MALWARE

What is a Malware ?

- Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems

In general it is called as ‘Bug’ or ‘Virus’

Basic Purpose Of Any Malware

- Malware can be used against individuals to gain information such as personal identification numbers or details, bank or credit card numbers, and passwords.

- Malware is used broadly against government or corporate websites to gather guarded information or to disrupt their operation in general.

- As a Security analyst, you will often analyze suspicious files in your daily work routine. With the Malware fundamentals training, the necessary basic information will be learned by introducing the subject of malware analysis.

We will get to know ;

- Definition of malware
- Malware types
- Malware analysis approaches
- How to analyze suspicious files.

How Malware Analysis Help Security Analysts

Have you ever heard of Stuxnet before?

The US and Israeli intelligence services created Stuxnet to disrupt Iran's nuclear work.

This malware, which was first detected in 2010, still has a complex structure even today.

Although it contains many zero-day vulnerabilities, it provides propagation with USB devices.

This malware damaged Iran’s Natanz uranium enrichment plants and caused it to be closed permanently.

HOW STUXNET WORKED

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

- As you can see in the Stuxnet example, even if you are not very close to technology in your life, the impact of malware on our lives is quite high.

- What about the importance of malwares in Security for a person who wants to be a security analyst?

- When you examine the work routine of a standard Security Analyst, you will see that the analysts frequently encounter suspicious files or processes.

- Considering that malware is used in the vast majority of cyber attacks, you can understand that this information is not unusual.

- As a Security Analyst, you should be able to analyze and figure out whether these files are harmful; and, if it is malicious, you should understand the purpose of this software and how it communicates with the command and control servers.

- It is an undeniable fact that malware analysis is an indispensable know-how for Security Analysts.

- Many malware analysis methods and techniques are available to examine suspicious files.

- you can analyze malware using the most appropriate technique for your needs.

Malware Definition and Malware Types

- The word Malware is a word derived from the words **Malicious software.**
- It is the name given to software that endangers the security and integrity of systems by targeting a malicious purpose.
- Today, cyber threat actors use malicious software to achieve various purposes such as ensuring persistence, damaging systems, demanding ransom.
- As Security analyst, we need to analyze suspicious software and understand whether the software is really harmful.

- Since there is no restriction, you can come across malicious software written in almost all programming languages.

- You don't need to know all programming languages to start analyzing malware. However, we can say that being familiar with programming makes it easy to analyze malicious software (it is even mandatory in matters such as reverse engineering).

- With each passing day, we see that cyber threat actors develop themselves and develop more complex malware.

- Attackers now use various methods to make analysis of their malicious software even more difficult.

- Since these methods are at an advanced level, they will not be explained in the "Malware Fundamentals" training, and a special training will be prepared for these methods.

- In this process, we must constantly improve ourselves in order to be prepared for current threats.
- As a Security analyst, you will encounter many suspicious files in your daily work routine.
- These files may have come via email, or may have been detected by the antivirus software on the user device, or they may have been detected by the network security products while being transferred.
- As a result of the analysis, you will be able to find whether the file is harmful or not; and its purpose if it is harmful, the command and control servers and the type of the malware.

Malware Types

- Although the names of the command and control servers and the methods they use vary, the purposes of malicious software are within certain categories. In this way, you can inform the other person about what the malware is doing by simply telling the category of the malware.

- **For example,** if you say that the software you are examining is a keylogger, everyone will know that this is a software that records and plays the keys pressed on the keyboard. You may provide this important initial information about the malware to your upper management to give the idea about it and the attacker's target then follow up with the detailed analysis report.

As we mentioned, malicious software are divided into types according to their functions/purposes/characters. After analyzing the malware, you will match it with one of the following types. Therefore, you should know what these types are.

Some types of malware and their descriptions are as follows.

- Backdoor
- Adware
- Ransomware
- Virus
- Worm
- Rootkit
- RAT (Remote Access Trojan)
- Banking malware
- Keylogger

Backdoor: Leaving a backdoor on the device where the malware is installed, it allows the attacker to access the system through this backdoor. For example, by opening a network port connected to the shell, it enables the attacker to connect to the system through this port.

Adware: It often comes with downloaded software, causing unwanted advertisements to be displayed on the device. While not all adware is harmful, some change the default search engine.

Ransomware: It is a type of malware that has been on the world agenda for the last few years. It demands ransom from people by encrypting and exfiltrating all files on the device.

Virus: It is one of the first types of malware seen in the wild. So we see that in daily life, it is often called a virus instead of the term malware. Viruses have a self-replicate feature. It provides persistence by infecting other files on the device.

Worm: Since this type of malware spreads from infected devices to other devices, it is named worm. WannaCry, a worm malware exploiting MS17-010 vulnerability, caused panic around the world.

Rootkit: It is a type of malware that disguises itself by providing access to a high level of authority on the device.

RAT (Remote Access Trojan): It is a type of malware that provides full control over the device to the threat actor.

Banking malware: A type of malware that targets banking applications and causes money to be stolen from the victim.

Keylogger: A type of malware that logs pushed keys and send this information to attacker.

A malware may contain more than one feature, so a malware can belong to more than one type. For example, WannaCry malware includes both worm and ransomware malware features.

Cryptography

- Many technologies make use of cryptography to provide security. It is also used by attackers for purposes such as complicating, preventing detection and preventing access.

- Popular ransomware uses cryptography nowadays to encrypt files and prevent access to files without paying a ransom.

- We often encounter cryptography during malware analysis.

Which Approach Should You Choose When Analyzing Malware?

If you work in the defensive field, analyzing malware becomes part of your job.

Now we will discuss with which approaches you can analyze malware and the advantages / disadvantages of these approaches to each other.

There are 2 different approaches to analyzing malware.

- **Static Analysis**
- **Dynamic Analysis**

What is Static Analysis?

- It is the approach of analyzing malicious software by reverse engineering methods without running them.

- Generally, by decompile / disassemble the malware, each step that the malware will execute is analyzed, hence the behavior / capacity of the malware can be analyzed.

Your device will not be infected as you do not run malicious software in static analysis. (However, we do not recommend performing static analysis on your host device, it will be more proper to do your analysis in a virtual operating system.)

The information examined during the static analysis is as follows.

P.E. (Portable Executable) Headers

Imported DLL's

Exported DLL's

Strings in binary

CPU Instructions

What is Dynamic Analysis?

It is the approach that examines the behavior of malicious software on the system by running it.

In dynamic analysis, applications that can examine registry, file, network and process events are installed in the system, and their behavior is examined by running malicious software.

While doing dynamic analysis, you should carefully examine the following events.

