*.service
rm -rf /etc/systemd/system/vboxapi_android.service
rm -rf /etc/systemd/system/multi-
user.target.wants/apkrobot_*.service /etc/systemd/system/apkrobot_*.
service
userdel -f -r dimas
rm -rf /var/lib/dimas
rm -rf /var/log/dimas
rm -rf /etc/dimas

# hyperbox
systemctl stop hbcheck
systemctl stop vboxsvc
systemctl stop hyperbox_winxpx86_vxcube hyperbox_win7x64_vxcube
hyperbox_win7x86_vxcube hyperbox_win10x64_1903_vxcube
hyperbox_win10x64_1511_vxcube
systemctl disable vboxsvc hbcheck hyperbox_winxpx86_vxcube
hyperbox_win7x64_vxcube hyperbox_win7x86_vxcube
hyperbox_win10x64_1903_vxcube hyperbox_win10x64_1511_vxcube
systemctl disable vboxdrv vboxautostart-service vboxballoonctrl-
service
```

```
rm -rf /etc/systemd/system/hbcheck.service
rm -rf /etc/systemd/system/hyperbox_*.service
rm -rf /etc/systemd/system/vboxapi.service
rm -rf /etc/systemd/system/vboxnet.service
rm -rf /etc/systemd/system/vboxsvc.service
rm -
rf /etc/fakenet /etc/vbox /etc/hyperbox /var/lib/vboxnet_workspace
rm -rf /var/log/hyperbox /var/log/vbox*
if [ "$1" == "keepvm" ]; then
  # this will keep vms and configs
  apt remove -y virtualbox-hyperbox
else
  # this will delete all
  apt purge -y virtualbox-hyperbox
  userdel -f -r hyperbox
  rm -rf /var/lib/hyperbox
  rm /var/lib/storage/* -r
fi
apt purge drweb-procdump -y
apt purge aksusbd -y

# evparser
systemctl stop evparser
systemctl disable evparser
rm -rf /var/lib/evparser /var/lib/evparser/
.cache /etc/evparser /var/log/evparser
rm -rf /etc/systemd/system/evparser.service
rm -rf /etc/systemd/system/multi-user.target.wants/evparser.service
userdel -f -r evparser

# pogreb
rm -rf /etc/pogreb-client /var/log/pogreb-client

# ftp
systemctl stop proftpd
```

```
sudo apt purge -y proftpd*
rm -rf /etc/proftpd /var/log/proftpd
rm -rf /srv/vxcube

# dhcp
apt purge -y dnsmasq
apt purge -y isc-dhcp-server
# remove includes from dhcp config (they will not be deleted by dpkg)
DHCP_CONF=/etc/dhcp/dhcpd.conf
if [ -f $DHCP_CONF ] ; then
    sed -i 's#include "/etc/dhcp/dhcpd.vbox";##g' $DHCP_CONF
    sed -i 's#include "/etc/dhcp/dhcpd_android.vbox";##g' $DHCP_CONF
fi
rm /etc/dhcp/dhcpd.vbox
rm /etc/dhcp/dhcpd_android.vbox

# openvpn
systemctl stop openvpn
rm -rf /var/log/openvpn
rm -rf /etc/openvpn
apt purge -y openvpn

# nginx
systemctl stop nginx
# dpkg warns on non-empty
rm -rf /etc/nginx /var/www/html /var/log/nginx
apt purge -y nginx*

# rabbitmq
systemctl stop rabbitmq-server
apt purge -y rabbitmq-server

# zabbix
```

```
apt purge -y zabbix-*
rm -rf /etc/systemd/system/multi-user.target.wants/zabbix-agent.service

# all virtualenvs
rm -rf /var/lib/virtualenvs

apt purge -y python-pip
apt purge -y python3-pip

# firewall clean
iptables -t nat -F
iptables -t mangle -F
iptables -F
iptables -X
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables-save | sudo tee /etc/iptables/rules.v4 >> /dev/null

