Malware Analysis in ANY.RUN: The Ultimate Guide

This crash course will walk you through the basics of using our interactive sandbox to help you achieve your malware analysis goals.

Let’s get started!

About ANY.RUN

ANY.RUN is an online sandbox for interactive malware research. The service delivers a comprehensive and instant analysis of cybersecurity threats, while allowing users to engage with potentially malicious samples in real time within a safe virtual machine (VM) environment.

The sandbox solves a host of problems related to malware analysis, as it:

- Simplifies SOC/DFIR operations by providing valuable data for threat detection and elimination
- Saves clients resources by offering a more affordable alternative to on-premises VMs
- Makes cybersecurity more accessible with an intuitive interface that is easy to grasp for both students and seasoned experts alike

Now, let’s dive into the platform’s interface.

Setting up your account

Step 1: Sign up

For non-business email users, use the #verification channel on our Discord server to request a free ANY.RUN account.

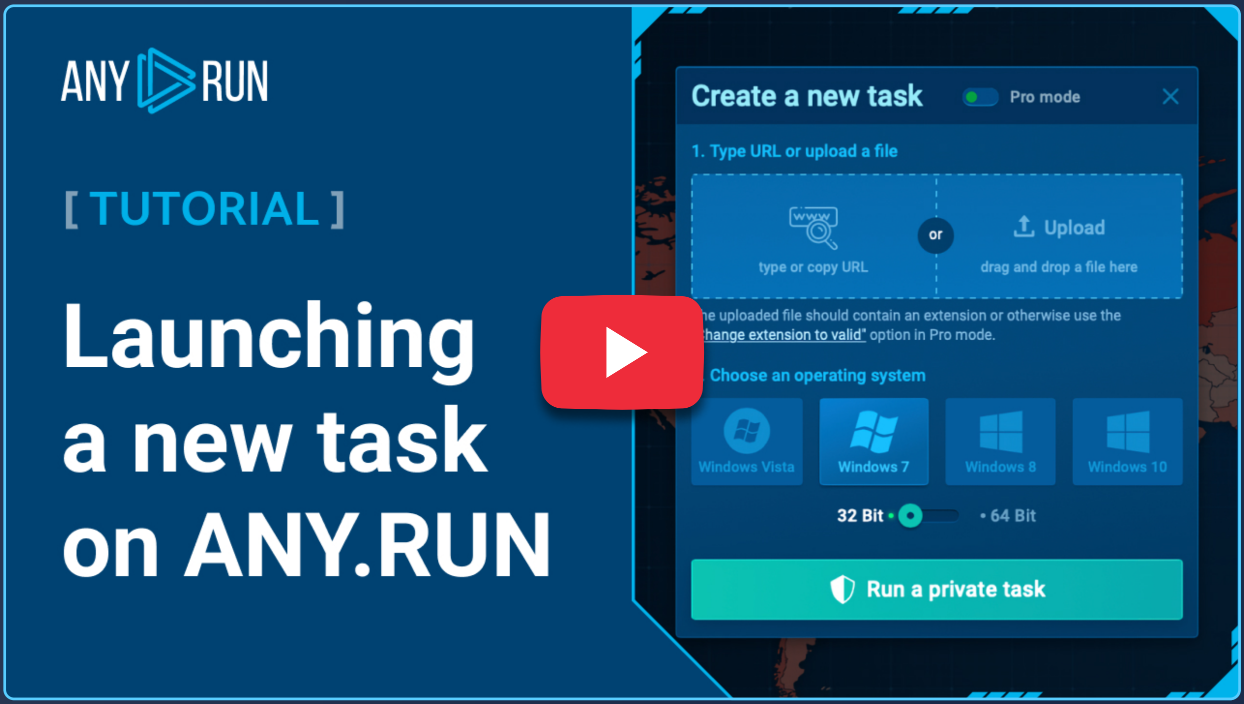
Step 2: Choose your subscription plan

After logging in to your account, you will be greeted by the dashboard page. From there, you can go to your Profile settings to choose your subscription plan. We offer a free Community plan that provides you with a wide range of tools for thorough analysis. However, if you require a more advanced level of malware analysis, our paid plans are the ideal choice.

Learn more: ANY.RUN plans

With your account all set-up and firing on all cylinders, it is time you get started with your first task.

