

Testoodo SRL

We play with cybersec.

Our job

- Malware analysis
- High Interaction Passive Defensive Systems - Honeypot
- Cybersec R&D
- Penetration Testing
- Cyberspace surveillance

Our product: H.A.T.E.

Honey-pot-based Analysis Threat Engine

- Is a distributed system. Each instance is a core. Cores are coordinated by a control center.
- Each core schedules honeypot based on real operating systems. Once the attacker instantiates a connection he gains its own sandbox (of course for a limited amount of time). Subsequent connections from the same IP are redirected to the same sandbox.
- Network, File System, Process Execution and Console operations are tracked and stored.
- Each one of the previous is a specialized probe which can be injected into the system on demand. Probes can be written in any programming language.

Realtime sandbox monitoring

H. A. T. E. sandbox instances

All cores (3) - 3 running, 0 stopped, 0 error.

Running sandboxes: 8 (all cores)

Name	Core	Started at	OS	Attacker infos	Activity	Probes	Address	Remaining lifetime (seconds)	Force kill
TELNET_4	hulk	02/28/2017 (12:26:23)	linux x86_64	Address: [redacted] (1 live connection)	Filesystem: 0 Binaries: 0 Network: 0 Process: 59 Shell: 0	Process Network Filesystem Shell FilesystemExtractor	10.10.0.40	34.529% 103 seconds	Kill
TELNET_4	redskull	02/28/2017 (12:28:41)	linux x86_64	Address: [redacted] (1 live connection)	Filesystem: 0 Binaries: 0 Network: 0 Process: 0 Shell: 0	Process Network Filesystem Shell FilesystemExtractor	10.10.0.39	60.548% 241 seconds	Kill
TELNET_4	daredevil	02/28/2017 (12:28:42)	linux x86_64	Address: [redacted] (2 live connections)	Filesystem: 0 Binaries: 0 Network: 54 Process: 60 Shell: 0	Process Network Filesystem Shell FilesystemExtractor	10.10.0.33	60.591% 242 seconds	Kill
TELNET_4	hulk	02/28/2017 (12:28:52)	linux x86_64	Address: [redacted] (1 live connection)	Filesystem: 0 Binaries: 0 Network: 0 Process: 59 Shell: 0	Process Network Filesystem Shell FilesystemExtractor	10.10.0.40	64.196% 252 seconds	Kill
TELNET_4	daredevil	02/28/2017 (12:29:04)	linux x86_64	Address: [redacted] (1 live connection)	Filesystem: 6 Binaries: 0 Network: 169 Process: 119 Shell: 1	Process Network Filesystem Shell FilesystemExtractor	10.10.0.33	68.225% 264 seconds	Kill
TELNET_4	hulk	02/28/2017 (12:29:19)	linux x86_64	Address: [redacted] (1 live connection)	Filesystem: 0 Binaries: 0 Network: 0 Process: 59 Shell: 0	Process Network Filesystem Shell FilesystemExtractor	10.10.0.40	69.186% 279 seconds	Kill
TELNET_4	daredevil	02/28/2017 (12:29:26)	linux x86_64	Address: [redacted] (1 live connection)	Filesystem: 0 Binaries: 0 Network: 0 Process: 0 Shell: 0	Process Network Filesystem Shell FilesystemExtractor	10.10.0.33	95.558% 286 seconds	Kill
TELNET_4	hulk	02/28/2017 (12:29:44)	linux x86_64	Address: [redacted] (1 live connection)	Filesystem: 0 Binaries: 0 Network: 0 Process: 58 Shell: 0	Process Network Filesystem Shell FilesystemExtractor	10.10.0.40	101.629% 304 seconds	Kill

Attacks storing and retrieving

The screenshot displays the H.A.T.E. sandboxes history interface. At the top, it shows 'H. A. T. E. sandboxes history' and 'All cores (3)'. Below this, there's a section for 'Sandboxes history (12094 sandboxes in repository) (all cores)'. A sidebar on the left lists instances by date, with 'February 2017' expanded to show a list of dates from Thursday 9 to Tuesday 28. The main area is titled 'Inspecting 1488276871-23004.' and contains two buttons: 'Download TAR archive' and 'Delete sandbox from repository'. Below these are tabs for 'Instance details', 'Shell logs', and 'Network logs'. The 'Shell logs' tab is active, showing 'Session 102 (5 commands)' with a list of 'enable' commands for various system services. The output shows the system prompt and a 'command not found' error for '/bin/sh'. Below this, 'Session 65445335 (5 commands)' is partially visible.