apt autoremove -y

systemctl daemon-reload
systemctl reset-failed
```

14. Technical Support

If you encounter any issues using Dr.Web vxCube, you can contact the Doctor Web technical support in the following ways:

- Fill in the web form: https://support.drweb.com/support_wizard/vxcube.
- Call by phone in Moscow: +7 (495) 789-45-86. Free phone call (within Russia): 8-800-333-7932.

Refer to the official website at https://company.drweb.com/contacts/offices/ for regional and international office information of Doctor Web company.

15. Appendix A. List of Software on Virtual Machines

Windows XP x86

- Microsoft Office Enterprise 2007 x86 (optional)
- Adobe Acrobat Reader 10.1.0
- Adobe Flash 12.0.0.77
- JAVA 6u45
- Adobe Flash Standalone 10.3.181.23 (%windir%\flash_sa.exe)
- Mozilla Firefox 52.0.2
- Opera 35.0
- Google Chrome 44.0.2403.155
- ICQ 8.3 build 7317
- QIP 2012 4.0.9380
- Pidgin 2.10.11
- Mozilla Thunderbird 31.7.0
- Visual C++ Redistributable 2005 x86
- Visual C++ Redistributable 2008 x86
- Visual C++ Redistributable 2010 x86
- Visual C++ Redistributable 2012 x86
- Visual C++ Redistributable 2013 x86
- Visual C++ Redistributable 2015 x86
- .NET Framework 1.1
- .NET Framework SDK (msvcp70.dll, msvcr70.dll)
- .NET Framework 2.0 Service Pack SP2
- .NET Framework 3.0 Service Pack SP2
- .NET Framework 3.5 Service Pack SP1
- .NET Framework 4.0
- Steam 2.91
- WinRAR 5.20 x86
- Telegram Desktop 1.2.17
- mIRC 7.43

Windows 7 x86

- Adobe Acrobat Reader 11.0.1
- Microsoft Office Professional Plus 2010 x86 (optional)
- Adobe Flash 12.0.0.77

- Adobe Flash ActiveX 17.0.0.188
- JAVA 7u11
- Adobe Flash Standalone 11.1.102.62 (%windir%\flash_sa.exe)
- Mozilla Firefox 68.0.2
- Opera 33.0.1990.115
- Google Chrome 43.0.2357.65
- ICQ 8.3 build 7317
- QIP 2012 4.0.9380
- Pidgin 2.10.11
- Mozilla Thunderbird 31.7.0я
- Visual C++ Redistributable 2005 x86
- Visual C++ Redistributable 2008 x86
- Visual C++ Redistributable 2010 x86
- Visual C++ Redistributable 2012 x86
- Visual C++ Redistributable 2013 x86
- Visual C++ Redistributable 2015 x86
- .NET Framework 1.1
- .NET Framework SDK (msvcp70.dll, msvcr70.dll)
- .NET Framework 4.8
- Steam 3.17
- .NET Framework 4.7.1
- Telegram Desktop 1.2.17
- WinRAR 5.20 x86

Windows 7 x64

- Adobe Acrobat Reader Document Cloud 15.10.20056
- Microsoft Office Professional Plus 2010 x64 (optional)
- Adobe Flash 18.0.0.261
- Adobe Flash ActiveX 19.0.0.207
- JAVA 8u45 x64
- Adobe Flash Standalone 19.0.0.226 (%windir%\flash_sa.exe)
- K-Lite Mega Codec Pack 11.1.0
- Mozilla Firefox 78.0.2
- Opera 29.0.1795.47
- Google Chrome 42.0.2311.135
- ICQ 8.3 build 7317

- Mail.Ru Agent 6.4 build 8614
- QIP 2012 4.0.9380
- Pidgin 2.10.11
- Total Commander 8.51a x64
- Mozilla Thunderbird 31.6.0
- Winamp 5.666
- Visual C++ Redistributable 2005 x86
- Visual C++ Redistributable 2008 x86
- Visual C++ Redistributable 2010 x86
- Visual C++ Redistributable 2012 x86
- Visual C++ Redistributable 2013 x86
- Visual C++ Redistributable 2015 x86
- Visual C++ Redistributable 2005 x64
- Visual C++ Redistributable 2008 x64
- Visual C++ Redistributable 2010 x64
- Visual C++ Redistributable 2012 x64
- Visual C++ Redistributable 2013 x64
- Visual C++ Redistributable 2015 x64
- .NET Framework 1.1
- .NET Framework SDK (msvcp70.dll, msvcr70.dll)
- .NET Framework 4.8
- Steam 3.17
- Telegram Desktop 1.4.3
- .NET Framework 4.7.1
- WinRAR 5.3 x64
- mIRC 7.41

Windows 10 x64

- Adobe Acrobat Reader Document Cloud 2015.010.20060
- Adobe Flash 21.0.0.197
- Adobe Flash ActiveX 21.0.0.197
- Microsoft Office Professional Plus 2016 x86 (optional)
- JAVA 8u77 x64
- Adobe Flash Standalone 19.0.0.226 (%windir%\flash_sa.exe)
- Mozilla Firefox 91.0.2 x64
- Opera 36.0.2130.46

- Google Chrome 47.0.2526.80
- ICQ 8.3 build 7317
- QIP 2012 4.0.9380
- Pidgin 2.10.11
- Mozilla Thunderbird 38.7.1
- Visual C++ Redistributable 2005 x86
- Visual C++ Redistributable 2008 x86
- Visual C++ Redistributable 2010 x86
- Visual C++ Redistributable 2012 x86
- Visual C++ Redistributable 2013 x86
- Visual C++ Redistributable 2017 x86
- Visual C++ Redistributable 2005 x64
- Visual C++ Redistributable 2010 x64
- Visual C++ Redistributable 2012 x64
- Visual C++ Redistributable 2013 x64
- Visual C++ Redistributable 2017 x64
- .NET Framework 4.6.2
- Steam 3.37
- Telegram Desktop 1.4.3
- mIRC 7.43
- WinRAR 5.31 x64

Android 7.1

- Android Keyboard (AOSP) 7.1.2
- Calculator 7.1.2
- Calendar 7.1.2
- Camera 2.0.002
- Clock 4.5.0
- Contacts 1.4.22
- Dev Tools 1.0
- Email 7.1.2
- Files 7.1.2
- Gallery 1.1.40030
- Google Play 31.6.13-21
- Google Play Games 2022.01.32371
- Google Play Services 22.09.20

- Launcher3 7.1.2
- Messaging 1.0.001
- Music 3.0
- NotePad 7.1.2
- Phone 3.00.00
- RSS Reader 7.1.2
- Search 7.1.2
- Settings 7.1.2
- Terminal Emulator 1.0.70
- WebView Shell 1.0

Astra SE 1.7 (Voronezh)

- Standard software

Astra CE 2.12 (Orel)

- Standard software

Debian 8 (Jessie) ARMel 32-bit

- Standard software

Debian 8 (Jessie) PowerPC 32-bit

- Standard software

Debian 10 (Buster) MIPS 32-bit

- Standard software

Debian 11 (Bullseye) ARM 64-bit

- Standard software

Debian 11 (Bullseye) ARMhf 32-bit

- Standard software

Debian 11 (Bullseye) Intel 32-bit

- Standard software

Debian 11 (Bullseye) Intel 64-bit

- Standard software

Debian 11 (Bullseye) MIPSel 32-bit

- Standard software

Debian 11 (Bullseye) MIPSel 64-bit

- Standard software

Debian 11 (Bullseye) PowerPCel 64-bit

- Standard software

16. Appendix B. Functions of the dr_sandbox Module

Downloads the files (download_file)

Downloads files (download_files)

Executes (exec)

Executes WMI operations (exec_wmi)

Creates and executes files (an exploit) (exploit_create_and_exec)

Creates and loads libraries (an exploit) (exploit_create_and_load_library)

Executes the following (an exploit) (exploit_exec)

Forces autorun for removable media (force_autorun_for_removable_media)

Forces the system to hide file extensions from view (hide_from_view_file_extensions)

Forces the system to hide hidden files from view (hide_from_view_hidden_files)

Hides processes (hide_processes)

Disables taskbar notifications (hide_taskbar_notifications)

Hooks functions in browsers (hook_in_browser)

Installs hooks to intercept notifications on keystrokes for all processes (hook_keyboard_all_processes)

Installs hooks to intercept notifications on keystrokes for specific processes (hook_keyboard_concrete_processes)

Installs hooks to intercept notifications on window messages (hook_keyboard_on_window_messages)

Injects code into numerous user processes (inject_to_a_lot_of_user_processes)

Injects code into system processes (inject_to_system_proc)

Injects code into user processes (inject_to_user_proc)

Modifies settings of Windows Explorer (modify_explorer_settings)

Modifies settings of Windows Internet Explorer (modify_ie_settings)

Removes or modifies registry (modify_registry_to_bypass_firewall)

Changes the DNS server (modify_system_dns)

Modifies system settings (modify_system_settings)

Reads files that store third party passwords (read_third_party_passwords)

Registers BHO (register_bho)

Registers a COM server (register_com_server)

Registers file system filter (register_filesystem_filter)

Restores hooked functions in SSDT (restore_ssdt_hooks)

Searches for registry branches that store third party passwords (search_password_in_registry)

Searches for windows to detect analytical utilities (search_wnd_for_analyzing_soft)

Searches for windows to detect programs and games (search_wnd_for_programs_and_games)

Searches for windows to bypass anti-viruses (search_wnd_to_bypass_av)

Searches for windows to bypass WFP system (search_wnd_to_bypass_wfp)

Hook specific functions in SSDT (set_concrete_ssdt_hooks)

Sets a home page for Windows IE (set_homepage_for_ie)

Hook specific functions in SSDT (set_ssdt_hooks)

Terminates numerous user processes (try_to_terminate_a_lot_of_user_processes)

Terminates system processes (try_to_terminate_system_processes)

Terminates user processes (try_to_terminate_user_processes)

Miscellaneous (the 'miscellaneous' category)

Adds a root certificate (add_root_certificate)

Creates and executes (create_and_exec)

Disables a certificate (disable_certificate)

Executes (exec)

Loads drivers (load_driver)

Changes the AutoConfigURL parameter (modify_auto_config_url)

The descriptions of the functions for the Android sandbox (the 'andr' category)

Function	Result	Examples
`archive_file(regex)`	The list of files that are included in APK and match the pattern: ARCHIVE_FILES_PATTERN = ['.dll', '.js', '.html', '.so'].	`dr_sandbox.andr.archive_files(/pattern/)`
`archive_file_num`	The list of files that are included in APK and match the pattern: ARCHIVE_FILES_PATTERN = ['.dll', '.js', '.html', '.so'].	`dr_sandbox.andr.archive_files_num`
`certificate_sha1(regex)`	The SHA1 hash of the certificate that an app is signed with.	`dr_sandbox.andr.certificate_sha1(/pattern/)`
`certificate_sha1_num`	The SHA1 hash of the certificate that an app is signed with.	`dr_sandbox.andr.certificate_sha1_num`
The **`dynamic`** `subcategory`		
`created_files.path(regex)`	Created files: a path.	`dr_sandbox.andr.`**`dynamic`**`.created_files.path(/pattern/)`
`created_files.path_num`	Created files: a path.	`dr_sandbox.andr.`**`dynamic`**`.created_files.path_num`
`created_files.sha1(regex)`	Created files: SHA1.	`dr_sandbox.andr.`**`dynamic`**`.created_files.sha1(/pattern/)`
`created_files.sha1_num`	Created files: SHA1.	`dr_sandbox.andr.`**`dynamic`**`.created_files.sha1_num`
`crypto_dumps(regex)`	Encrypted dumps.	`dr_sandbox.andr.`**`dynamic`**`.crypto_dumps(/pattern/)`
`crypto_dumps_num`	Encrypted dumps.	`dr_sandbox.andr.`**`dynamic`**`.crypto_dumps_num`
`downloaders.detect(regex)`	The list of samples that download an analyzed sample.	`dr_sandbox.andr.`**`dynamic`**`.downloaders.detect(/pattern/)`

Function	Result	Examples
`downloaders.detect_num`	The list of samples that download an analyzed sample.	`dr_sandbox.andr.`**`dynamic`**`.downloaders.detect_num`
`downloaders.sha1(regex)`	The list of samples that download an analyzed sample.	`dr_sandbox.andr.`**`dynamic`**`.downloaders.sha1(/pattern/)`
`downloaders.sha1_num`	The list of samples that download an analyzed sample.	`dr_sandbox.andr.`**`dynamic`**`.downloaders.sha1_num`
`downloads.detect(regex)`	The downloaded payload (apk/dex).	`dr_sandbox.andr.`**`dynamic`**`.downloads.detect(/pattern/)`
`downloads.detect_num`	The downloaded payload (apk/dex).	`dr_sandbox.andr.`**`dynamic`**`.downloads.detect_num`
`downloads.sha1(regex)`	The downloaded payload (apk/dex).	`dr_sandbox.andr.`**`dynamic`**`.downloads.sha1(/pattern/)`
`downloads.sha1_num`	The downloaded payload (apk/dex).	`dr_sandbox.andr.`**`dynamic`**`.downloads.sha1_num`
`downloads.url(regex)`	The downloaded payload (apk/dex).	`dr_sandbox.andr.`**`dynamic`**`.downloads.url(/pattern/)`
`downloads.url_num`	The downloaded payload (apk/dex).	`dr_sandbox.andr.`**`dynamic`**`.downloads.url_num`
`droppers.detect(regex)`	The list of samples that upload an analyzed sample.	`dr_sandbox.andr.`**`dynamic`**`.droppers.detect(/pattern/)`
`droppers.detect_num`	The list of samples that upload an analyzed sample.	`dr_sandbox.andr.`**`dynamic`**`.droppers.detect_num`
`droppers.sha1(regex)`	The list of samples that upload an analyzed sample.	`dr_sandbox.andr.`**`dynamic`**`.droppers.sha1(/pattern/)`
`droppers.sha1_num`	The list of samples that upload an analyzed sample.	`dr_sandbox.andr.`**`dynamic`**`.droppers.sha1_num`
`dumps.detect(regex)`	The payload dump: a detect.	`dr_sandbox.andr.`**`dynamic`**`.dumps.detect(/pattern/)`

Function	Result	Examples
`dumps.detect_num`	The payload dump: a detect.	`dr_sandbox.andr.`**`dynamic`**`.dumps.detect_num`
`dumps.path(regex)`	The payload dump: a path.	`dr_sandbox.andr.`**`dynamic`**`.dumps.path(/pattern/)`
`dumps.path_num`	The payload dump: a path.	`dr_sandbox.andr.`**`dynamic`**`.dumps.path_num`