Setting up a virtual machine for malware analysis



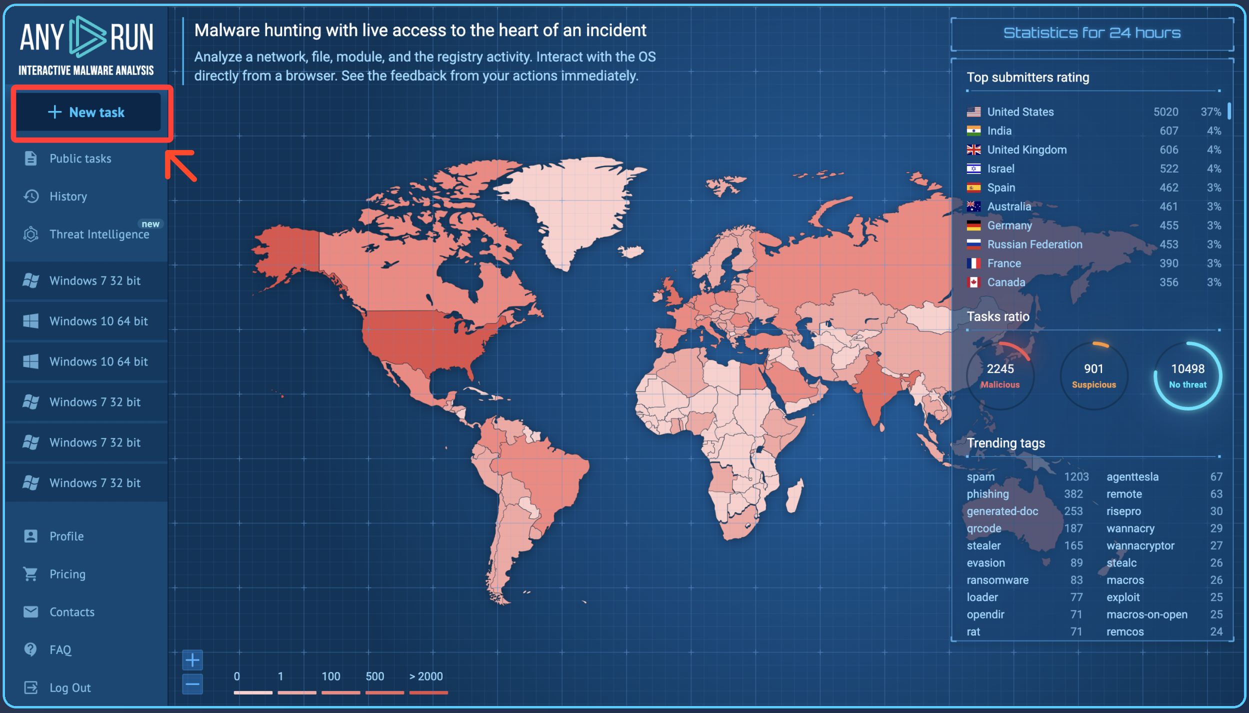
he uploaded file should contain an extension or otherwise use the "hange extension to valid" option in Pro mode.

See how to launch your first task in ANY.RUN using this video

In order to set up a virtual machine (VM) for malware analysis in ANY.RUN, you need to create a new task. Access an interactive tutorial by visiting the FAQ page's Tutorials tab and clicking the "How to analyze threats" button.

In case you prefer written instructions, continue reading this article and follow these steps.

Step 1: Open the task window



Malware hunting with live access to the heart of an incident

Analyze a network, file, module, and the registry activity. Interact with the OS directly from a browser. See the feedback from your actions immediately.

Statistics for 24 hours

Top submitters rating

United States	5020	37%
India	607	4%
United Kingdom	606	4%
Israel	522	4%
Spain	462	3%
Australia	461	3%
Germany	455	3%
Russian Federation	453	3%
France	390	3%
Canada	356	3%