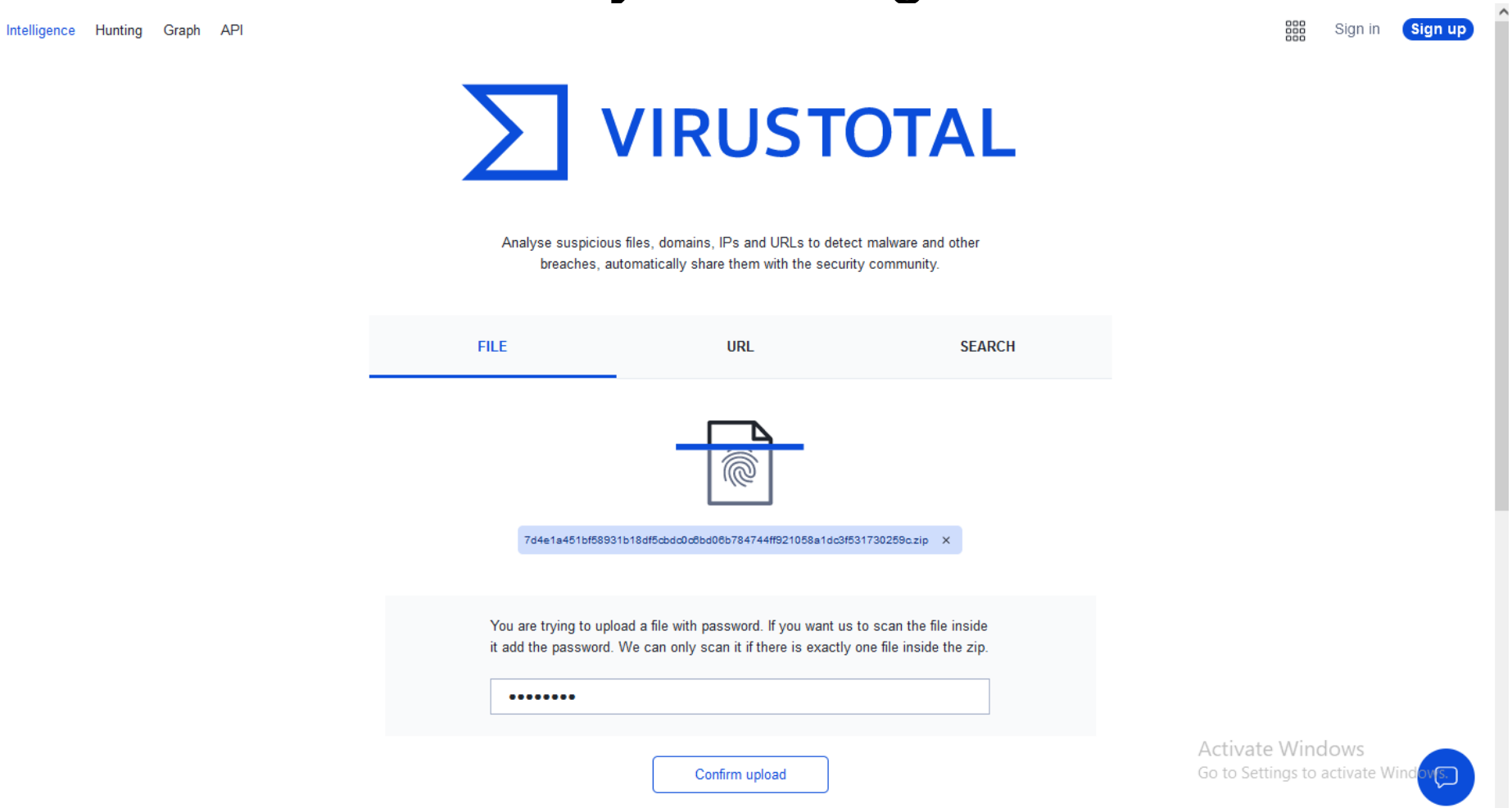
- Network Connections
- File Events
- Process Events
- Registry Events

Static Analysis vs Dynamic Analysis

Which approach to use when analyzing malware depends on the current circumstances. In cases where you want to get fast results, you can choose dynamic analysis, but we cannot say that the analysis is complete without doing both static and dynamic analysis.

It should also be noted that using only one approach may not be sufficient to analyze malware. Using both approaches together will lead you to victory!

Static Analysis Using VirusTotal



41 / 61

Community Score

41 security vendors and no sandboxes flagged this file as malicious

7d4e1a451bf58931b18df5cbdc0c6bd06b784744ff921058a1dc3f531730259c
7d4e1a451bf58931b18df5cbdc0c6bd06b784744ff921058a1dc3f531730259c.rar
rar

60.58 KB
Size

2022-11-30 09:51:04 UTC
1 minute ago

RAR

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Security Vendors' Analysis

AhnLab-V3	Malware/Win32.RL_Generic.R368070	ALYac	Gen:Variant.Fugrafa.5911
Antiy-AVL	Trojan/Win32.DiskWriter	Arcabit	Trojan.Fugrafa.D1717
Avast	MBR:Ransom-C [Trj]	AVG	MBR:Ransom-C [Trj]
Avira (no cloud)	TR/Petya.vmdsd	BitDefender	Gen:Variant.Fugrafa.5911
BitDefenderTheta	Gen:NN.ZelphiF.36106.sGX@aO6sNSc	ClamAV	Win.Ransomware.Petya-6992434-0
Cynet	Malicious (score: 99)	Cyren	W32/Injector.PEQY-5235
DrWeb	Trojan.Siggen7.57150	Emsisoft	Gen:Variant.Fugrafa.5911 (B)
eScan	Gen:Variant.Fugrafa.5911	ESET-NOD32	Win32/Diskcoder.Petya.A
Fortinet	W32/Petya.Altr.ransom	GData	Gen:Variant.Fugrafa.5911
Google	Detected	Gridinsoft (no cloud)	Ransom.Win32.Blocker.oa!s1
Ikarus	Trojan.Win32.Diskcoder	K7AntiVirus	Trojan (004e19001)

Microsoft	Ransom:Win32/Petya.A	NANO-Antivirus	Trojan.Win32.Diskcoder.fhbqwx
Rising	Ransom.MBBlocker!8.31B7 (TFE:3:wH...	Sangfor Engine Zero	Ransom.Win32.Petya.V56f
Sophos	ML/PE-A	Symantec	Trojan.Gen.NPE
Tencent	Win32.Trojan.Petr.Aujl	Trellix (FireEye)	Gen:Variant.Fugrafa.5911
TrendMicro	Ransom_Petya.R002C0CGP22	TrendMicro-HouseCall	Ransom_Petya.R002C0CGP22
VIPRE	Gen:Variant.Fugrafa.5911	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	Baidu	Undetected
Bkav Pro	Undetected	CMC	Undetected
Comodo	Undetected	F-Secure	Undetected
Jiangmin	Undetected	Kingsoft	Undetected
Panda	Undetected	QuickHeal	Undetected
SentinelOne (Static ML)	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	VBA32	Undetected
ViRobot	Undetected	Yandex	Undetected
Zillya	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	VirIT	Timeout
Alibaba	Unable to process file type	Avast-Mobile	Unable to process file type
BitDefenderFalx	Unable to process file type	CrowdStrike Falcon	Unable to process file type

?