`dumps.sha1(regex)`	The payload dump: a SHA1 hash.	`dr_sandbox.andr.`**`dynamic`**`.dumps.sha1(/pattern/)`
`dumps.sha1_num`	The payload dump: a SHA1 hash.	`dr_sandbox.andr.`**`dynamic`**`.dumps.sha1_num`
`executed_commands(regex)`	Executed shell commands.	`dr_sandbox.andr.`**`dynamic`**`.executed_commands(/pattern/)`
`executed_commands_num`	Executed shell commands.	`dr_sandbox.andr.`**`dynamic`**`.executed_commands_num`
`flags(regex)`	Behavior flags.	`dr_sandbox.andr.`**`dynamic`**`.flags(/pattern/)`
`flags_num`	Behavior flags.	`dr_sandbox.andr.`**`dynamic`**`.flags_num`
`phone_calls(regex)`	Phone calls.	`dr_sandbox.andr.`**`dynamic`**`.phone_calls(/pattern/)`
`phone_calls_num`	Phone calls.	`dr_sandbox.andr.`**`dynamic`**`.phone_calls_num`
`sms.message(regex)`	Sent SMS: a message content.	`dr_sandbox.andr.`**`dynamic`**`.sms.message(/pattern/)`
`sms.message_num`	Sent SMS: a message content.	`dr_sandbox.andr.`**`dynamic`**`.sms.message_num`
`sms.number(regex)`	Sent SMS: a phone number.	`dr_sandbox.andr.`**`dynamic`**`.sms.number(/pattern/)`
`sms.number_num`	Sent SMS: a phone number.	`dr_sandbox.andr.`**`dynamic`**`.sms.number_num`
`urls(regex)`	Found URLs. Only the URLs that match the regular expression are counted.	`dr_sandbox.andr.`**`dynamic`**`.urls(/pattern/)`

Function	Result	Examples
urls_num	Found URLs.	dr_sandbox.andr.**dynamic**.urls_num
The **manifest** subcategory		
activities(regex)	The list of app activities (screens).	dr_sandbox.andr.**manifest**.activities(/pattern/)
activities_num	The list of all app activities (screens).	dr_sandbox.andr.**manifest**.activities_num
app_name(regex)	The app name on the device.	dr_sandbox.andr.**manifest**.app_name(/pattern/)
app_name_num	The app name on the device.	dr_sandbox.andr.**manifest**.app_name_num
filters(regex)	The list of actions from the manifest.	dr_sandbox.andr.**manifest**.filters(/pattern/)
filters_num	The list of actions from the manifest.	dr_sandbox.andr.**manifest**.filters_num
home_activity(regex)	Activity, the app entry point.	dr_sandbox.andr.**manifest**.home_activity(/pattern/)
home_activity_num	Activity, the app entry point.	dr_sandbox.andr.**manifest**.home_activity_num
is_firmware(regex)	Is app from firmware or not.	dr_sandbox.andr.**manifest**.is_firmware(/pattern/)
is_firmware_num	Is app from firmware or not.	dr_sandbox.andr.**manifest**.is_firmware_num
main_activity(regex)	Main activity, the app entry point.	dr_sandbox.andr.**manifest**.main_activity(/pattern/)
main_activity_num	Main activity, the app entry point.	dr_sandbox.andr.**manifest**.main_activity_num
meta_data.name(regex)	Metadata: the name.	dr_sandbox.andr.**manifest**.meta_data.name(/pattern/)
meta_data.name_num	Metadata: the name.	dr_sandbox.andr.**manifest**.meta_data.name_num
meta_data.resour	Metadata: the resource.	dr_sandbox.andr.**manifest**.meta_data.resource(/pattern/)

Function	Result	Examples
`ce(regex)`		
`meta_data.resource_num`	Metadata: the resource.	`dr_sandbox.andr.`**`manifest`**`.meta_data.resource_num`
`meta_data.value(regex)`	Metadata: the value.	`dr_sandbox.andr.`**`manifest`**`.meta_data.value(/pattern/)`
`meta_data.value_num`	Metadata: the value.	`dr_sandbox.andr.`**`manifest`**`.meta_data.value_num`
`package(regex)`	The app package name.	`dr_sandbox.andr.`**`manifest`**`.package(/pattern/)`
`package_num`	The app package name.	`dr_sandbox.andr.`**`manifest`**`.package_num`
`permissions(regex)`	The list of permissions that the app needs.	`dr_sandbox.andr.`**`manifest`**`.permissions(/pattern/)`
`permissions_num`	The list of permissions that the app needs.	`dr_sandbox.andr.`**`manifest`**`.permissions_num`
`receivers(regex)`	The list of broadcast receivers.	`dr_sandbox.andr.`**`manifest`**`.receivers(/pattern/)`
`receivers_num`	The list of broadcast receivers.	`dr_sandbox.andr.`**`manifest`**`.receivers_num`
`services(regex)`	The list of app services.	`dr_sandbox.andr.`**`manifest`**`.services(/pattern/)`
`services_num`	The list of app services.	`dr_sandbox.andr.`**`manifest`**`.services_num`
`strings_resources(regex)`	The list of all string resources.	`dr_sandbox.andr.`**`manifest`**`.strings_resources(/pattern/)`
`strings_resources_num`	The list of all string resources.	`dr_sandbox.andr.`**`manifest`**`.strings_resources_num`
`version_code(regex)`	The version code.	`dr_sandbox.andr.`**`manifest`**`.version_code(/pattern/)`
`version_code_num`	The version code.	`dr_sandbox.andr.`**`manifest`**`.version_code_num`
`version_name(regex)`	The version name.	`dr_sandbox.andr.`**`manifest`**`.version_name(/pattern/)`

Function	Result	Examples
`version_name_num`	The version name.	`dr_sandbox.andr.`**`manifest`**`.version_name_num`
`resources_digests(regex)`	The list of SHA1-Digest for APK resource files.	`dr_sandbox.andr.resources_digests(/pattern/)`
`resources_digests_num`	The list of SHA1-Digest for APK resource files.	`dr_sandbox.andr.resources_digests_num`
`sha1(regex)`	SHA1 of the sample.	`dr_sandbox.andr.sha1(/pattern/)`
`sha1_num`	SHA1 of the sample.	`dr_sandbox.andr.sha1_num`
`source_host(regex)`	The sample source.	`dr_sandbox.andr.source_host(/pattern/)`
`source_host_num`	The sample source.	`dr_sandbox.andr.source_host_num`

The descriptions of the functions for the Windows sandbox (the 'descr_tech' category)

Enabling autorun and distribution (the 'autorun' category)

Function	Result	Event type	Examples
`change_system_executable_files(regex)`	Returns the number of events of a specific type.	Changes executable system files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.autorun.change_system_executable_files(/beep.sys/)`
`change_system_executable_files_num`	Returns the amount of events of a certain type.	Changes executable system files.	`dr_sandbox.descr_tech.autorun.change_system_executable_files_num > 0`
`create_files_on_removable_media(regex)`	Returns the number of events of a specific type.	Creates files on removable media. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.autorun.create_files_on_removable_media(/10thingscondoms.pdf/)`
`create_files_on_removable_media_num`	Returns the number of events of a specific type.	Creates files on removable media.	`dr_sandbox.descr_tech.autorun.create_files_on_removable_media_num > 0`

Function	Result	Event type	Examples
`create_or_modify_files(regex)`	Returns the number of events of a specific type.	Creates or changes files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.autorun.create_or_modify_files(/YogaGuide.job/)`
`create_or_modify_files_num`	Returns the number of events of a specific type.	Creates or modifies files.	`dr_sandbox.descr_tech.autorun.create_or_modify_files_num == 1`
`create_services(regex)`	Returns the number of events of a specific type.	Creates services. Only the services that match the regular expression are counted.	`dr_sandbox.descr_tech.autorun.create_services(/rsdsys/)`
`create_services_num`	Returns the amount of events of a certain type.	Creates services.	`dr_sandbox.descr_tech.autorun.create_services_num > 0`
`infect_executables(regex)`	Returns the amount of events of a certain type.	Infects executable files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.autorun.infect_executables(/eirmayxm/)`
`infect_executables_num`	Returns the number of events of a specific type.	Infects executable files.	`dr_sandbox.descr_tech.autorun.infect_executables_num > 0`
`modify_mbr`	Returns 1 if a master boot record (MBR) is modified, 0 otherwise.	Modifies the master boot record (MBR).	`dr_sandbox.descr_tech.autorun.modify_mbr`
`modify_registry(regex)`	Returns the number of events of a specific type.	Modifies registry keys. Only the keys that match the regular expression are counted.	`dr_sandbox.descr_tech.autorun.modify_registry(/C:\Users\user\AppData\Roaming\Sample.lnk/)`
`modify_registry_num`	Returns the number of events of a specific type.	Modifies registry keys.	`dr_sandbox.descr_tech.autorun.modify_registry_num >= 2`
`replace_system_executable_files(regex)`	Returns the number of events of a specific type.	Replaces executable system files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.autorun.replace_system_executable_files(/ir50_qc.dll/)`

Function	Result	Event type	Examples
`replace_system_executable_files_num`	Returns the number of events of a specific type.	Replaces executable system files.	`dr_sandbox.descr_tech.autorun.replace_system_executable_files_num > 0`

Modifies a file system (the 'filesystem' category)

Function	Result	Event type	Examples
`change_user_data_extensions`	Returns the number of events of a specific type.	Changes file extensions in user data (Trojan.Encoder).	`dr_sandbox.descr_tech.filesystem.change_user_data_extensions`
`create_files(regex)`	Returns the number of events of a specific type.	Creates files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.filesystem.create_files(/nsArray.dll/)`
`create_files_num`	Returns the number of events of a specific type.	Creates files.	`dr_sandbox.descr_tech.filesystem.create_files_num >= 2`
`create_ransom_message_files`	Returns the number of events of a specific type.	Creates files and demands payment for file decoding (Trojan.Encoder).	`dr_sandbox.descr_tech.filesystem.create_ransom_message_files`
`modify_hosts`	Returns 1 if the HOSTS file is modified, 0 otherwise.	Modifies the HOSTS file.	`dr_sandbox.descr_tech.filesystem.modify_hosts`
`modify_user_data_files`	Returns the number of events of a specific type.	Changes a large amount of user data (Trojan.Encoder).	`dr_sandbox.descr_tech.filesystem.modify_user_data_files`
`move_files(regex)`	Returns the number of events of a specific type.	Moves files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.filesystem.move_files(/%WINDIR%.*CONFIG\security.config.cch/)`
`move_files_num`	Returns the number of events of a specific type.	Moves files.	`dr_sandbox.descr_tech.filesystem.move_files_num >= 2`
`move_self(regex)`	Returns the number of events of a	Moves itself.	`dr_sandbox.descr_tech.filesystem.move_self(/CreativeAudi`

Function	Result	Event type	Examples
	specific type.		o/)
move_self_num	Returns the number of events of a specific type.	Moves itself.	dr_sandbox.descr_tech.filesystem.move_self_num >= 2
move_system_files(regex)	Returns the number of events of a specific type.	Moves system files. Only the files that match the regular expression are counted.	dr_sandbox.descr_tech.filesystem.move_system_files(/ir50_qc.dll/)
move_system_files_num	Returns the number of events of a specific type.	Moves system files.	dr_sandbox.descr_tech.filesystem.move_system_files_num >= 2
remove_files(regex)	Returns the number of events of a specific type.	Deletes files. Only the files that match the regular expression are counted.	dr_sandbox.descr_tech.filesystem.remove_files(/^%TEMP%\7zS1.tmp\GOMPLAYERENSETUP.EXE$/)
remove_files_num	Returns the number of events of a specific type.	Deletes files.	dr_sandbox.descr_tech.filesystem.remove_files_num >= 2
remove_self	Returns the number of events of a specific type.	Deletes itself.	dr_sandbox.descr_tech.filesystem.remove_self
set_hidden(regex)	Returns the number of events of a specific type.	Assigns the 'hidden' attribute to files. Only the files that match the regular expression are counted.	dr_sandbox.descr_tech.filesystem.set_hidden(/^%TEMP%\~2.cmd$/)
set_hidden_num	Returns the number of events of a specific type.	Assigns the 'hidden' attribute to files.	dr_sandbox.descr_tech.filesystem.set_hidden_num >= 2
substitute_executables(regex)	Returns the number of events of a specific type.	Substitutes executable files. Only the files that match the regular expression are counted.	dr_sandbox.descr_tech.filesystem.substitute_executables(/pattern/)
substitute_executables_num	Returns the number of events of a specific type.	Substitutes executable files.	dr_sandbox.descr_tech.filesystem.substitute_executables_num >= 2

Function	Result	Event type	Examples
substitute_files(regex)	Returns the number of events of a specific type.	Substitutes files. Only the files that match the regular expression are counted.	dr_sandbox.descr_tech.filesystem.substitute_files(/pattern/)