Tasks ratio

2245 Malicious · 901 Suspicious · 10498 No threat

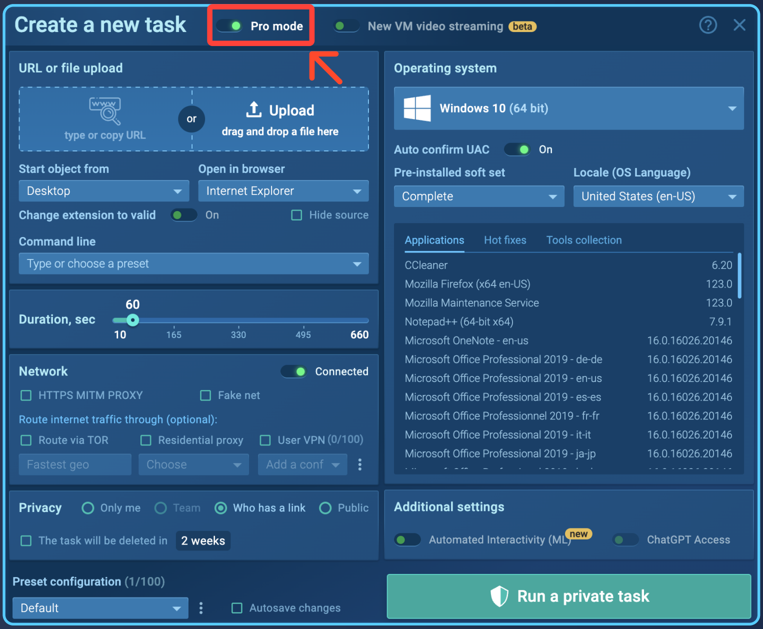
Trending tags

spam	1203	agenttesla	67
phishing	382	remote	63
generated-doc	253	risepro	30
qrcode	187	wannacry	29
stealer	165	wannacryptor	27
evasion	89	stealc	26
ransomware	83	macros	26
loader	77	exploit	25
opendir	71	macros-on-open	25
rat	71	remcos	24

Launch your task in two clicks

Click the New Task button on the left sidebar to open the task window.

Step 2: Choose an analysis mode



Create a new task

URL or file upload

Start object from: Desktop

Open in browser: Internet Explorer

Change extension to valid: On · □ Hide source

Command line: Type or choose a preset

Duration, sec: 60 (10 · 165 · 330 · 495 · 660)

Network: Connected

□ HTTPS MITM PROXY · □ Fake net

Route internet traffic through (optional):

□ Route via TOR · □ Residential proxy · □ User VPN (0/100)

Fastest geo · Choose · Add a conf

Privacy: ○ Only me ○ Team ● Who has a link ○ Public

□ The task will be deleted in 2 weeks

Preset configuration (1/100): Default · □ Autosave changes

Operating system: Windows 10 (64 bit)

Auto confirm UAC: On

Pre-installed soft set: Complete

Locale (OS Language): United States (en-US)

Applications · Hot fixes · Tools collection

CCleaner	6.20
Mozilla Firefox (x64 en-US)	123.0
Mozilla Maintenance Service	123.0
Notepad++ (64-bit x64)	7.9.1
Microsoft OneNote - en-us	16.0.16026.20146
Microsoft Office Professional 2019 - de-de	16.0.16026.20146
Microsoft Office Professional 2019 - en-us	16.0.16026.20146
Microsoft Office Professional 2019 - es-es	16.0.16026.20146
Microsoft Office Professionnel 2019 - fr-fr	16.0.16026.20146
Microsoft Office Professional 2019 - it-it	16.0.16026.20146
Microsoft Office Professional 2019 - ja-jp	16.0.16026.20146

Additional settings

Automated Interactivity (ML) new · ChatGPT Access

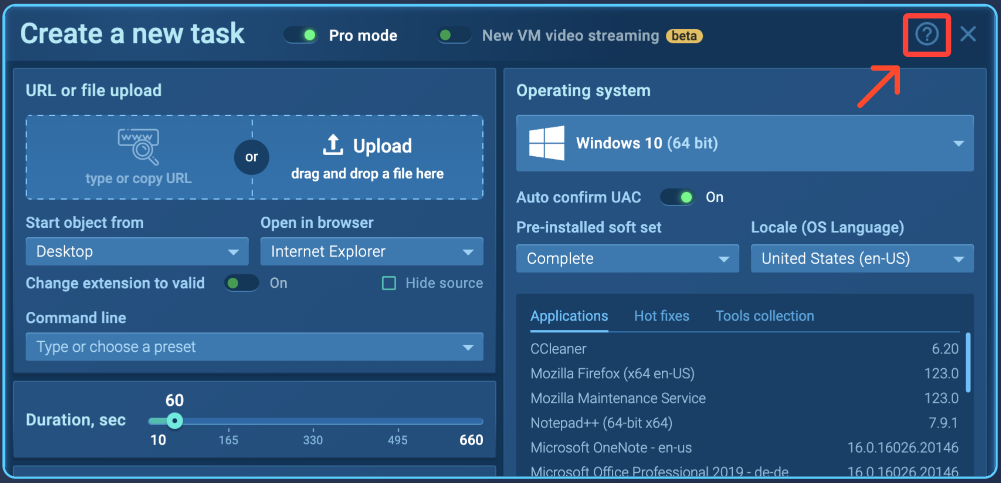
Switch to the Pro mode to customize your VM environment

The newly opened task window will be set to the User Mode by default, which lets you quickly analyze your file or link but limits your VM settings to only choosing an OS version:

- Windows from 7 through 11 — 32-bit or 64-bit versions.
- Linux — Ubuntu 22.04.2.