Community Score

41 security vendors and no sandboxes flagged this file as malicious

7d4e1a451bf58931b18df5cbdc0c6bd06b784744ff921058a1dc3f531730259c

7d4e1a451bf58931b18df5cbdc0c6bd06b784744ff921058a1dc3f531730259c.rar

rar

60.58 KB
Size

2022-11-30 09:51:04 UTC
1 minute ago

RAR

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Basic Properties

MD5	c1eae1005deaf0a83cff5185fc8045b8
SHA-1	40a18c00c9f4f471792d88b2bded52aaff41c810
SHA-256	7d4e1a451bf58931b18df5cbdc0c6bd06b784744ff921058a1dc3f531730259c
SSDEEP	1536:PCeyxgsCFqX4MREQDBLmbl8cGSlVjh5f4nHhW:Pfyjv4ANqCrhuHo
TLSH	T12D5302934C7A96B541086E2E7955BAEC3FF7E096CCDA30CF271A075A7C4B8A2C019875
File type	RAR
Magic	RAR archive data, v84, os: Unix
TrID	RAR compressed archive (v5.0) (61.5%) | RAR compressed archive (gen) (38.4%)
File size	60.58 KB (62032 bytes)

History

First Submission	2022-07-16 20:10:49 UTC
Last Submission	2022-11-30 09:51:04 UTC
Last Analysis	2022-11-30 09:51:04 UTC

Names

7d4e1a451bf58931b18df5cbdc0c6bd06b784744ff921058a1dc3f531730259c.rar

Fast Dupe.rar

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

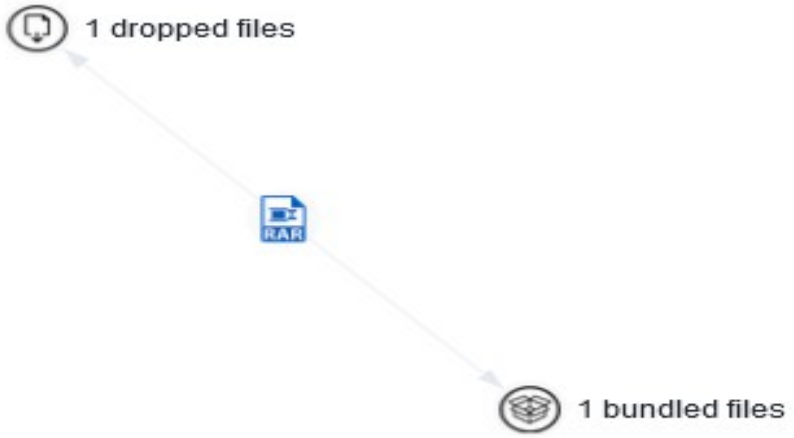
Bundled Files (1)

Scanned	Detections	File type	Name
2022-07-16	46 / 69	Win32 EXE	Fast Dupe.exe

Dropped Files (1)

Scanned	Detections	File type	Name
2022-07-16	46 / 69	Win32 EXE	Fast Dupe.exe

Graph Summary



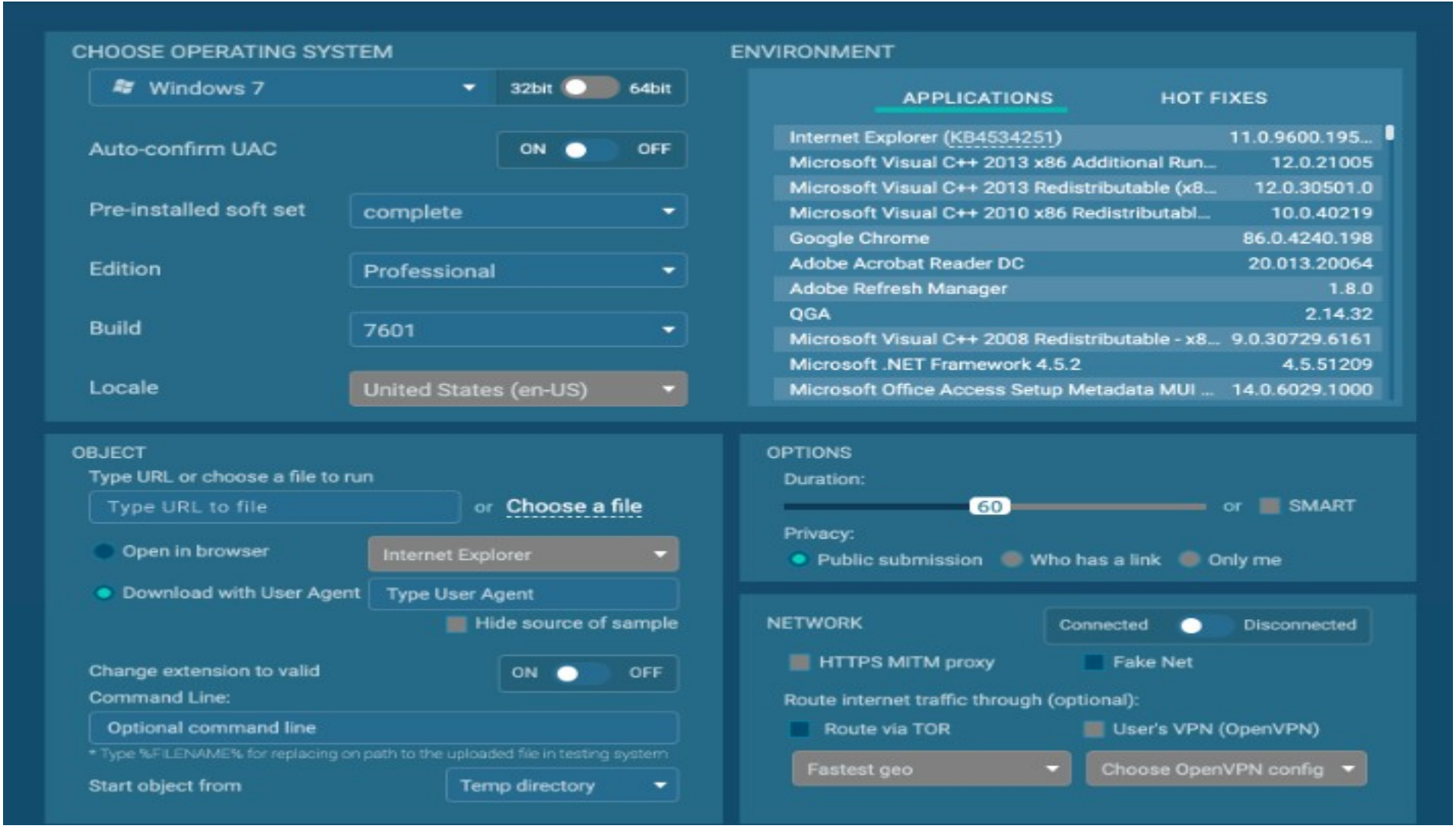
Dynamic Analysis Using AnyRun

You can take advantage of sandbox services / products to quickly analyze malware.

AnyRun is an interactive sandbox that you can use when you want to analyze malware quickly.

AnyRun has options for paid or free use. If you want to take advantage of it for free, all your analysis is visible to others, therefore we do not recommend that you upload files that may contain personal data to AnyRun. In addition, the free plan has restrictions such as usage time.

How can we use AnyRun for our malware analysis, what kind of outputs we can get, let's examine it together.