substitute_files_num	Returns the number of events of a specific type.	Substitutes files.	dr_sandbox.descr_tech.filesystem.substitute_files_num >= 2
substitute_hosts	Returns the number of events of a specific type.	Replaces the HOSTS file.	dr_sandbox.descr_tech.filesystem.substitute_hosts

Malicious functions (the 'malicious' category)

Function	Result	Event type	Examples
add_antivirus_exclusion(regex)	Returns the number of events of a specific type.	In order to make it harder to detect in the operating system, adds anti-virus exclusions using the registry keys. Only the keys that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.add_antivirus_exclusion(/pattern/)
add_antivirus_exclusion_num	Returns the number of events of a specific type.	In order to make it harder to detect in the operating system, adds anti-virus exclusions using the registry keys.	dr_sandbox.descr_tech.malicious.add_antivirus_exclusion_num
block_cmd	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks the Command Prompt (CMD) system utility.	dr_sandbox.descr_tech.malicious.block_cmd
block_regedit	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks the	dr_sandbox.descr_tech.malicious.block_regedit

Function	Result	Event type	Examples
		Registry Editor (RegEdit) system utility.	
`block_system_file_checker`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks System File Checker (SFC).	`dr_sandbox.descr_tech.malicious.block_system_file_checker`
`block_system_restore`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks System Restore (SR).	`dr_sandbox.descr_tech.malicious.block_system_restore`
`block_taskmgr`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks the Windows Task Manager (Taskmgr) system utility.	`dr_sandbox.descr_tech.malicious.block_taskmgr`
`block_user_account_control`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks User Account Control (UAC).	`dr_sandbox.descr_tech.malicious.block_user_account_control`
`block_windows_action_center`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks Windows Action Center.	`dr_sandbox.descr_tech.malicious.block_windows_action_center`
`block_windows_defender`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks the Windows Defender system utility.	`dr_sandbox.descr_tech.malicious.block_windows_defender`
`block_windows_file_protection`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks	`dr_sandbox.descr_tech.malicious.block_windows_file_protection`

Function	Result	Event type	Examples
		Windows File Protection (WFP).	
`block_windows_firewall`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks the Windows Firewall system utility.	`dr_sandbox.descr_tech.malicious.block_windows_firewall`
`block_windows_security_center`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks Windows Security Center.	`dr_sandbox.descr_tech.malicious.block_windows_security_center`
`block_windows_updates`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, blocks the Windows Update system utility.	`dr_sandbox.descr_tech.malicious.block_windows_updates`
`bruteforce_os_accounts`	Returns 1 if the event occurred, 0 otherwise.	Brute forces passwords of OS accounts.	`dr_sandbox.descr_tech.malicious.bruteforce_os_accounts`
`create_and_exec(regex)`	Returns the number of events of a specific type.	Creates and executes. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.create_and_exec(/Total Commander/)`
`create_and_exec_num`	Returns the number of events of a specific type.	Creates and executes.	`dr_sandbox.descr_tech.malicious.create_and_exec_num > 0`
`create_onion_service`	Returns the number of events of a specific type.	Creates an onion service.	`dr_sandbox.descr_tech.malicious.create_onion_service`
`delete_volume_shadow_copies`	Returns the number of events of a specific type.	In order to make it harder to detect in the operating system, deletes volume shadow copies.	`dr_sandbox.descr_tech.malicious.delete_volume_shadow_copies`

Function	Result	Event type	Examples
`detect_virtual_machine(regex)`	Returns the number of events of a specific type.	Searches for windows to detect virtual machines. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.detect_virtual_machine(/pattern/)`
`detect_virtual_machine_num`	Returns the number of events of a specific type.	Searches for windows to detect virtual machines.	`dr_sandbox.descr_tech.malicious.detect_virtual_machine_num`
`disable_amsi`	Returns the number of events of a specific type.	Disables AMSI.	`dr_sandbox.descr_tech.malicious.disable_amsi`
`downloads_and_executes(regex)`	Returns the number of events of a specific type.	Downloads and executes. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.downloads_and_executes(/pattern/)`
`downloads_and_executes_num`	Returns the number of events of a specific type.	Downloads and executes.	`dr_sandbox.descr_tech.malicious.downloads_and_executes_num`
`downloads_and_executes_files`	Returns the number of events of a specific type.	Downloads and executes the files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.downloads_and_executes_files`
`download_file(regex)`	Returns the number of events of a specific type.	Downloads files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.download_file(/pattern/)`
`download_file_num`	Returns the number of events of a specific type.	Downloads files.	`dr_sandbox.descr_tech.malicious.download_file_num`
`download_files`	Returns 1 if the event occurred, 0 otherwise.	Downloads files.	`dr_sandbox.descr_tech.malicious.download_files`
`exec(regex)`	Returns the number of events of a specific type.	Executes. Only the objects that match the regular	`dr_sandbox.descr_tech.malicious.exec(/netsh.exe/)`

Function	Result	Event type	Examples
		expression are counted.	
exec_num	Returns the number of events of a specific type.	Executes.	dr_sandbox.descr_tech.malicious.exec_num > 0
exec_wmi(regex)	Returns the number of events of a specific type.	Executes WMI operations. Only the operations that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.exec_wmi(/pattern/)
exec_wmi_num	Returns the number of events of a specific type.	Executes WMI operations.	dr_sandbox.descr_tech.malicious.exec_wmi_num
exploit_create_and_exec(regex)	Returns the number of events of a specific type.	Creates and executes (an exploit). Only the objects that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.exploit_create_and_exec(/pattern/)
exploit_create_and_exec_num	Returns the number of events of a specific type.	Creates and executes files (an exploit).	dr_sandbox.descr_tech.malicious.exploit_create_and_exec_num
exploit_create_and_load_library(regex)	Returns the number of events of a specific type.	Creates and loads libraries (an exploit). Only the libraries that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.exploit_create_and_load_library(/pattern/)
exploit_create_and_load_library_num	Returns the number of events of a specific type.	Creates and loads libraries (an exploit).	dr_sandbox.descr_tech.malicious.exploit_create_and_load_library_num
exploit_exec(regex)	Returns the number of events of a specific type.	Executes (an exploit). Only the objects that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.exploit_exec(/pattern/)
exploit_exec_num	Returns the number of events of a specific type.	Executes (an exploit).	dr_sandbox.descr_tech.malicious.exploit_exec_num

Function	Result	Event type	Examples
`force_autorun_for_removable_media`	Returns 1 if the event occurred, 0 otherwise.	Forces autorun for removable media.	`dr_sandbox.descr_tech.malicious.force_autorun_for_removable_media`
`hide_from_view_file_extensions`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, forces the system to hide file extensions from view.	`dr_sandbox.descr_tech.malicious.hide_from_view_file_extensions`
`hide_from_view_hidden_files`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, forces the system to hide hidden files from view.	`dr_sandbox.descr_tech.malicious.hide_from_view_hidden_files`
`hide_processes(regex)`	Returns the number of events of a specific type.	Hides processes. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.hide_processes(/cscript.exe/)`
`hide_processes_num`	Returns the number of events of a specific type.	Hides processes.	`dr_sandbox.descr_tech.malicious.hide_processes_num > 0`
`hide_taskbar_notifications`	Returns 1 if the event occurred, 0 otherwise.	In order to make it harder to detect in the operating system, disables taskbar notifications.	`dr_sandbox.descr_tech.malicious.hide_taskbar_notifications`
`hook_in_browser(regex)`	Returns the number of events of a specific type.	Hooks functions in browsers. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.hook_in_browser(/pattern/)`
`hook_in_browser_num`	Returns the number of events of a specific type.	Hooks functions in browsers.	`dr_sandbox.descr_tech.malicious.hook_in_browser_num`
`hook_keyboard_all_processes(regex)`	Returns the number of events of a specific type.	Installs hooks to intercept	`dr_sandbox.descr_tech.malicious.hook_keyboard_all_processes(/OQKWHP\BJX.01/)`

Function	Result	Event type	Examples
		notifications on keystrokes. Handler for all processes (?LibraryPath).	
`hook_keyboard_all_processes_num`	Returns the number of events of a specific type.	Installs hooks to intercept notifications on keystrokes.	`dr_sandbox.descr_tech.malicious.hook_keyboard_all_processes_num > 0`
`hook_keyboard_concrete_processes(regex)`	Returns the number of events of a specific type.	Installs hooks to intercept notifications on keystrokes. Handler for the '(?HookedProcess.Name)' process: (?LibraryPath).	`dr_sandbox.descr_tech.malicious.hook_keyboard_concrete_processes(/IMDCSC.exe/)`
`hook_keyboard_concrete_processes_num`	Returns the number of events of a specific type.	Installs hooks to intercept notifications on keystrokes.	`dr_sandbox.descr_tech.malicious.hook_keyboard_concrete_processes_num > 0`
`hook_keyboard_on_window_messages(regex)`	Returns the number of events of a specific type.	Installs hooks to intercept notifications on window messages. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.hook_keyboard_on_window_messages(/pattern/)`
`hook_keyboard_on_window_messages_num`	Returns the number of events of a specific type.	Installs hooks to intercept notifications on window messages.	`dr_sandbox.descr_tech.malicious.hook_keyboard_on_window_messages_num`
`inject_to_a_lot_of_user_processes`	Returns 1 if the event occurred, 0 otherwise.	Injects code into numerous user processes.	`dr_sandbox.descr_tech.malicious.inject_to_a_lot_of_user_processes`
`inject_to_system_proc(regex)`	Returns the number of events of a specific type.	Injects code into system processes. Only the processes that match the	`dr_sandbox.descr_tech.malicious.inject_to_system_proc(/RegAsm.exe/)`

Function	Result	Event type	Examples
		regular expression are counted.	
inject_to_system_proc_num	Returns the number of events of a specific type.	Injects code into system processes.	dr_sandbox.descr_tech.malicious.inject_to_system_proc_num > 0
inject_to_user_proc(regex)	Returns the number of events of a specific type.	Injects code into user processes. Only the processes that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.inject_to_user_proc(/^iexplore.exe$/)
inject_to_user_proc_num	Returns the number of events of a specific type.	Injects code into user processes.	dr_sandbox.descr_tech.malicious.inject_to_user_proc_num > 0
modify_explorer_settings(regex)	Returns the number of events of a specific type.	Modifies settings of Windows Explorer. Only the settings that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.modify_explorer_settings(/’NoFolderOptions’ = ‘00000001’/)
modify_explorer_settings_num	Returns the number of events of a specific type.	Modifies settings of Windows Explorer.	dr_sandbox.descr_tech.malicious.modify_explorer_settings_num > 0