To open the rest of the VM customization features, enable the Pro Mode by pressing the respective button on top of the task window.

Step 3: Configure the VM



Start object from: Desktop

Open in browser: Internet Explorer

Change extension to valid: On

□ Hide source

Command line: Type or choose a preset

Duration, sec: 60 (10 – 165 – 330 – 495 – 660)

Operating system: Windows 10 (64 bit)

Auto confirm UAC: On

Pre-installed soft set: Complete

Locale (OS Language): United States (en-US)

CCleaner	6.20
Mozilla Firefox (x64 en-US)	123.0
Mozilla Maintenance Service	123.0
Notepad++ (64-bit x64)	7.9.1
Microsoft OneNote - en-us	16.0.16026.20146
Microsoft Office Professional 2019 - de-de	16.0.16026.20146

Open tooltips to explore every VM setting available to you

In the Pro mode, you can fine-tune your analysis environment. Click on the question mark icon in the top right corner to access tooltips with detailed explanations of each setting. After completing the VM setup, begin your analysis by pressing the Run a Private/Public Task button.

Learn more: [Guide to Creating a Task in ANY.RUN]

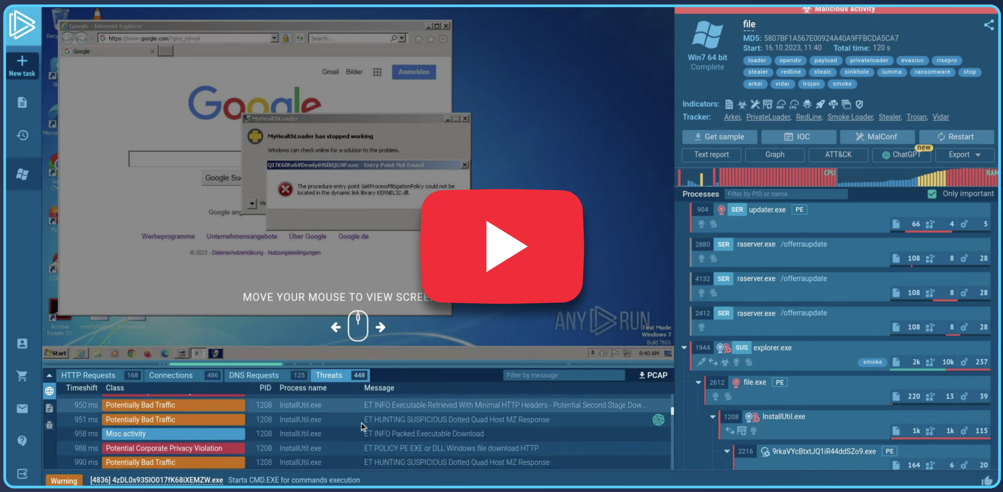
Analyzing malware

Once your task is launched, you will be taken to a page where you will be able to analyze your sample in real time and, once it is done, review the findings of the investigation. Here are the things you can perform as part of your analysis.

Interact with the sample

ANY.RUN enables you to manually interact with your sample in a VM environment like you would on a normal computer. You can run programs, open tabs in a browser, and even restart the system without delay.

Learn more: [Interactive Malware Analysis]



file

MD5: 5807BF1A567E00924A40A9FFBCDA5CA7

Start: 16.10.2023, 11:40   Total time: 120 s

Win7 64 bit Complete

loader, opendir, payload, privateloader, evasion, risepro, stealer, redline, stealc, sinkhole, lumma, ransomware, stop, arkei, vidar, trojan, smoke

Indicators:

Tracker: Arkei, PrivateLoader, RedLine, Smoke Loader, Stealer, Trojan, Vidar

Processes ☑ Only important

```
904   SER updater.exe PE                          66    4    5
2880  SER raserver.exe /offerraupdate            108    8   28
4132  SER raserver.exe /offerraupdate            108    8   28
2412  SER raserver.exe /offerraupdate            108    8   28
1944  SUS explorer.exe                 smoke     2k  10k  237
2612  file.exe PE                                220   13   39
1208  InstallUtil.exe                             1k   1k  115
2216  9rkaVYcBtxtJQ1iR44ddSZo9.exe PE            164    6   20
```