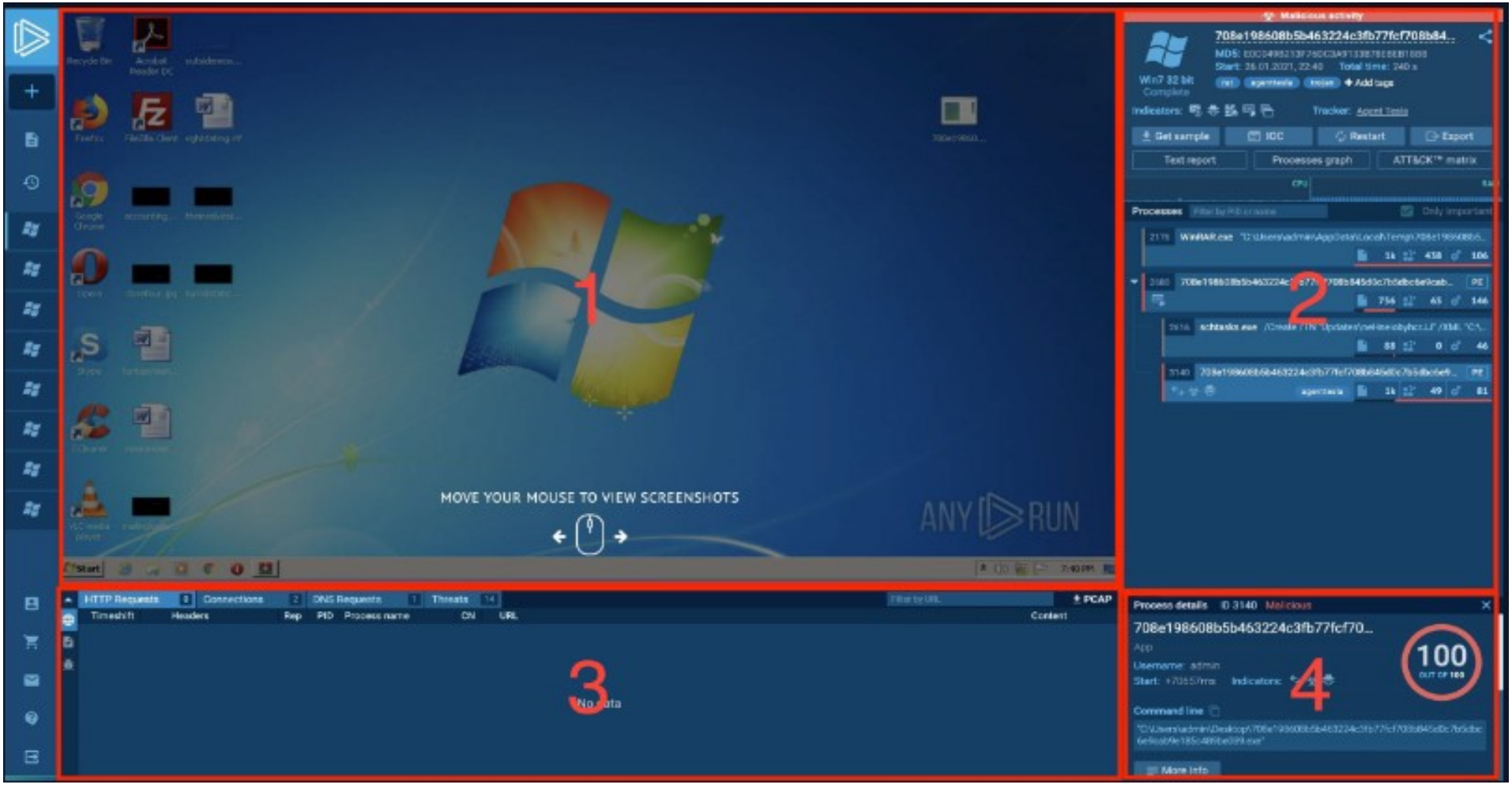

CHOOSE OPERATING SYSTEM
Windows 7
32bit
64bit
Auto-confirm UAC
ON
OFF
Pre-installed soft set
complete
Edition
Professional
Build
7601
Locale
United States (en-US)
ENVIRONMENT
APPLICATIONS
HOT FIXES
Internet Explorer (KB4534251) 11.0.9600.195...
Microsoft Visual C++ 2013 x86 Additional Run... 12.0.21005
Microsoft Visual C++ 2013 Redistributable (x8... 12.0.30501.0
Microsoft Visual C++ 2010 x86 Redistributabl... 10.0.40219
Google Chrome 86.0.4240.198
Adobe Acrobat Reader DC 20.013.20064
Adobe Refresh Manager 1.8.0
QGA 2.14.32
Microsoft Visual C++ 2008 Redistributable - x8... 9.0.30729.6161
Microsoft .NET Framework 4.5.2 4.5.51209
Microsoft Office Access Setup Metadata MUI ... 14.0.6029.1000
OBJECT
Type URL or choose a file to run
Type URL to file
or
Choose a file
Open in browser
Internet Explorer
Download with User Agent
Type User Agent
Hide source of sample
Change extension to valid
ON
OFF
Command Line:
Optional command line
* Type %FILENAME% for replacing on path to the uploaded file in testing system
Start object from
Temp directory
OPTIONS
Duration:
60
or
SMART
Privacy:
Public submission
Who has a link
Only me
NETWORK
Connected
Disconnected
HTTPS MITM proxy
Fake Net
Route internet traffic through (optional):
Route via TOR
User's VPN (OpenVPN)
Fastest geo
Choose OpenVPN config

Let's upload the file we want to analyze on the screen that opens with the help of the "Choose a file" button.

After the file is uploaded, we can determine the parameters such as which operating system we want to run the malware and 32/64 bit of operating system to use. After determining these, we open our sandbox with the help of the "Run" button at the bottom right of the screen that opens.

When our machine is turned on, we run the malicious software we uploaded to see it's activities.

Some malware stays dormant for a certain period of time before performing its malicious activities, making analysis difficult. Let's allow time for the malware to perform its activities, during this time, let's examine the AnyRun interface together.


1
MOVE YOUR MOUSE TO VIEW SCREENSHOTS
ANY RUN
2
HTTP Requests
Connections
DNS Requests
Threats
PCAP
Timeshift
Headers
Rep
PID
Process name
CN
URL
Content
3
No data
Process details
ID 3140
Malicious
708e198608b5b463224c3fb77fcf70...
App
Username: admin
Start:
Indicators:
4
100
OUT OF 100
Command line
More info

From this area, you can use the operating system interactively.