modify_ie_settings(regex)	Returns the number of events of a specific type.	Modifies settings of Windows Internet Explorer. Only the settings that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.modify_ie_settings(/Zones\1] ‘1206’ = ‘00000000’/)
modify_ie_settings_num	Returns the number of events of a specific type.	Modifies settings of Windows Internet Explorer.	dr_sandbox.descr_tech.malicious.modify_ie_settings_num > 0
modify_registry_to_bypass_firewall(regex)	Returns the number of events of a specific type.	To bypass firewall, removes or modifies registry keys. Only the keys that match the regular expression are counted.	dr_sandbox.descr_tech.malicious.modify_registry_to_bypass_firewall(/Enabled:taskmg.exe/)
modify_registry_to_bypass_	Returns the number of events of a	To bypass firewall, removes or modifies	dr_sandbox.descr_tech.malicious.modify_registry_to_bypas

Function	Result	Event type	Examples
`firewall_num`	specific type.	registry keys.	`s_firewall_num > 0`
`modify_system_dns(regex)`	Returns the number of events of a specific type.	In order to make it harder to detect in the operating system, modifies DNS servers. Only the servers that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.modify_system_dns(/pattern/)`
`modify_system_dns_num`	Returns the number of events of a specific type.	In order to make it harder to detect in the operating system, modifies DNS servers.	`dr_sandbox.descr_tech.malicious.modify_system_dns_num`
`modify_system_settings(regex)`	Returns the number of events of a specific type.	In order to make it harder to detect in the operating system, modifies system settings. Only the settings that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.modify_system_settings(/pattern/)`
`modify_system_settings_num`	Returns the number of events of a specific type.	In order to make it harder to detect in the operating system, modifies system settings.	`dr_sandbox.descr_tech.malicious.modify_system_settings_num`
`read_third_party_passwords(regex)`	Returns the number of events of a specific type.	Reads files that store third party app passwords. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.read_third_party_passwords(/pattern/)`
`read_third_party_passwords_num`	Returns the number of events of a specific type.	Reads files that store third party app passwords.	`dr_sandbox.descr_tech.malicious.read_third_party_passwords_num`
`register_bho(regex)`	Returns the number of events of a specific type.	Registers BHO. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.register_bho(/pattern/)`

Function	Result	Event type	Examples
`register_com_server(regex)`	Returns the number of events of a specific type.	Registers a COM server. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.register_com_server(/pattern/)`
`register_com_server_num`	Returns the number of events of a specific type.	Registers a COM server.	`dr_sandbox.descr_tech.malicious.register_com_server_num`
`register_filesystem_filter(regex)`	Returns the number of events of a specific type.	Registers a file system filter. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.register_filesystem_filter(/pattern/)`
`restore_ssdt_hooks`	Returns 1 if the event occurred, 0 otherwise.	Restores hooked functions in the System Service Descriptor Table (SSDT).	`dr_sandbox.descr_tech.malicious.restore_ssdt_hooks`
`search_password_in_registry(regex)`	Returns the number of events of a specific type.	Searches for registry branches where third party apps store their passwords. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.search_password_in_registry(/MessengerService/)`
`search_password_in_registry_num`	Returns the number of events of a specific type.	Searches for registry branches where third-party apps store their passwords.	`dr_sandbox.descr_tech.malicious.search_password_in_registry_num > 0`
`search_wnd_for_analyzing_soft(regex)`	Returns the number of events of a specific type.	Searches for windows to detect analytical utilities. Only the objects that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.search_wnd_for_analyzing_soft(/PEiD/)`
`search_wnd_for_analyzing_soft_num`	Returns the number of events of a specific type.	Searches for windows to detect analytical utilities.	`dr_sandbox.descr_tech.malicious.search_wnd_for_analyzing_soft_num > 0`

Function	Result	Event type	Examples
`search_wnd_for_programs_and_games(regex)`	Returns the number of events of a specific type.	Searches for windows to detect apps and games. Only the windows that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.search_wnd_for_programs_and_games(/The Wireshark Network Analyzer/)`
`search_wnd_for_programs_and_games_num`	Returns the number of events of a specific type.	Searches for windows to detect apps and games.	`dr_sandbox.descr_tech.malicious.search_wnd_for_programs_and_games_num > 0`
`search_wnd_to_bypass_av(regex)`	Returns the number of events of a specific type.	Searches for windows to bypass anti-viruses. Only the windows that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.search_wnd_to_bypass_av(/AVP.AlertDialog/)`
`search_wnd_to_bypass_av_num`	Returns the number of events of a specific type.	Searches for windows to bypass anti-viruses.	`dr_sandbox.descr_tech.malicious.search_wnd_to_bypass_av_num > 0`
`search_wnd_to_bypass_wfp(regex)`	Returns the number of events of a specific type.	Searches for windows to bypass Windows Files Protection (WFP). Only the windows that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.search_wnd_to_bypass_wfp(/Windows File Protection/)`
`search_wnd_to_bypass_wfp_num`	Returns the number of events of a specific type.	Searches for windows to bypass Windows Files Protection (WFP).	`dr_sandbox.descr_tech.malicious.search_wnd_to_bypass_wfp_num > 0`
`set_concrete_ssdt_hooks(regex)`	Returns the number of events of a specific type.	Hooks functions in System Service Descriptor Table (SSDT). Only the functions that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.set_concrete_ssdt_hooks(/pattern/)`
`set_concrete_ssdt_hooks_num`	Returns the number of events of a specific type.	Hooks functions in System Service Descriptor Table (SSDT).	`dr_sandbox.descr_tech.malicious.set_concrete_ssdt_hooks_num`

Function	Result	Event type	Examples
`set_homepage_for_ie`	Returns 1 if the event occurred, 0 otherwise.	Sets a new unauthorized home page for Windows Internet Explorer.	`dr_sandbox.descr_tech.malicious.set_homepage_for_ie`
`set_ssdt_hooks`	Returns the number of events of a specific type.	Hooks functions in System Service Descriptor Table (SSDT).	`dr_sandbox.descr_tech.malicious.set_ssdt_hooks`
`try_to_terminate_a_lot_of_user_processes`	Returns 1 if the event occurred, 0 otherwise.	Terminates or attempts to terminate numerous user processes.	`dr_sandbox.descr_tech.malicious.try_to_terminate_a_lot_of_user_processes`
`try_to_terminate_system_processes(regex)`	Returns the number of events of a specific type.	Terminates or attempts to terminate system processes. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.try_to_terminate_system_processes(/ctfmon.exe/)`
`try_to_terminate_system_processes_num`	Returns the number of events of a specific type.	Terminates or attempts to terminate system processes.	`dr_sandbox.descr_tech.malicious.try_to_terminate_system_processes_num > 0`
`try_to_terminate_user_processes(regex)`	Returns the number of events of a specific type.	Terminates or attempts to terminate user processes. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech.malicious.try_to_terminate_user_processes(/^AVSYNMGR.EXE$/)`
`try_to_terminate_user_processes_num`	Returns the number of events of a specific type.	Terminates or attempts to terminate user processes.	`dr_sandbox.descr_tech.malicious.try_to_terminate_user_processes_num > 0`

Miscellaneous (the 'miscellaneous' category)

Function	Result	Event type	Examples
`add_root_certificate`	Returns 1 if the scanned object adds certificate, 0 otherwise.	Adds a root certificate.	`dr_sandbox.descr_tech.miscellaneous.add_root_certificate`
`create_and_exec`	Returns 1 if the event occurred, 0 otherwise.	Creates and executes (with a hidden window).	`dr_sandbox.descr_tech.miscellaneous.create_and_exec`
`disable_certificate`	Returns 1 if the event occurred, 0 otherwise.	Disables a certificate.	`dr_sandbox.descr_tech.miscellaneous.disable_certificate`
`exec(regex)`	Returns the number of events of a specific type.	Executes. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech.miscellaneous.exec(/pattern/)`
`load_driver(regex)`	Returns the number of events of a specific type.	Loads the drivers. Only the drivers that match the regular expression are counted.	`dr_sandbox.descr_tech.miscellaneous.load_driver(/pattern/)`
`load_driver_num`	Returns the number of events of a specific type.	Loads drivers.	`dr_sandbox.descr_tech.miscellaneous.load_driver_num`
`modify_auto_config_url(regex)`	Returns the number of events of a specific type.	Changes the AutoConfigURL parameter. Only the values that match the regular expression are counted.	`dr_sandbox.descr_tech.miscellaneous.modify_auto_config_url(/pattern/)`
`search_wnd(regex)`	Returns the number of events of a specific type.	Searches for windows. Only the windows that match the regular expression are counted.	`dr_sandbox.descr_tech.miscellaneous.search_wnd(/MS_WebcheckMonitor/)`
`search_wnd_num`	Returns the number of events of a specific type.	Searches for windows.	`dr_sandbox.descr_tech.miscellaneous.search_wnd_num == 3`

Function	Result	Event type	Examples
`shut_down_windows`	Returns 1 if the event occurred, 0 otherwise.	Attempts to shut down Windows OS.	`dr_sandbox.descr_tech.miscellaneous.shut_down_windows`
`use_ntfs_data_streams`	Returns 1 if the event occurred, 0 otherwise.	Uses NTFS alternate data streams.	`dr_sandbox.descr_tech.miscellaneous.use_ntfs_data_streams`

Network activity (the 'network' category)

Function	Result	Event type	Examples
`connect_to(regex)`	Returns the number of events of a specific type.	Connects to the objects listed in the regular expression.	`dr_sandbox.descr_tech.network.connect_to(/www.xfo.cn/)`
`connect_to_num`	Returns the number of events of a specific type.	Connects to the objects.	`dr_sandbox.descr_tech.network.connect_to_num >= 2`
`tcp(regex)`	Returns the number of events of a specific type.	TCP requests.	`dr_sandbox.descr_tech.network.tcp(/pattern/)`
`tcp_num`	Returns the number of events of a specific type.	TCP requests.	`dr_sandbox.descr_tech.network.tcp_num`
`tcp_http_get(regex)`	Returns the number of events of a specific type.	HTTP GET requests using TCP.	`dr_sandbox.descr_tech.network.tcp_http_get(/addurl.html$/)`
`tcp_http_get_num`	Returns the number of events of a specific type.	HTTP GET requests using TCP.	`dr_sandbox.descr_tech.network.tcp_http_get_num >= 2`
`tcp_http_post(regex)`	Returns the number of events of a specific type.	HTTP POST requests using TCP.	`dr_sandbox.descr_tech.network.tcp_http_post(/addurl.html$/)`
`tcp_http_post_num`	Returns the number of events of a specific type.	HTTP POST requests using TCP.	`dr_sandbox.descr_tech.network.tcp_http_post_num >= 2`
`tcp_http_unk(regex)`	Returns the number of events of a specific type.	Unknown HTTP requests.	`dr_sandbox.descr_tech.network.tcp_http_unk(/pattern/)`

Function	Result	Event type	Examples
tcp_http_unk_num	Returns the number of events of a specific type.	Unknown HTTP requests.	dr_sandbox.descr_tech.network.tcp_http_unk_num
udp(regex)	Returns the number of events of a specific type.	UDP requests.	dr_sandbox.descr_tech.network.udp(/disk57/)
udp_num	Returns the number of events of a specific type.	UDP requests.	dr_sandbox.descr_tech.network.udp_num >= 2

Functions for the Linux sandbox (the 'descr_tech_lbcl' category)

Enabling autorun and distribution (the 'autorun' category)

Function	Result	Event type	Examples
create_or_modify_files(regex)	Returns the number of events of a specific type.	Creates or changes files. Only the files that match the regular expression are counted.	dr_sandbox.descr_tech_lbcl.autorun.create_or_modify_files(/pattern/)