Sandboxes history (12094 sandboxes in repository) (all cores)

Repository filters

Instances

- February 2017
 - Thursday 9
 - Friday 10
 - Monday 13
 - Tuesday 14
 - Wednesday 15
 - Friday 17
 - Saturday 18
 - Sunday 19
 - Monday 20
 - Tuesday 21
 - Wednesday 22
 - Thursday 23
 - Friday 24
 - Saturday 25
 - Sunday 26
 - Monday 27
 - Tuesday 28
 - 1488273144-22405
 - 1488274962-22624
 - 1488274945-22615
 - 1488276844-22993
 - 1488276871-23004
 - 1488276951-1462
 - 1488276991-1500
 - 1488277043-1506
 - 1488277063-1512
 - 1488276893-23010
 - 1488277059-954
 - 1488277081-967
 - 1488277091-1519
 - 1488277036-23063
 - 1488277102-23070
 - 1488277130-23077
 - 1488277099-973
 - 1488277326-1538
 - 1488277190-23082
 - 1488277349-1544
 - 1488277371-1550
 - 1488277392-1558
 - 1488277313-23087
 - 1488277413-1565
 - 1488277361-23092
 - 1488277254-978
 - 1488277435-1571
 - 1488277385-23097

Inspecting 1488276871-23004.

Download TAR archive Delete sandbox from repository

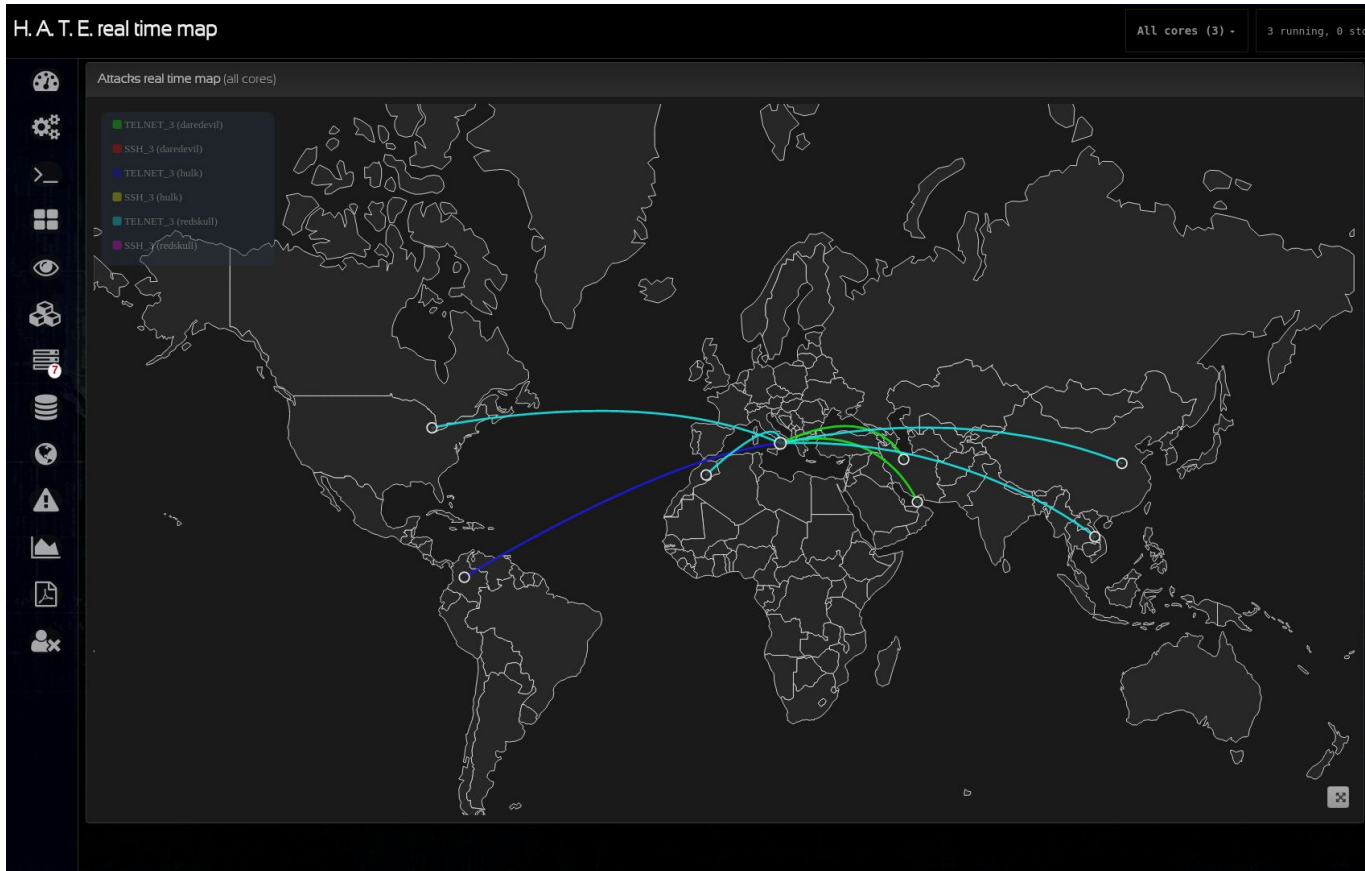
Instance details Shell logs Network logs