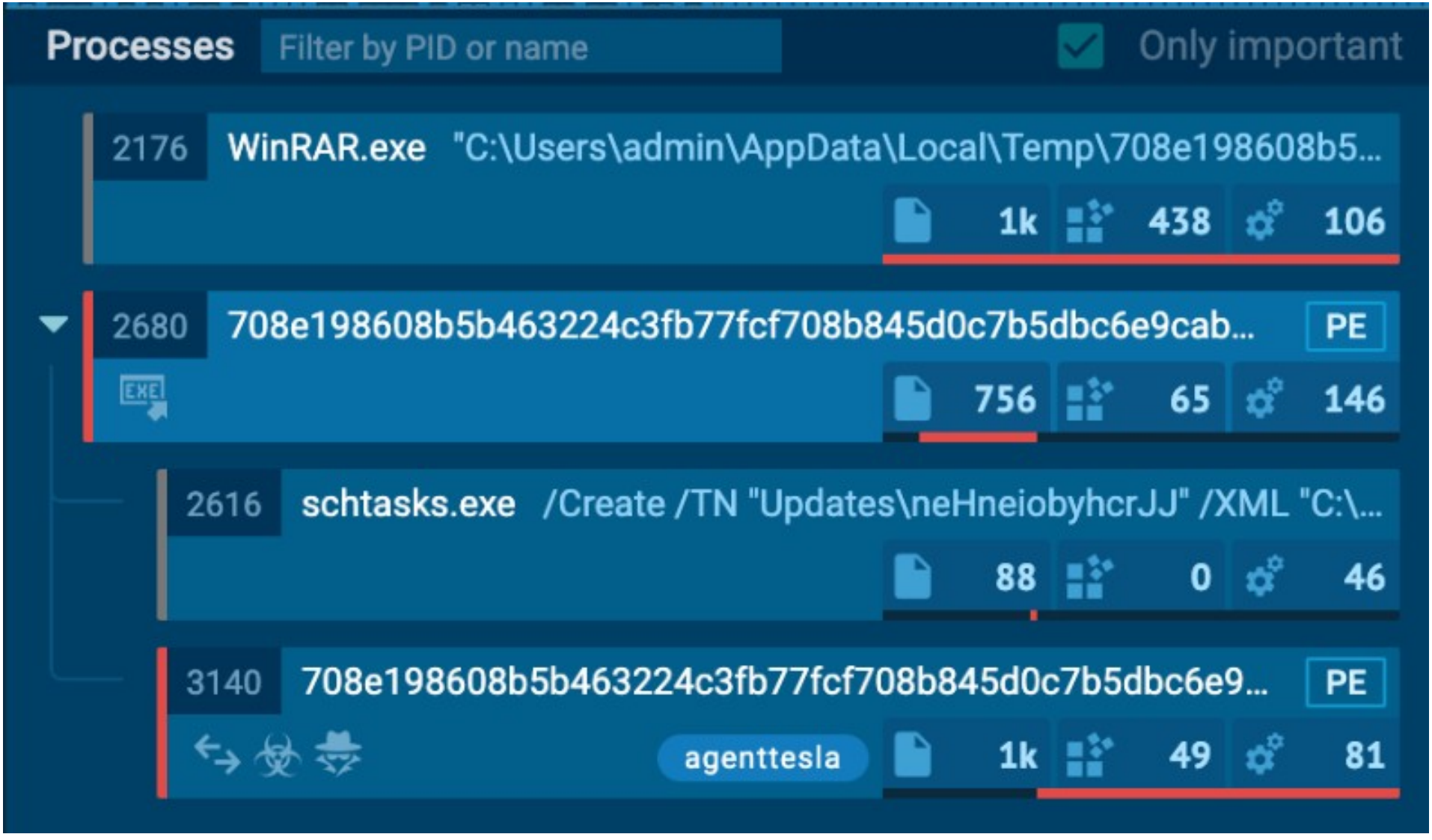
Here is a list of processes in this section. From here, you can easily see which childprocesses the malware you run has.

In this area there is network and files events.

This section contains details of the process.

Let's examine these outputs.

First, let's examine the process events of the malware in the section marked "2" in the image above.

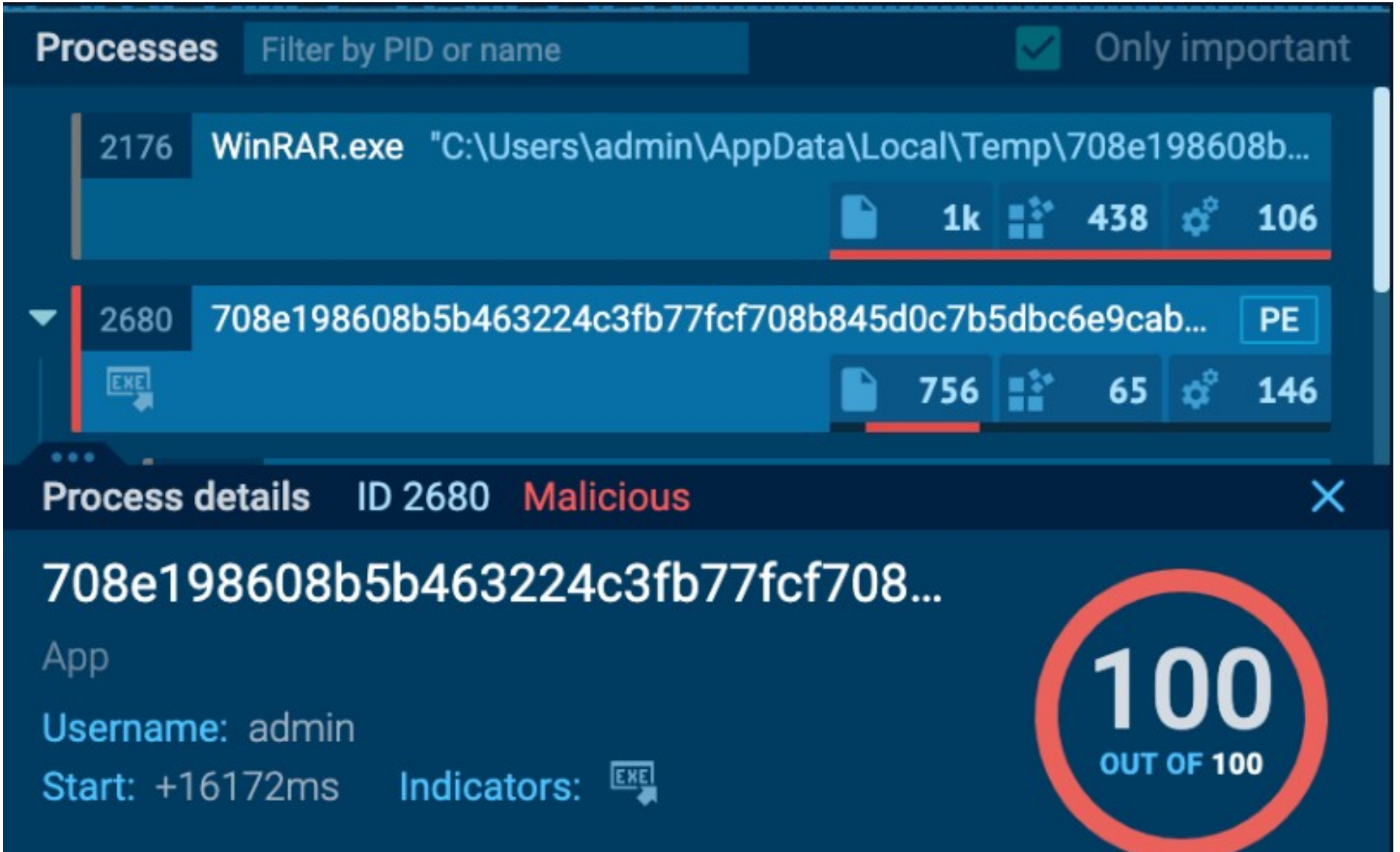

Processes
Filter by PID or name
Only important
2176
WinRAR.exe "C:\Users\admin\AppData\Local\Temp\708e198608b5...
1k
438
106
2680
708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab...
PE
EXE
756
65
146
2616
schtasks.exe /Create /TN "Updates\neHneiobyhcrJJ" /XML "C:\...
88
0
46
3140
708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9...
PE
agenttesla
1k
49
81