create_or_modify_files_num	Returns the number of events of a specific type.	Creates or modifies files.	dr_sandbox.descr_tech_lbcl.autorun.create_or_modify_files_num
create_or_modify_symlinks(regex)	Returns the number of events of a specific type.	Creates or modifies symbolic links. Only the links that match the regular expression are counted.	dr_sandbox.descr_tech_lbcl.autorun.create_or_modify_symlinks(/pattern/)
create_or_modify_symlinks_num	Returns the number of events of a specific type.	Creates or modifies symbolic links.	dr_sandbox.descr_tech_lbcl.autorun.create_or_modify_symlinks_num

Modifies a file system (the 'filesystem' category)

Function	Result	Event type	Examples
change_time_o	Returns the number of events of a	Changes the time when the file was	dr_sandbox.descr_tech_lbcl.filesystem.change_time_of_fil

Function	Result	Event type	Examples
`f_file(regex)`	specific type.	created, accessed, or modified. Only the files that match the regular expression are counted.	`e(/pattern/)`
`change_time_of_file_num`	Returns the number of events of a specific type.	Changes the time when the file was created, accessed, or modified.	`dr_sandbox.descr_tech_lbcl.filesystem.change_time_of_file_num`
`create_dir(regex)`	Returns the number of events of a specific type.	Creates directories. Only the directories that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.filesystem.create_dir(/pattern/)`
`create_dir_num`	Returns the number of events of a specific type.	Creates directories.	`dr_sandbox.descr_tech_lbcl.filesystem.create_dir_num`
`create_or_modify_file(regex)`	Returns the number of events of a specific type.	Creates or changes files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.filesystem.create_or_modify_file(/pattern/)`
`create_or_modify_file_num`	Returns the number of events of a specific type.	Creates or modifies files.	`dr_sandbox.descr_tech_lbcl.filesystem.create_or_modify_file_num`
`create_symlink(regex)`	Returns the number of events of a specific type.	Creates symbolic links.	`dr_sandbox.descr_tech_lbcl.filesystem.create_symlink(/pattern/)`
`create_symlink_num`	Returns the number of events of a specific type.	Only the links that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.filesystem.create_symlink_num`
`lock_file(regex)`	Returns the number of events of a specific type.	Blocks files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.filesystem.lock_file(/pattern/)`
`lock_file_num`	Returns the number of events of a specific type.	Blocks files.	`dr_sandbox.descr_tech_lbcl.filesystem.lock_file_num`
`modify_file_a`	Returns the number of events of a	Changes file access rights.	`dr_sandbox.descr_tech_lbcl.filesystem.modify_file_access`

Function	Result	Event type	Examples
`ccess_rights(regex)`	specific type.		`_rights(/pattern/)`
`modify_file_access_rights_num`	Returns the number of events of a specific type.	Changes file access rights.	`dr_sandbox.descr_tech_lbcl.filesystem.modify_file_access_rights_num`
`modify_file_owner(regex)`	Returns the number of events of a specific type.	Changes a file owner.	`dr_sandbox.descr_tech_lbcl.filesystem.modify_file_owner(/pattern/)`
`modify_file_owner_num`	Returns the number of events of a specific type.	Changes a file owner.	`dr_sandbox.descr_tech_lbcl.filesystem.modify_file_owner_num`
`mount_file_system(regex)`	Returns the number of events of a specific type.	Mounts file systems. Only the systems that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.filesystem.mount_file_system(/pattern/)`
`mount_file_system_num`	Returns the number of events of a specific type.	Mounts file systems.	`dr_sandbox.descr_tech_lbcl.filesystem.mount_file_system_num`
`remove_dir(regex)`	Returns the number of events of a specific type.	Deletes directories. Only the directories that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.filesystem.remove_dir(/pattern/)`
`remove_dir_num`	Returns the number of events of a specific type.	Deletes directories.	`dr_sandbox.descr_tech_lbcl.filesystem.remove_dir_num`
`remove_file(regex)`	Returns the number of events of a specific type.	Deletes files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.filesystem.remove_file(/pattern/)`
`remove_file_num`	Returns the number of events of a specific type.	Deletes files.	`dr_sandbox.descr_tech_lbcl.filesystem.remove_file_num`
`unmount_file_system(regex)`	Returns the number of events of a specific type.	Unmounts file systems. Only the systems that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.filesystem.unmount_file_system(/pattern/)`

Function	Result	Event type	Examples
unmount_file_system_num	Returns the number of events of a specific type.	Unmounts file systems.	dr_sandbox.descr_tech_lbcl.filesystem.unmount_file_system_num

Malicious functions (the 'malicious' category)

Function	Result	Event type	Examples
attempt_kill_system_proc(regex)	Returns the number of events of a specific type.	Tries to kill system processes. Only the processes that match the regular expression are counted.	dr_sandbox.descr_tech_lbcl.malicious.attempt_kill_system_proc(/pattern/)
attempt_kill_system_proc_num	Returns the number of events of a specific type.	Tries to kill system processes.	dr_sandbox.descr_tech_lbcl.malicious.attempt_kill_system_proc_num
attept_kill_analyzers(regex)	Returns the number of events of a specific type.	Tries to kill analyzers. Only the analyzers that match the regular expression are counted.	dr_sandbox.descr_tech_lbcl.malicious.attept_kill_analyzers(/pattern/)
attept_kill_analyzers_num	Returns the number of events of a specific type.	Tries to kill analyzers.	dr_sandbox.descr_tech_lbcl.malicious.attept_kill_analyzers_num
attept_kill_proc(regex)	Returns the number of events of a specific type.	Tries to kill processes. Only the processes that match the regular expression are counted.	dr_sandbox.descr_tech_lbcl.malicious.attept_kill_proc(/pattern/)
attept_kill_proc_num	Returns the number of events of a specific type.	Tries to kill processes.	dr_sandbox.descr_tech_lbcl.malicious.attept_kill_proc_num
compile_program_from_source_codes(regex)	Returns the number of events of a specific type.	Compiles source code.	dr_sandbox.descr_tech_lbcl.malicious.compile_program_from_source_codes(/pattern/)
compile_program_from_source_codes_num	Returns the number of events of a specific type.	Compiles source code.	dr_sandbox.descr_tech_lbcl.malicious.compile_program_from_source_codes_num

Function	Result	Event type	Examples
`gain_root_privileges`	Returns the number of events of a specific type.	Gains root access.	`dr_sandbox.descr_tech_lbcl.malicious.gain_root_privileges`
`get_access_to_ssh_keys`	Returns the number of events of a specific type.	Accesses SSH keys.	`dr_sandbox.descr_tech_lbcl.malicious.get_access_to_ssh_keys`
`inject_to_proc(regex)`	Returns the number of events of a specific type.	Injects itself in processes. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.inject_to_proc(/pattern/)`
`inject_to_proc_num`	Returns the number of events of a specific type.	Injects itself in processes.	`dr_sandbox.descr_tech_lbcl.malicious.inject_to_proc_num`
`kill_analyzers(regex)`	Returns the number of events of a specific type.	Kills analyzers. Only the analyzers that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.kill_analyzers(/pattern/)`
`kill_analyzers_num`	Returns the number of events of a specific type.	Kills analyzers.	`dr_sandbox.descr_tech_lbcl.malicious.kill_analyzers_num`
`kill_proc(regex)`	Returns the number of events of a specific type.	Kills processes. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.kill_proc(/pattern/)`
`kill_proc_num`	Returns the number of events of a specific type.	Kills processes.	`dr_sandbox.descr_tech_lbcl.malicious.kill_proc_num`
`kill_system_proc(regex)`	Returns the number of events of a specific type.	Kills system processes. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.kill_system_proc(/pattern/)`
`kill_system_proc_num`	Returns the number of events of a specific type.	Kills system processes.	`dr_sandbox.descr_tech_lbcl.malicious.kill_system_proc_num`

Function	Result	Event type	Examples
`launch_itself_as_daemon`	Returns the number of events of a specific type.	Launches itself as a daemon.	`dr_sandbox.descr_tech_lbcl.malicious.launch_itself_as_daemon`
`launch_processes(regex)`	Returns the number of events of a specific type.	Launches processes. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.launch_processes(/pattern/)`
`launch_processes_num`	Returns the number of events of a specific type.	Launches processes.	`dr_sandbox.descr_tech_lbcl.malicious.launch_processes_num`
`manage_services(regex)`	Returns the number of events of a specific type.	Manages services. Only the services that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.manage_services(/pattern/)`
`manage_services_num`	Returns the number of events of a specific type.	Manages services.	`dr_sandbox.descr_tech_lbcl.malicious.manage_services_num`
`modify_firewall_settings(regex)`	Returns the number of events of a specific type.	Changes firewall settings. Only the settings that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.modify_firewall_settings(/pattern/)`
`modify_firewall_settings_num`	Returns the number of events of a specific type.	Changes firewall settings.	`dr_sandbox.descr_tech_lbcl.malicious.modify_firewall_settings_num`
`modify_router_settings(regex)`	Returns the number of events of a specific type.	Changes router settings. Only the settings that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.modify_router_settings(/pattern/)`
`modify_router_settings_num`	Returns the number of events of a specific type.	Changes router settings.	`dr_sandbox.descr_tech_lbcl.malicious.modify_router_settings_num`
`operate_kernel_modules(regex)`	Returns the number of events of a specific type.	Operates kernel modules.	`dr_sandbox.descr_tech_lbcl.malicious.operate_kernel_modules(/pattern/)`

Function	Result	Event type	Examples
`operate_kernel_modules_num`	Returns the number of events of a specific type.	Operates kernel modules.	`dr_sandbox.descr_tech_lbcl.malicious.operate_kernel_modules_num`
`perform_process_tracing(regex)`	Returns the number of events of a specific type.	Performs process tracing. Only the processes that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.perform_process_tracing(/pattern/)`
`perform_process_tracing_num`	Returns the number of events of a specific type.	Performs process tracing.	`dr_sandbox.descr_tech_lbcl.malicious.perform_process_tracing_num`
`remove_self`	Returns the number of events of a specific type.	Deletes itself.	`dr_sandbox.descr_tech_lbcl.malicious.remove_self`
`remove_system_files(regex)`	Returns the number of events of a specific type.	Deletes system files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.remove_system_files(/pattern/)`
`remove_system_files_num`	Returns the number of events of a specific type.	Deletes system files.	`dr_sandbox.descr_tech_lbcl.malicious.remove_system_files_num`
`replace_system_files(regex)`	Returns the number of events of a specific type.	Replaces system files. Only the files that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.replace_system_files(/pattern/)`
`replace_system_files_num`	Returns the number of events of a specific type.	Replaces system files.	`dr_sandbox.descr_tech_lbcl.malicious.replace_system_files_num`
`stops_system_services(regex)`	Returns the number of events of a specific type.	Stops system services. Only the services that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.malicious.stops_system_services(/pattern/)`
`stops_system_services_num`	Returns the number of events of a specific type.	Stops system services.	`dr_sandbox.descr_tech_lbcl.malicious.stops_system_services_num`

Function	Result	Event type	Examples
substitute_application_name_for(regex)	Returns the number of events of a specific type.	Substitutes an application name.	dr_sandbox.descr_tech_lbcl.malicious.substitute_application_name_for(/pattern/)