Session 102 (5 commands)

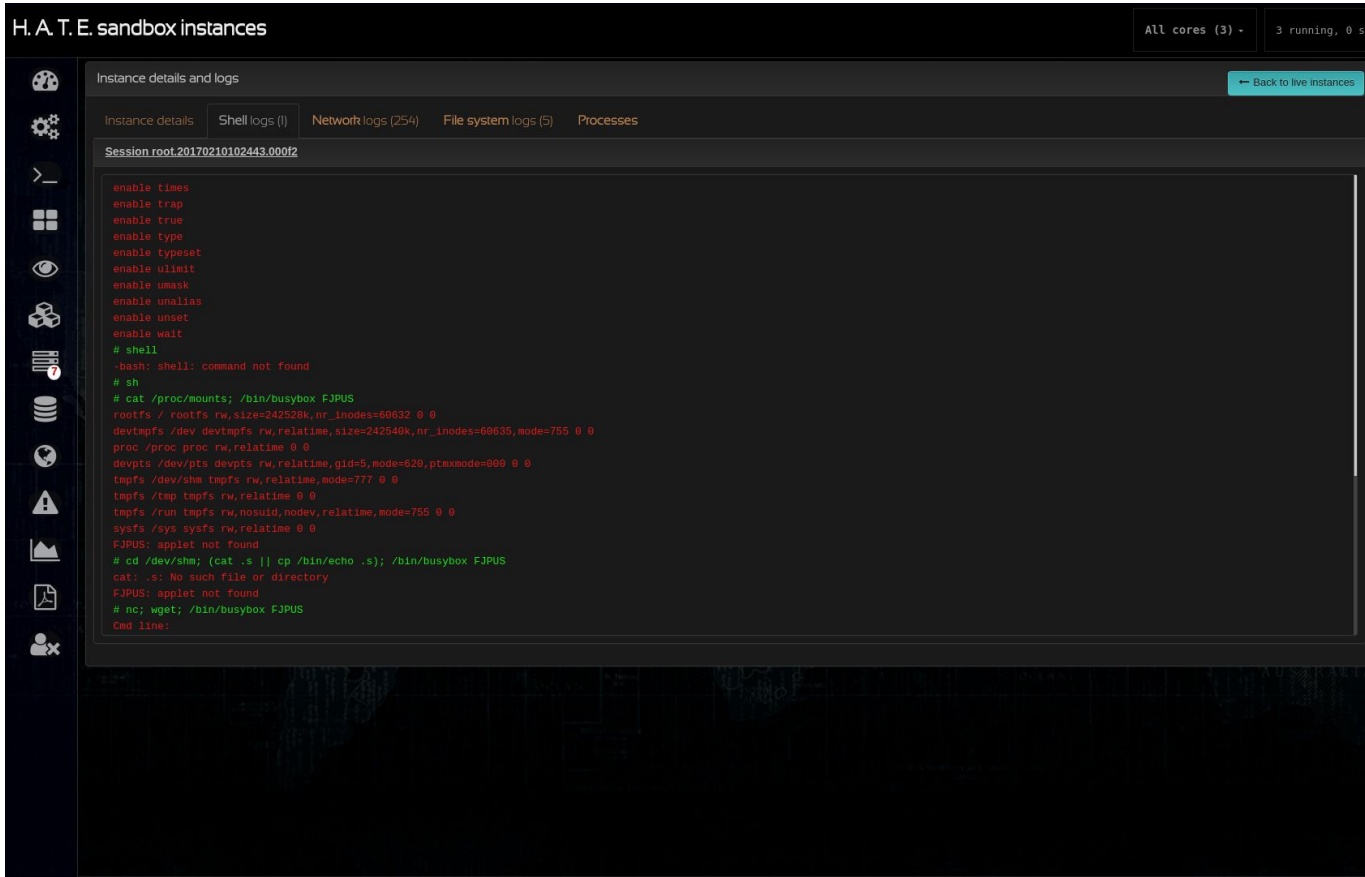
```
enable ltr
enable local
enable logout
enable mailFile
enable popd
enable printf
enable psnls
enable pwd
enable read
enable readarray
enable readonly
enable return
enable set
enable shift
enable sleep
enable source
enable suspend
enable text
enable times
enable trap
enable true
enable type
enable typeset
enable ulimit
enable umask
enable unalias
enable unset
enable wait
Tue Feb 28 2017 11:10:14 GMT+0100 (CET): system
/bin/sh: system: command not found
Tue Feb 28 2017 11:10:14 GMT+0100 (CET): shell
Tue Feb 28 2017 11:10:14 GMT+0100 (CET): sh
Tue Feb 28 2017 11:19:14 GMT+0100 (CET): /bin/busybox MERA!
```