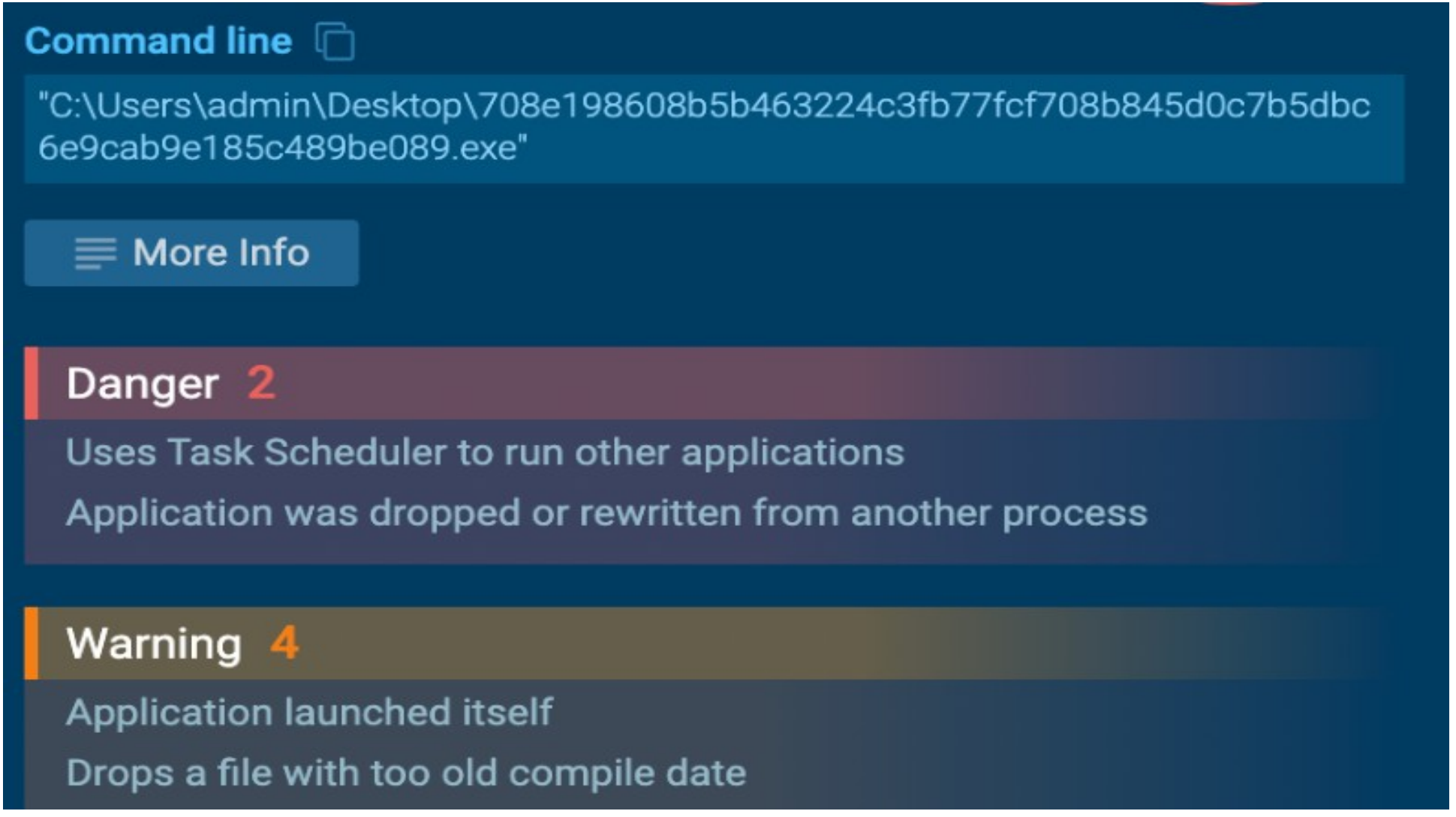
The malware we run manually seems to have created 2 child processes. One of them is schtasks.exe, which is run to ensure persistence on the system by creating a schedule task and the other is the process specified as "AgentTesla" malware by AnyRun.

When we click on Processes, information about this process is displayed in panel number 4. Let's examine the details of all processes respectively.

Since the process named "WinRAR.exe" is created when we extract the malware from the archive file to run it, we will not examine this process.

When we click on the process with ID 2680, information about this process is listed on panel number 4.


Processes
Filter by PID or name
Only important
2176 WinRAR.exe "C:\Users\admin\AppData\Local\Temp\708e198608b...
1k 438 106
2680 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab... PE
EXE
756 65 146
Process details ID 2680 Malicious
708e198608b5b463224c3fb77fcf708...
App
Username: admin
Start: +16172ms Indicators:
EXE
100
OUT OF 100


Command line
"C:\Users\admin\Desktop\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe"
More Info
Danger 2
Uses Task Scheduler to run other applications
Application was dropped or rewritten from another process
Warning 4
Application launched itself
Drops a file with too old compile date

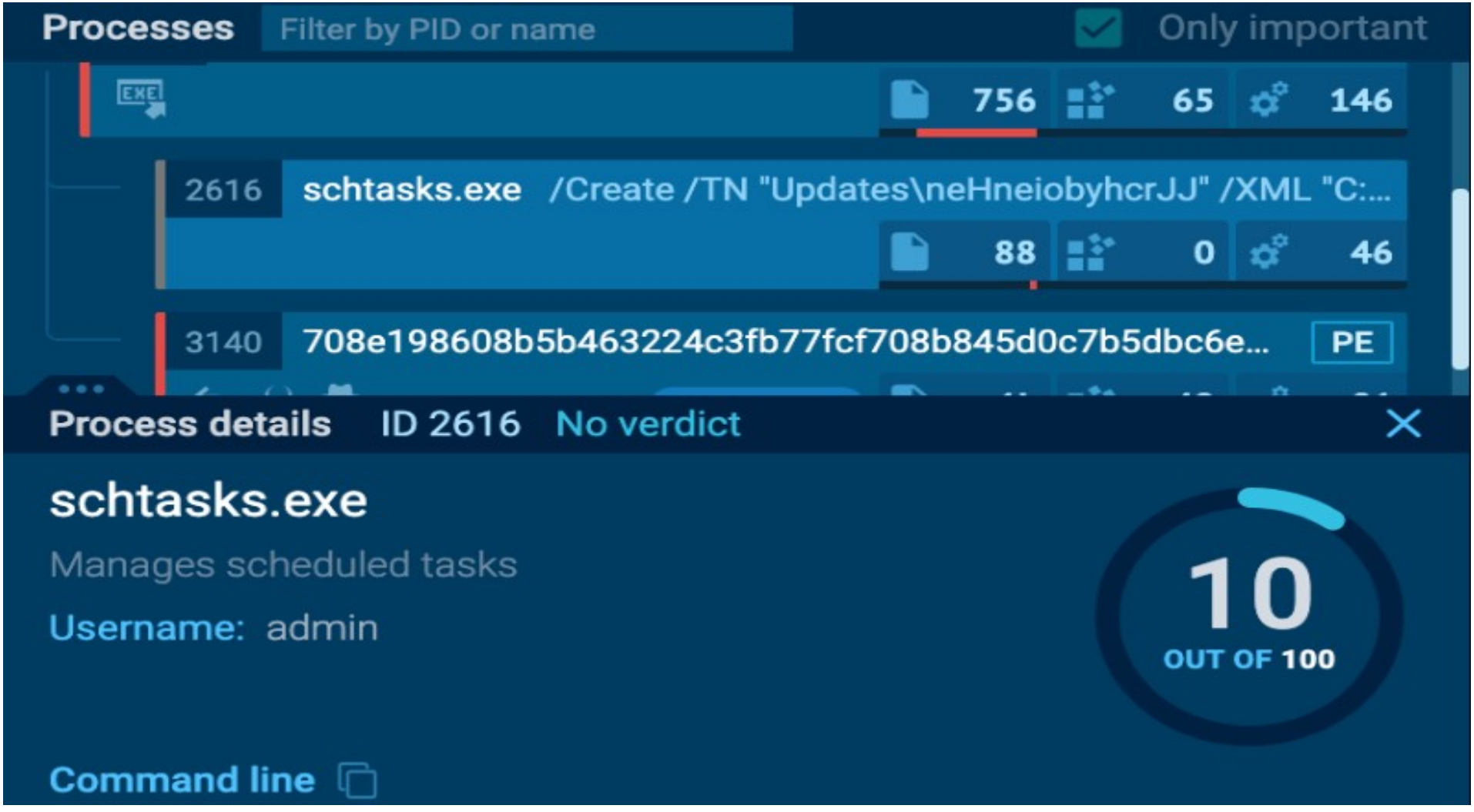
With the "More Info" button on this panel, a page with detailed information about the process is opened. When we want to reach detailed information, we can use this section.