substitute_application_name_for_num	Returns the number of events of a specific type.	Substitutes an application name.	dr_sandbox.descr_tech_lbcl.malicious.substitute_application_name_for_num

Network activity (the 'network' category)

Function	Result	Event type	Examples
attack_bruteforce_via_ssh	Returns the number of events of a specific type.	Performs a bruteforce attack via the SSH protocol.	dr_sandbox.descr_tech_lbcl.network.attack_bruteforce_via_ssh
attack_bruteforce_via_telnet	Returns the number of events of a specific type.	Performs a bruteforce attack via the TELNET protocol.	dr_sandbox.descr_tech_lbcl.network.attack_bruteforce_via_telnet
attack_bruteforce_via_unk_protocol	Returns the number of events of a specific type.	Performs a bruteforce attack via the undefined protocol.	dr_sandbox.descr_tech_lbcl.network.attack_bruteforce_via_unk_protocol
connect_to(regex)	Returns the number of events of a specific type.	Connects to servers. Only the servers that match the regular expression are counted.	dr_sandbox.descr_tech_lbcl.network.connect_to(/pattern/)
connect_to_num	Returns the number of events of a specific type.	Connects to servers.	dr_sandbox.descr_tech_lbcl.network.connect_to_num
connect_to_irc(regex)	Returns the number of events of a specific type.	Connects to servers over the IRC protocol. Only the servers that match the regular expression are counted.	dr_sandbox.descr_tech_lbcl.network.connect_to_irc(/pattern/)
dns_ask(regex)	Returns the number of events of a specific type.	DNS queries.	dr_sandbox.descr_tech_lbcl.network.dns_ask(/pattern/)

Function	Result	Event type	Examples
`dns_ask_num`	Returns the number of events of a specific type.	DNS queries.	`dr_sandbox.descr_tech_lbcl.network.dns_ask_num`
`http_get(regex)`	Returns the number of events of a specific type.	HTTP GET requests.	`dr_sandbox.descr_tech_lbcl.network.http_get(/pattern/)`
`http_get_num`	Returns the number of events of a specific type.	HTTP GET requests.	`dr_sandbox.descr_tech_lbcl.network.http_get_num`
`http_other(regex)`	Returns the number of events of a specific type.	Other HTTP requests.	`dr_sandbox.descr_tech_lbcl.network.http_other(/pattern/)`
`http_other_num`	Returns the number of events of a specific type.	Other HTTP requests.	`dr_sandbox.descr_tech_lbcl.network.http_other_num`
`http_post(regex)`	Returns the number of events of a specific type.	HTTP POST requests.	`dr_sandbox.descr_tech_lbcl.network.http_post(/pattern/)`
`http_post_num`	Returns the number of events of a specific type.	HTTP POST requests.	`dr_sandbox.descr_tech_lbcl.network.http_post_num`
`listening_port(regex)`	Returns the number of events of a specific type.	Awaits incoming connections on ports. Only the ports that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.network.listening_port(/pattern/)`
`listening_port_num`	Returns the number of events of a specific type.	Awaits incoming connections on ports.	`dr_sandbox.descr_tech_lbcl.network.listening_port_num`
`receive_data_from_server(regex)`	Returns the number of events of a specific type.	Receives data from servers. Only the servers that match the regular expression are counted.	`dr_sandbox.descr_tech_lbcl.network.receive_data_from_server(/pattern/)`
`receive_data_from_server_num`	Returns the number of events of a specific type.	Receives data from servers.	`dr_sandbox.descr_tech_lbcl.network.receive_data_from_server_num`

Function	Result	Event type	Examples
send_data_to_server(regex)	Returns the number of events of a specific type.	Sends data to servers. Only the servers that match the regular expression are counted.	dr_sandbox.descr_tech_lbcl.network.send_data_to_server(/pattern/)
send_data_to_server_num	Returns the number of events of a specific type.	Sends data to servers.	dr_sandbox.descr_tech_lbcl.network.send_data_to_server_num

Other (the 'other' category)

Function	Result	Event type	Examples
collect_cpu_info	Returns the number of events of a specific type.	Collects information about the CPU.	dr_sandbox.descr_tech_lbcl.other.collect_cpu_info
collect_network_info	Returns the number of events of a specific type.	Collects information about the network activity.	dr_sandbox.descr_tech_lbcl.other.collect_network_info
collect_os_info	Returns the number of events of a specific type.	Collects information about the OS.	dr_sandbox.descr_tech_lbcl.other.collect_os_info
collect_ram_info	Returns the number of events of a specific type.	Collects information about RAM.	dr_sandbox.descr_tech_lbcl.other.collect_ram_info
read_info_from_proc_kallsyms	Returns the number of events of a specific type.	Reads information from /proc/kallsyms.	dr_sandbox.descr_tech_lbcl.other.read_info_from_proc_kallsyms

Detects (the 'detects' category)

Function	Result	Event type	Examples
all_detects_here(regexp)	Returns the number of events of a specific type.	All detects.	dr_sandbox.detects.all_detects_here(/Virlock/)
all_detects_here_num	Returns the number of events of a	All detects.	dr_sandbox.detects.all_detects_here_num

Function	Result	Event type	Examples
	specific type.		
`detects_of_allocs(regexp)`	Returns the number of events of a specific type.	Detects of alloc files.	`dr_sandbox.detects.detects_of_allocs(/Virlock/)`
`detects_of_allocs_num`	Returns the number of events of a specific type.	Detects of alloc files.	`dr_sandbox.detects.detects_of_allocs_num`
`detects_of_drops(regexp)`	Returns the number of events of a specific type.	Detects of drops.	`dr_sandbox.detects.detects_of_drops(/Virlock/)`
`detects_of_drops_num`	Returns the number of events of a specific type.	Detects of drops.	`dr_sandbox.detects.detects_of_drops_num`
`detects_of_dumps(regexp)`	Returns the number of events of a specific type.	Detects of dumps.	`dr_sandbox.detects.detects_of_dumps(/Virlock/)`
`detects_of_dumps_num`	Returns the number of events of a specific type.	Detects of dumps.	`dr_sandbox.detects.detects_of_dumps_num`
`detects_of_injects(regexp)`	Returns the number of events of a specific type.	Detects of injects.	`dr_sandbox.detects.detects_of_injects(/Virlock/)`
`detects_of_injects_num`	Returns the number of events of a specific type.	Detects of injects.	`dr_sandbox.detects.detects_of_injects_num`
`detects_of_src(regexp)`	Returns the number of events of a specific type.	Detects of src files.	`dr_sandbox.detects.detects_of_src(/Virlock/)`
`detects_of_src_num`	Returns the number of events of a specific type.	Detects of src files.	`dr_sandbox.detects.detects_of_src_num`

Other functions

Function	Description	Examples
`check_buffer(offset, buffer_asciihex_value)`	Check an asciihex buffer at the specified offset. Length must be even. Can be used instead of 'strings' part, for example, to not slow down the scanning. Returns 1 if the string is found, 0 otherwise.	`dr_sandbox.check_buffer(0,"4d5A")`
`check_byte(offset, byte_value)`	Check bytes at the specified offset. Can be used instead of 'strings' part, for example, to not slow down the scanning. Returns 1 if a value in bytes is found, 0 otherwise.	`dr_sandbox.check_byte(0,0x4d)`
`check_dword(offset, dword_value)`	Check dwords at the specified offset. Can be used instead of 'strings' part, for example, to not slow down the scanning. Returns 1 if a DWORD value is found, 0 otherwise.	`dr_sandbox.check_dword(0,0x00905A4D)`
`check_word(offset, word_value)`	Check words at the specified offset. Can be used instead of the 'strings' part, for example, to not slow down the scanning. Returns 1 if a WORD value is found, 0 otherwise.	`dr_sandbox.check_word(0,0x5a4d)`
`ci_any(string)`	Returns 1 if the case-insensitive ASCII or wide string is found, 0 otherwise.	`dr_sandbox.ci_any("string")`
`ci_any_num(string)`	Returns the number of case-insensitive ASCII or wide strings that are found, 0 otherwise.	`dr_sandbox.ci_any_num("string")`

Function	Description	Examples
`ci_ascii(string)`	Returns 1 if the case-insensitive ASCII string is found, 0 otherwise.	`dr_sandbox.ci_ascii("string")`
`ci_ascii_num(string)`	Returns the number of case-insensitive ASCII strings that are found, 0 otherwise.	`dr_sandbox.ci_ascii_num("string")`
`ci_wide(string)`	Returns 1 if a case-insensitive wide string is found, 0 otherwise.	`dr_sandbox.ci_wide("string")`
`ci_wide_num(string)`	Returns the number of case-insensitive wide strings that are found, 0 otherwise.	`dr_sandbox.ci_wide_num("string")`
`ci_xor(string)`	Returns 1 if the case-insensitive XOR-ed 1-byte ASCII string is found, 0 otherwise.	`dr_sandbox.ci_xor("string")`
`ci_xor_num(string)`	Returns the number of case-insensitive XOR-ed 1-byte ASCII strings that are found, 0 otherwise.	`dr_sandbox.ci_xor_num("string")`
`crc32(integer, integer)`	Calculates and returns the crc32 hash of the buffer. The first parameter is the offset, and the second parameter is the length of the buffer.	`dr_sandbox.crc32(0, 0)`
`cs_any(string)`	Returns 1 if the case-sensitive ASCII or wide string is found, 0 otherwise.	`dr_sandbox.cs_any("string")`
`cs_any_num(string)`	Returns the number of case-sensitive ASCII or wide strings that are found, 0 otherwise.	`dr_sandbox.cs_any_num("string")`
`cs_ascii(string)`	Returns 1 if the case-sensitive ASCII string is found, 0 otherwise.	`dr_sandbox.cs_ascii("string")`
`cs_ascii_num(string)`	Returns the number of case-sensitive ASCII strings that are found, 0 otherwise.	`dr_sandbox.cs_ascii_num("string")`

Function	Description	Examples
`cs_wide(string)`	Returns 1 if the case-sensitive wide string is found, 0 otherwise.	`dr_sandbox.cs_wide("string")`
`cs_wide_num(string)`	Returns the number of case-sensitive wide strings that are found, 0 otherwise.	`dr_sandbox.cs_wide_num("string")`
`detects_of_this_file(regex)`	Returns the number of detects on a scanned file.	`dr_sandbox.detects_of_this_file(/Virlock/) == 0`
`detects_of_this_file_num`	Returns the number of detects on a scanned file.	`dr_sandbox.detects_of_this_file_num`
`filename(regex)`	Returns 1 if the regular expression is found in the file name, 0 otherwise.	`dr_sandbox.filename(/xtbl/)`
`filename_boost_regex(string_with_regex)`	Search for a regular expression in a file name using `boost::regex`. Flags for regex: `boost::regex::perl`. Search by `boost::regex_search`. Can be used if you need regex features like negative lookahead or backreferences, which are not supported in the YARA regex. Note that invalid regex will slow down the scanning. Moreover, `boost::regex` is slower than the YARA regex, it's recommended to use `dr_sandbox.filename(//)` if possible. Returns 1 if the regular expression is found, 0 otherwise.	`dr_sandbox.filename_boost_regex(“(?<!abc)def”)`
`filesystem_access(regex)`	The high-level function, which matches all filesystem operations to the regular expression.	`dr_sandbox.filesystem_access(/AnnaKournikova\.jpg\.vbs/)`
`network_access(re`	The high-level function, which matches all network	`dr_sandbox.network_access(/\.php\?id=[0-9]+&token=[0-9]+/)`

Function	Description	Examples
`gex)`	operations to the regular expression.	
`registry_access(regex)`	Returns the number of actions with a registry.	`dr_sandbox.registry_access(/pattern/)`
`sb_filetype`	Returns a file type. Used for comparing with the following `SB_FILETYPE_*` constants: `SB_FILETYPE_SRC`; `SB_FILETYPE_DROP`; `SB_FILETYPE_MEMDMP`; `SB_FILETYPE_ALLOC`; `SB_FILETYPE_DUMP`; `SB_FILETYPE_INJECT`.	`dr_sandbox.sb_filetype == dr_sandbox.SB_FILETYPE_SRC`
`search_substring_in_range(string, integer, integer)`	Search for the substring in the buffer using the Boyer–Moore algorithm. The first argument is the asciihex string, the second parameter is the offset, and the third parameter is the length. Use it carefully because it's not performance free.	`dr_sandbox.search_substring_in_range("string", 0, 0)`

17. Appendix C. Configuring a separate VPN server

Command examples for CentOS are listed below. For other OS use equivalent commands.

To configure a separate VPN server

1. Switch to account with administrative access to the system:

```
$ su
```

2. Install EPEL repository:

```
# yum install epel-release
```

3. Install OpenVPN and Easy-RSA utility:

```
# yum install openvpn easy-rsa
```

4. Change to the directory with installed Easy-RSA utility:

```
# cd /usr/share/easy-rsa/3
```

5. Create PKI key infrastructure:

```
# ./easyrsa init-pki
```

6. Create root certificate authority (CA):

```
# ./easyrsa build-ca
```

7. At the request Enter New CA Key Passphrase, set a password for signing certificates.
8. Generate a certificate request for the server without using a password:

```
# ./easyrsa gen-req server nopass
```

9. Sign a CA request:

```
# ./easyrsa sign-req server server
```

10. Enter the password from CA if it was set earlier.
11. Generate Diffie-Hellman key:

```
# ./easyrsa gen-dh
```

12. Copy created files to OpenVPN server directory:

```
# cp pki/ca.crt /etc/openvpn/ca.crt

# cp pki/dh.pem /etc/openvpn/dh.pem
# cp pki/issued/server.crt /etc/openvpn/server.crt

# cp pki/private/server.key /etc/openvpn/server.key
```

13. Generate TLS Control Channel encryption key:

```
# openvpn --genkey --secret /etc/openvpn/tc.key
```

14. Generate keys for OpenVPN server client:

```
# ./easyrsa gen-req vxcube nopass

# ./easyrsa sign-req client vxcube
```

15. Copy client keys (`vxcube.key`, `vxcube.crt`) and server key (`ca.crt`) to the directory with Dr.Web vxCube distribution kit (directory `~/confs`) from the following directories:

```
# /usr/share/easy-rsa/3/pki/private/vxcube.key

# /usr/share/easy-rsa/3/pki/issued/vxcube.crt

# /etc/openvpn/ca.crt
```

16. Create OpenVPN config file:

```
nano /etc/openvpn/server/server.conf
```

Values:

```
port 1194
proto udp
dev tap
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh.pem
server 10.42.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 10 120
comp-lzo
user nobody
group nobody
```

```
persist-key
persist-tun
status openvpn-status.log
log-append /var/log/openvpn.log
verb 1
```

17. Start the server:

```
# systemctl start openvpn-server@server.service
```

18. Make sure that server is running:

```
# netstat -tulnp | grep 1194
```

19. Make sure that server has IP forwarding enabled:

```
# nano /etc/sysctl.conf
```

Add string:

```
net.ipv4.ip_forward = 1
```

20. Force re-read the configuration of sysctl:

```
# sysctl -p /etc/sysctl.conf
```

21. Make sure that there are no other services accepting connections from the external interface or access to them is blocked by the system firewall settings:

```
# netstat -nlpt
```

22. If there are such services, add a rule to block access to them from a VPN tunnel:

```
# iptables -A INPUT -i tap0 -j DROP
```

23. Configure masquerading for packets from a subnet of a VPN tunnel to the default interface:

```
# iptables -t nat -A POSTROUTING -s 10.42.0.0/24 -o eth0 -j
MASQUERADE
```

18. Appendix D. List of network ports used by components

If all components are on the same server, they communicate locally, and you will only have to open port 80 (for HTTP) and/or port 443 (for HTTPS).

If the components are on different servers, then for them to communicate, you need to open the following ports:

vxCube Web (vxcube_web_host), in:

- 80 (for HTTP)
- 443 (for HTTPS)
- 21 (storage, ONLY for other nodes), out:
- hyperbox_api_host:5003

vxCube DB (hyperbox_api_host), in:

- 25672 (RabbitMQ, inter-node communication)
- 4369 (RabbitMQ, peer discovery service)
- 5672 (RabbitMQ, AMQP)
- 5003 (vxcube flow api app), out:
- vxcube_web_host:21

Windows/Android/Linux Sandbox Service (hyperbox_hosts, dimas_hosts, linuxbox_hosts), out:

- hyperbox_api_host:25672
- hyperbox_api_host:4369
- hyperbox_api_host:5672
- vxcube_web_host:21
- vpn_server:vpn_port (EXTERNAL, redirect traffic from sandboxes)
- proxy_server:proxy_port (EXTERNAL, depends on analysis settings)

Dr.Web Scan Service (drweb_srv_hosts), out:

- hyperbox_api_host:25672
- hyperbox_api_host:4369
- hyperbox_api_host:5672
- vxcube_web_host:21
- update.geo.drweb.com:80 (EXTERNAL, AV updates)

Yara Service (yara_hosts), out:

- hyperbox_api_host:25672
- hyperbox_api_host:4369
- hyperbox_api_host:5672
- vxcube_web_host:21

Analyser Service (evparser_hosts), out:

- hyperbox_api_host:25672
- hyperbox_api_host:4369
- hyperbox_api_host:5672
- vxcube_web_host:21
- links-checker.dev.drweb.com:80 (EXTERNAL, optional, domain checker)