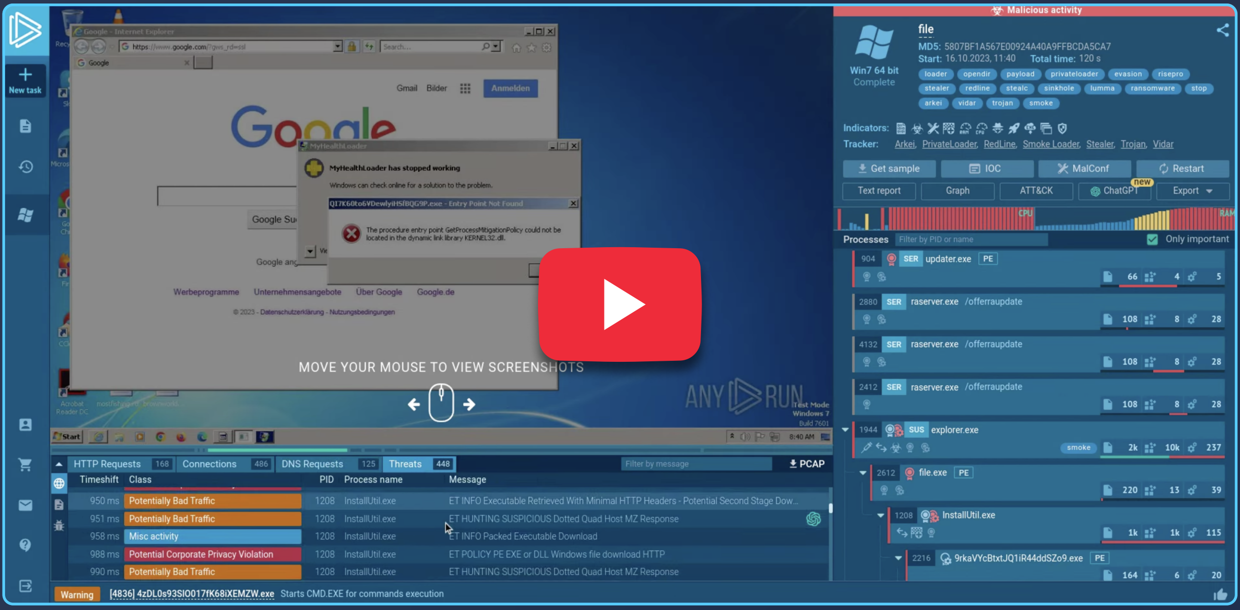
HTTP Requests 168 | Connections 486 | DNS Requests 125 | Threats 448

Timeshift	Class	PID	Process name	Message
950 ms	Potentially Bad Traffic	1208	InstallUtil.exe	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Dow...
951 ms	Potentially Bad Traffic	1208	InstallUtil.exe	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
958 ms	Misc activity	1208	InstallUtil.exe	ET INFO Packed Executable Download
988 ms	Potential Corporate Privacy Violation	1208	InstallUtil.exe	ET POLICY PE EXE or DLL Windows file download HTTP
990 ms	Potentially Bad Traffic	1208	InstallUtil.exe	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response

Warning [4836] 4zDL0s93SIO017fK68iXEMZW.exe Starts CMD.EXE for commands execution

The interactive VM lets you copy and paste any content via the Clipboard tool

Track network activity



Malicious activity

file
MD5: 5807BF1A567E00924A40A9FFBCDA5CA7
Start: 16.10.2023, 11:40 Total time: 120 s
Win7 64 bit Complete
loader opendir payload privateloader evasion risepro stealer redline stealc sinkhole lumma ransomware stop arkei vidar trojan smoke
Indicators:
Tracker: Arkei, PrivateLoader, RedLine, Smoke Loader, Stealer, Trojan, Vidar

Processes
904 SER updater.exe PE
2880 SER raserver.exe /offerraupdate
4132 SER raserver.exe /offerraupdate
2412 SER raserver.exe /offerraupdate
1944 SUS explorer.exe
2612 file.exe PE
1208 InstallUtil.exe
2216 9rkaVYcBtxtJQ1iR44ddSZo9.exe PE