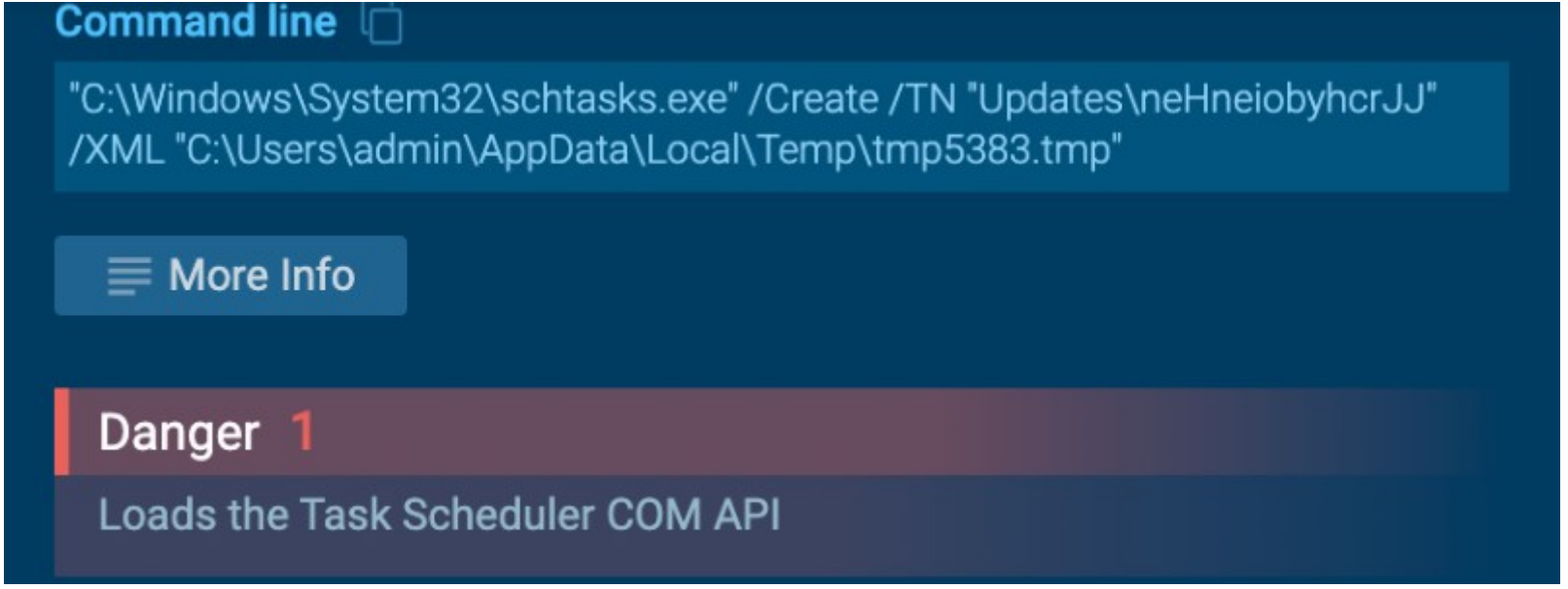
When the process information with 2680 ID is examined,

The malware: Uses Task Scheduler,

Writes a program to the file system which compile time is too old,

Writes many files to the user directory


Processes
Filter by PID or name
Only important
EXE
756
65
146
2616
schtasks.exe /Create /TN "Updates\neHneiobyhcrJJ" /XML "C:...
88
0
46
3140
708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e...
PE
Process details
ID 2616
No verdict
schtasks.exe
Manages scheduled tasks
Username: admin
10
OUT OF 100
Command line


Command line
"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\neHneiobyhcrJJ" /XML "C:\Users\admin\AppData\Local\Temp\tmp5383.tmp"
More Info
Danger 1
Loads the Task Scheduler COM API

When we examine the process with ID 2616, we see that it is schtasks.exe belonging to Task Scheduler.

When we examine the "Command Line" parameters, we see that it creates a schedule task named "Updates\neHneiobyhcrJJ". The configurations for this schedule task are in the file "tmp5383.tmp"

> tmp5383.tmp

⚠ Dropped from process

Σ Look up on VirusTotal

Submit to analysis | Download

Mime: text/xml

Size: 1.58 Kb

TrID - File Identifier

100% | Generic XML (ASCII)