Session 65445335 (5 commands)

Realtime worldwide map of attacks



*Nix Console Monitoring and logging



The screenshot displays a web-based interface for monitoring Nix sandbox instances. The top header shows "H. A. T. E. sandbox instances" and status indicators for "All cores (3)" and "3 running, 0 st". The main content area is titled "Instance details and logs" and includes a "Back to live instances" button. Below this, there are tabs for "Instance details", "Shell logs (1)", "Network logs (254)", "File system logs (5)", and "Processes". The "Shell logs" tab is active, showing a session for "root.20170210102443.000f2". The log output is as follows:

```
enable times
enable trap
enable true
enable type
enable typeset
enable ulimit
enable umask
enable unalias
enable unset
enable wait
# shell
-bash: shell: command not found
# sh
# cat /proc/mounts; /bin/busybox FJPUS
rootfs / rootfs rw,size=242528k,nr_inodes=60632 0 0
devtmpfs /dev devtmpfs rw,relatime,size=242540k,nr_inodes=60635,mode=755 0 0
proc /proc proc rw,relatime 0 0
devpts /dev/pts devpts rw,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /dev/shm tmpfs rw,relatime,mode=777 0 0
tmpfs /tmp tmpfs rw,relatime 0 0
tmpfs /run tmpfs rw,nosuid,nodev,relatime,mode=755 0 0
sysfs /sys sysfs rw,relatime 0 0
FJPUS: applet not found
# cd /dev/shm; (cat .s || cp /bin/echo .s); /bin/busybox FJPUS
cat: .s: No such file or directory
FJPUS: applet not found
# nc; wget; /bin/busybox FJPUS
Cmd line:
```

Filesystem actions tracking

H. A. T. E. sandboxes history

All cores (3) + 3 running, 0 stopped, 0 error.

Sandboxes history (82 sandboxes in repository) (all cores)

Repository filters

Instances

- February 2017
 - Thursday 9
 - Friday 10
 - Friday 17
 - Sunday 19
 - Monday 20
 - Tuesday 21
 - Thursday 23
 - Friday 24
 - 1487912446-13371
 - 1487916496-13747
 - 1487917172-13780
 - 1487930092-14318
 - 1487938010-11861
 - 1487958186-12585
 - 1487958282-4314
 - 1487958673-16022
 - 1487958917-12615
 - Saturday 25
 - Monday 27

Inspecting: 1487917172-13780

Download TAR archive Delete sandbox from repository

Instance details Shell logs Network logs **Filesystem logs** Dropped binaries

0 file(s) available.

Download file

	07:20:29	07:20:30
	000 050 100 150 200 250 300 350 400 450 500 550 600 650 700 750 800 850 900 950 000	
/tmp/.ptmx	MODIFY*2 CREATE*3	
/dev/shm/.ptmx		
/root/manjaro		MODIFY*ATTRIB*1
	000 050 100 150 200 250 300 350 400 450 500 550 600 650 700 750 800 850 900 950 000	
	07:20:29	07:20:30

Download and view the downloaded malware

The screenshot displays the H.A.T.E. sandboxes history interface. At the top, the title is "H. A. T. E. sandboxes history". On the right side of the header, there are two status boxes: "All cores (3)" and "3 running, 0 stopped, 0 error.". Below the header, the main content area is titled "Sandboxes history (82 sandboxes in repository) [all cores]".

On the left side, there is a sidebar with a navigation menu. The "Instances" section is expanded, showing a list of dates from February 2017. The date "Friday 24" is selected, and a list of instance IDs is shown below it. The instance ID "1487930092-14318" is highlighted in blue.

The main content area shows the details for the selected instance "Inspecting: 1487930092-14318". At the top of this section, there are two buttons: "Download TAR archive" and "Delete sandbox from repository". Below these buttons, there are four tabs: "Instance details", "Shell logs", "Network logs", "Filesystem logs", and "Dropped binaries". The "Dropped binaries" tab is currently selected.

The "Dropped binaries" list contains the following entries:

- apache2
- bash
- cron
- ftp
- ntpd
- openssh
- pftp
- sh
- sshd
- sshd.1
- fttp
- wget
- wget.1

Lot of other features.
If you are curious contact us.