HTTP Requests 168 | Connections 486 | DNS Requests 125 | Threats 448

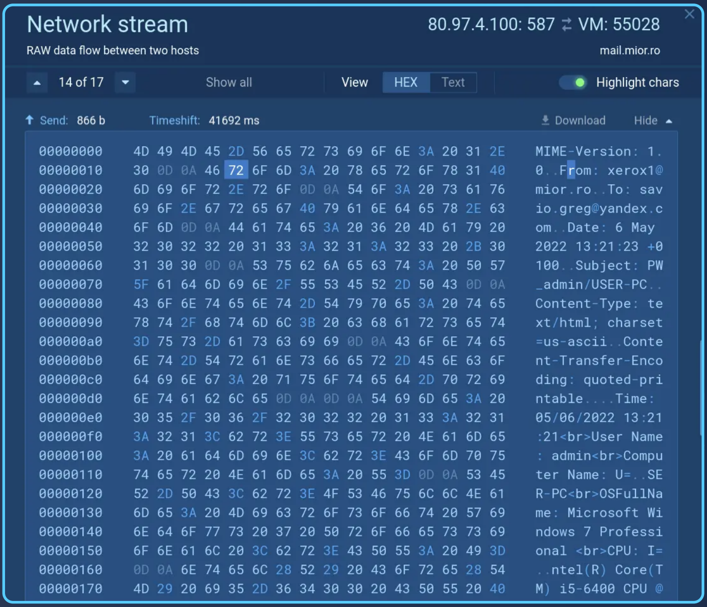
Timeshift	Class	PID	Process name	Message
950 ms	Potentially Bad Traffic	1208	InstallUtil.exe	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Dow...
951 ms	Potentially Bad Traffic	1208	InstallUtil.exe	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
958 ms	Misc activity	1208	InstallUtil.exe	ET INFO Packed Executable Download
988 ms	Potential Corporate Privacy Violation	1208	InstallUtil.exe	ET POLICY PE EXE or DLL Windows file download HTTP
990 ms	Potentially Bad Traffic	1208	InstallUtil.exe	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response

Warning [4836] 4zDL0s93SIO017fK68iXEMZW.exe Starts CMD.EXE for commands execution

You can view malware's connections and traffic

The Network section monitors and records network activity as it is occurring and provides the following information:

- **HTTP Requests:** Displays details of connection requests, including URL connection response and content
- **Connections:** Shows other protocols that were not mentioned in HTTP Requests
- **DNS Requests:** Indicates the correlation between a domain name and IP address
- **Threats:** Detects intrusion using Suricata rules (Detection with Suricata IDS)



Network stream
RAW data flow between two hosts
80.97.4.100: 587 ⇄ VM: 55028
mail.mior.ro