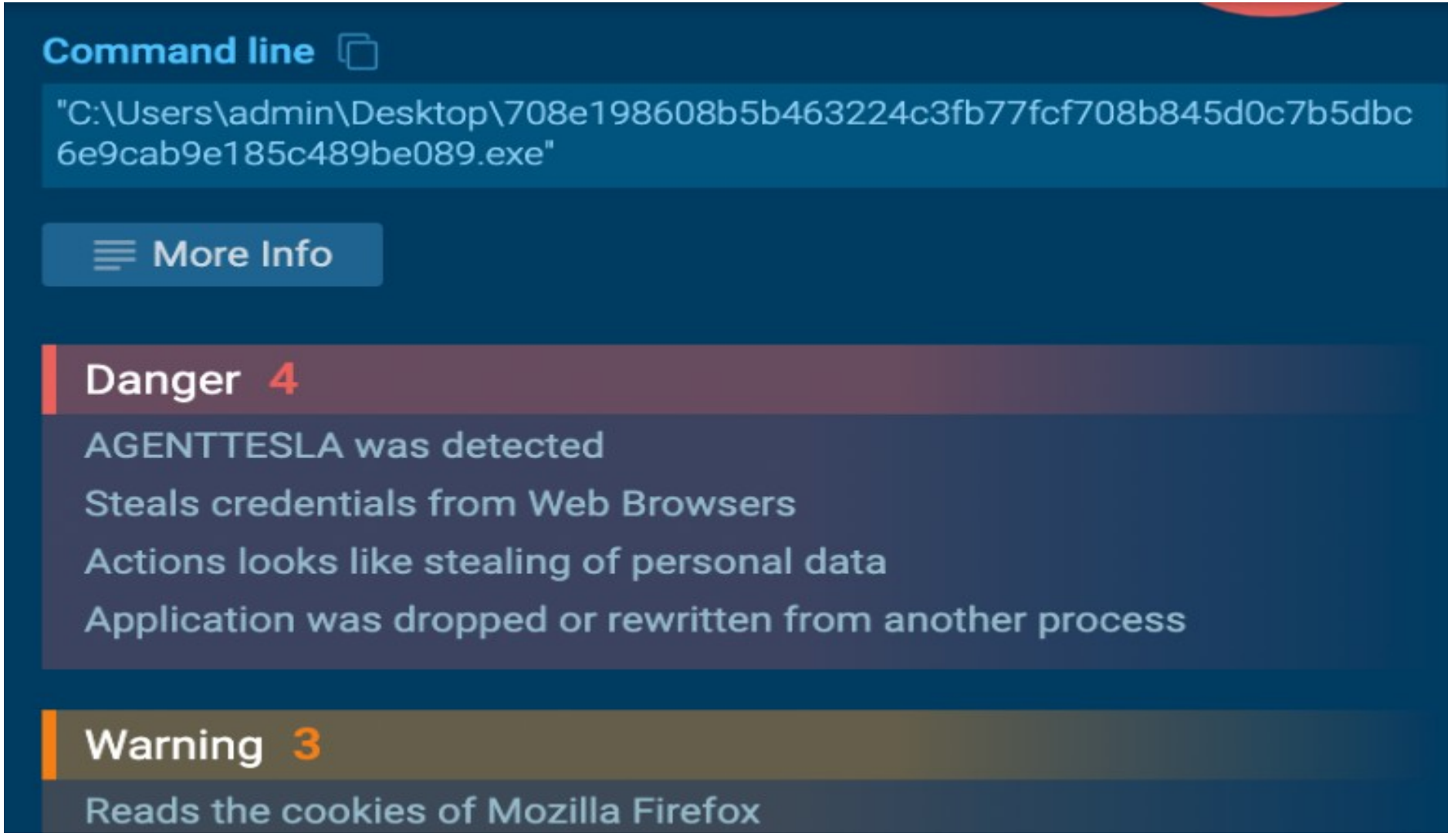
Hashes

MD5	9B4EC3A9799C9300727FC04436E9F3A4
SHA1	7BC2DFA5A20A95DB0E703BD3803EFD21AD825440
SHA256	16D44F358DBF6AAD7FCACC3B68A0506FFD7395B7887D7847A77D55170BCF02B7
SSDEEP	48:cbhQY7SJlNQa9/rydbz9I3YODOLNdq3BT:yhT1a/rydbz9ddq3BT

PREVIEW | EXIF | HEX

```
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Users\admin\AppData\Roaming\neHneiobyhcrJJ.exe</Command>
    </Exec>
  </Actions>
</Task>
```

When we examine the schedule task configuration file named tmp5383.tmp, we see that the program named "neHneiobyhcrJJ.exe" will run


Command line
"C:\Users\admin\Desktop\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe"
More Info
Danger 4
AGENTTESLA was detected
Steals credentials from Web Browsers
Actions looks like stealing of personal data
Application was dropped or rewritten from another process
Warning 3
Reads the cookies of Mozilla Firefox

When we examine the process with ID 3140:

This malware is recognized by AnyRun as **AgentTesla**,

Steals credentials,

Creating files in the user directory


HTTP Requests 0
Connections 2
DNS Requests 1
Threats 14
Filter by IP
PCAP
Timeshift Protocol Rep PID Process name CN IP Port Domain ASN Traffic
162.88 s TCP 3140 708e198608b5b46322... 208.91.199.225 587 smtp.godforeu.com PDR 988 b 415 b
165.94 s TCP 3140 708e198608b5b46322... 208.91.199.225 587 smtp.godforeu.com PDR 7.32 Kb 400 b

When we examine the network connections made from **panel number 3**, we see that malware connects to **smtp.godforeu.com**.

With the help of the button on the right of the panel, we can examine the incoming/outgoing data.

When the network activities of the malware are examined, we find that malware exfiltrates data with the SMTP protocol.


208.91.199.225 : 587 ⇄ VM : 51658
smtp.godforeu.com
RECV 162.88 s
00000000: 32 32 30 20 75 73 32 2E 6F 75 74 62 6F 75 6E 64 220 us2.outbound
00000010: 2E 6D 61 69 6C 68 6F 73 74 62 6F 78 2E 63 6F 6D .mailhostbox.com
00000020: 20 45 53 4D 54 50 20 50 6F 73 74 66 69 78 0D 0A ESMTP Postfix..
SEND 162.88 s
00000000: 45 48 4C 4F 20 55 73 65 72 2D 50 43 0D 0A EHLO User-PC..
RECV 163.89 s
00000000: 32 35 30 2D 75 73 32 2E 6F 75 74 62 6F 75 6E 64 250-us2.outbound
00000010: 2E 6D 61 69 6C 68 6F 73 74 62 6F 78 2E 63 6F 6D .mailhostbox.com
00000020: 0D 0A 32 35 30 2D 50 49 50 45 4C 49 4E 49 4E 47 ..250-PIPELINING
00000030: 0D 0A 32 35 30 2D 53 49 5A 45 20 34 31 36 34 38 ..250-SIZE 41648
00000040: 31 32 38 0D 0A 32 35 30 2D 56 52 46 59 0D 0A 32 128..250-VRFY..2

```
  s       00000020:    0D 0A 32 35 30 2D 50 49 50 45 4C 49 4E 49 4E 47    ..250-PIPELINING
          00000030:    0D 0A 32 35 30 2D 53 49 5A 45 20 34 31 36 34 38    ..250-SIZE 41648
          00000040:    31 32 38 0D 0A 32 35 30 2D 56 52 46 59 0D 0A 32    128..250-VRFY..2
          00000050:    35 30 2D 45 54 52 4E 0D 0A 32 35 30 2D 53 54 41    50-ETRN..250-STA
          00000060:    52 54 54 4C 53 0D 0A 32 35 30 2D 41 55 54 48 20    RTTLS..250-AUTH
          00000070:    50 4C 41 49 4E 20 4C 4F 47 49 4E 0D 0A 32 35 30    PLAIN LOGIN..250
          00000080:    2D 41 55 54 48 3D 50 4C 41 49 4E 20 4C 4F 47 49    -AUTH=PLAIN LOGI
          00000090:    4E 0D 0A 32 35 30 2D 45 4E 48 41 4E 43 45 44 53    N..250-ENHANCEDS
          000000A0:    54 41 54 55 53 43 4F 44 45 53 0D 0A 32 35 30 2D    TATUSCODES..250-
          000000B0:    38 42 49 54 4D 49 4D 45 0D 0A 32 35 30 20 44 53    8BITMIME..250 DS
          000000C0:    4E 0D 0A                                           N..

SEND      00000000:    41 55 54 48 20 6C 6F 67 69 6E 20 62 47 39 6E 63    AUTH login bG9nc
163.89    00000010:    30 42 6E 62 32 52 6D 62 33 4A 6C 64 53 35 6A 62    0Bnb2Rmb3JldS5jb
  s       00000020:    32 30 3D 0D 0A                                     20=..

RECV      00000000:    33 33 34 20 55 47 46 7A 63 33 64 76 63 6D 51 36    334 UGFzc3dvcmQ6
163.89    00000010:    0D 0A                                              ..
```

We constantly spend time analyzing malware.

We have listed 29 addresses that can be useful for analysis effectively:

Anlyz

Any.run

Comodo Valkyrie

Cuckoo

Hybrid Analysis

Intezer Analyze

SecondWrite Malware Deepview

Jevereg

IObit Cloud

BinaryGuard

Joe Sandbox

AMAaaS

BitBlaze

SandDroid

IRIS-H

Gatewatcher Intelligence

Hatching Triage

InQuest Labs

Manalyzer

SandBlast Analysis

SNDBOX

firmware

opswat

virusade

virustotal

malware config

malware hunter team

virscan

jotti