Send: 866 b Timeshift: 41692 ms

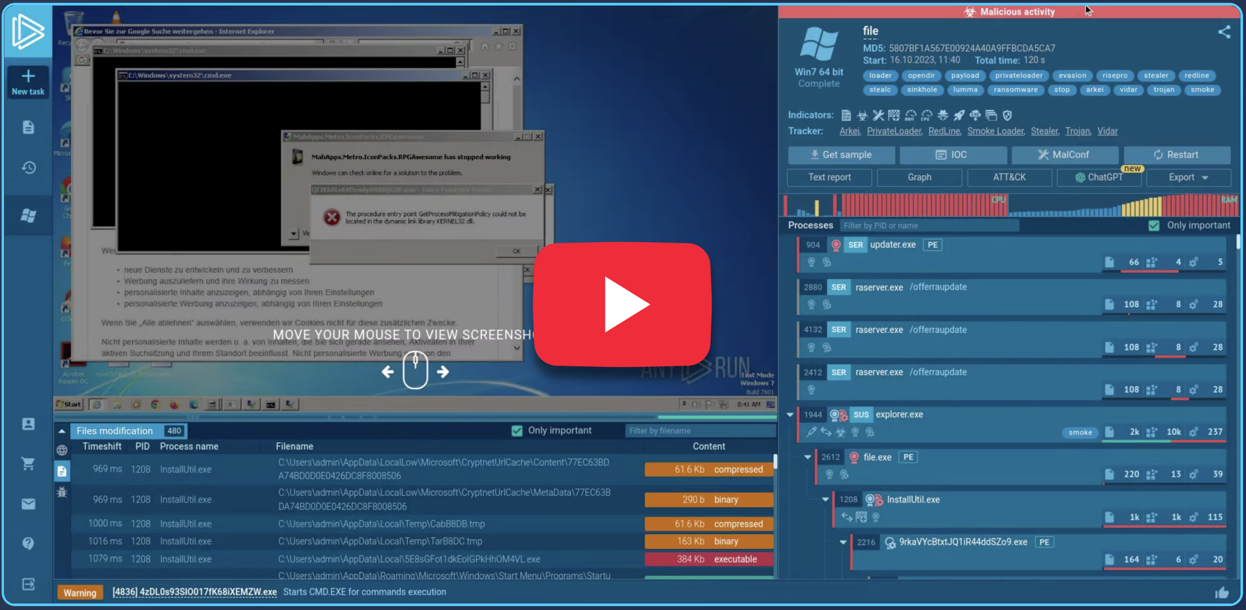
```
00000000   4D 49 4D 45 2D 56 65 72 73 69 6F 6E 3A 20 31 2E   MIME-Version: 1.
00000010   30 0D 0A 46 72 6F 6D 3A 20 78 65 72 6F 78 31 40   0..From: xerox1@
00000020   6D 69 6F 72 2E 72 6F 0D 0A 54 6F 3A 20 73 61 76   mior.ro..To: sav
00000030   69 6F 2E 67 72 65 67 40 79 61 6E 64 65 78 2E 63   io.greg@yandex.c
00000040   6F 6D 0D 0A 44 61 74 65 3A 20 36 20 4D 61 79 20   om..Date: 6 May 
00000050   32 30 32 32 20 31 33 3A 32 31 3A 32 33 20 2B 30   2022 13:21:23 +0
00000060   31 30 30 0D 0A 53 75 62 6A 65 63 74 3A 20 50 57   100..Subject: PW
00000070   5F 61 64 6D 69 6E 2F 55 53 45 52 2D 50 43 0D 0A   _admin/USER-PC..
00000080   43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65   Content-Type: te
00000090   78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74   xt/html; charset
000000a0   3D 75 73 2D 61 73 63 69 69 0D 0A 43 6F 6E 74 65   =us-ascii..Conte
000000b0   6E 74 2D 54 72 61 6E 73 66 65 72 2D 45 6E 63 6F   nt-Transfer-Enco
000000c0   64 69 6E 67 3A 20 71 75 6F 74 65 64 2D 70 72 69   ding: quoted-pri
000000d0   6E 74 61 62 6C 65 0D 0A 0D 0A 54 69 6D 65 3A 20   ntable....Time: 
000000e0   30 35 2F 30 36 2F 32 30 32 32 20 31 33 3A 32 31   05/06/2022 13:21
000000f0   3A 32 31 3C 62 72 3E 55 73 65 72 20 4E 61 6D 65   :21<br>User Name
00000100   3A 20 61 64 6D 69 6E 3C 62 72 3E 43 6F 6D 70 75   : admin<br>Compu
00000110   74 65 72 20 4E 61 6D 65 3A 20 55 3D 0D 0A 53 45   ter Name: U=..SE
00000120   52 2D 50 43 3C 62 72 3E 4F 53 46 75 6C 6C 4E 61   R-PC<br>OSFullNa
00000130   6D 65 3A 20 4D 69 63 72 6F 73 6F 66 74 20 57 69   me: Microsoft Wi
00000140   6E 64 6F 77 73 20 37 20 50 72 6F 66 65 73 73 69   ndows 7 Professi
00000150   6F 6E 61 6C 20 3C 62 72 3E 43 50 55 3A 20 49 3D   onal <br>CPU: I=
00000160   0D 0A 6E 74 65 6C 28 52 29 20 43 6F 72 65 28 54   ..ntel(R) Core(T
00000170   4D 29 20 69 35 2D 36 34 30 30 20 43 50 55 20 40   M) i5-6400 CPU @
```

Use network stream analysis to expose evasive malware

You can examine traffic packet by packet using the Network stream feature, enabling you to identify unusual patterns or connections, stolen data, C2 addresses, proxies, and downloaded files.

Learn more: Analyzing the Network Stream

Review modified files



Malicious activity

file
MD5: 5807BF1A567E00924A40A9FFBCDA5CA7
Start: 16.10.2023, 11:40 Total time: 120 s
Win7 64 bit Complete

loader opendir payload privateloader evasion risepro stealer redline stealc sinkhole lumma ransomware stop arkei vidar trojan smoke

Indicators:
Tracker: Arkei, PrivateLoader, RedLine, Smoke Loader, Stealer, Trojan, Vidar

Processes ☑ Only important

PID	Type	Process	Command
904	SER	updater.exe PE	
2880	SER	raserver.exe	/offerraupdate
4132	SER	raserver.exe	/offerraupdate
2412	SER	raserver.exe	/offerraupdate
1944	SUS	explorer.exe	
2612		file.exe PE	
1208		InstallUtil.exe	
2216		9rkaVYcBtxtJQ1iR44ddSZo9.exe PE	

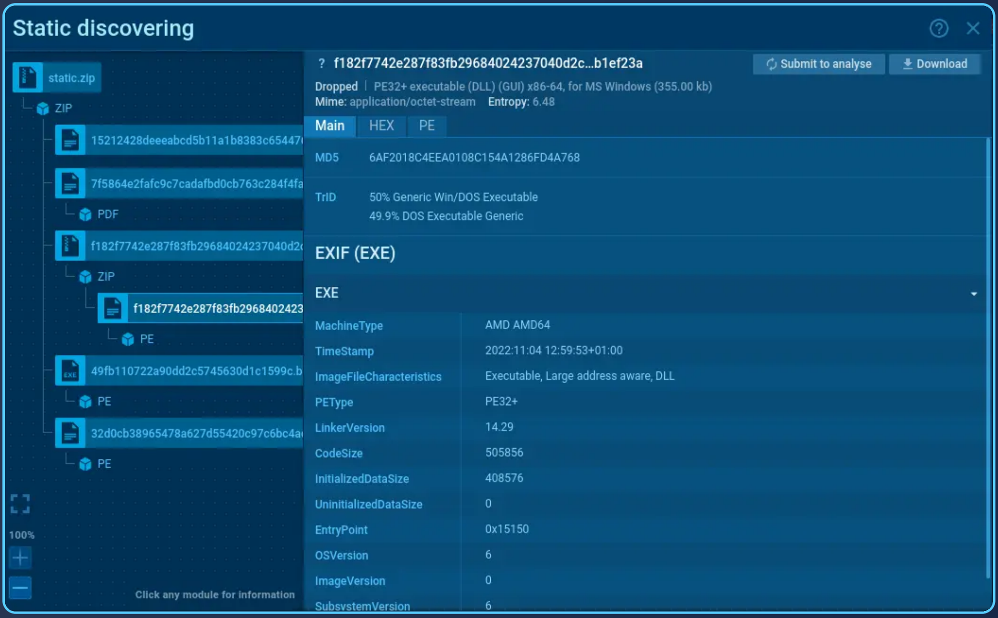
Files modification 480 ☑ Only important

Timeshift	PID	Process name	Filename	Content
969 ms	1208	InstallUtil.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	61.6 Kb compressed
969 ms	1208	InstallUtil.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	290 b binary
1000 ms	1208	InstallUtil.exe	C:\Users\admin\AppData\Local\Temp\CabB8DB.tmp	61.6 Kb compressed
1016 ms	1208	InstallUtil.exe	C:\Users\admin\AppData\Local\Temp\TarB8DC.tmp	163 Kb binary
1079 ms	1208	InstallUtil.exe	C:\Users\admin\AppData\Local\5E8sGFot1dkEoIGPkHhOM4VL.exe	384 Kb executable
			C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startu	

Warning [4836] 4zDL0s93SIO017fK68iXEMZW.exe Starts CMD.EXE for commands execution

Easily switch between the Network and Files sections

The Files Modification section lists all files used during the task execution. Click on each file's content to access downloadable Static discovering data.



Static discovering

static.zip
- ZIP
  - 15212428deeeabcd5b11a1b8383c65447
  - 7f5864e2fafc9c7cadafbd0cb763c284f4fa
    - PDF
  - f182f7742e287f83fb29684024237040d2c
    - ZIP
      - f182f7742e287f83fb2968402423
        - PE
  - 49fb110722a90dd2c5745630d1c1599c.b
    - PE
  - 32d0cb38965478a627d55420c97c6bc4a
    - PE

? f182f7742e287f83fb29684024237040d2c...b1ef23a

Dropped | PE32+ executable (DLL) (GUI) x86-64, for MS Windows (355.00 kb)
Mime: application/octet-stream Entropy: 6.48

MD5 6AF2018C4EEA0108C154A1286FD4A768

TrID 50% Generic Win/DOS Executable
49.9% DOS Executable Generic

EXIF (EXE)

EXE

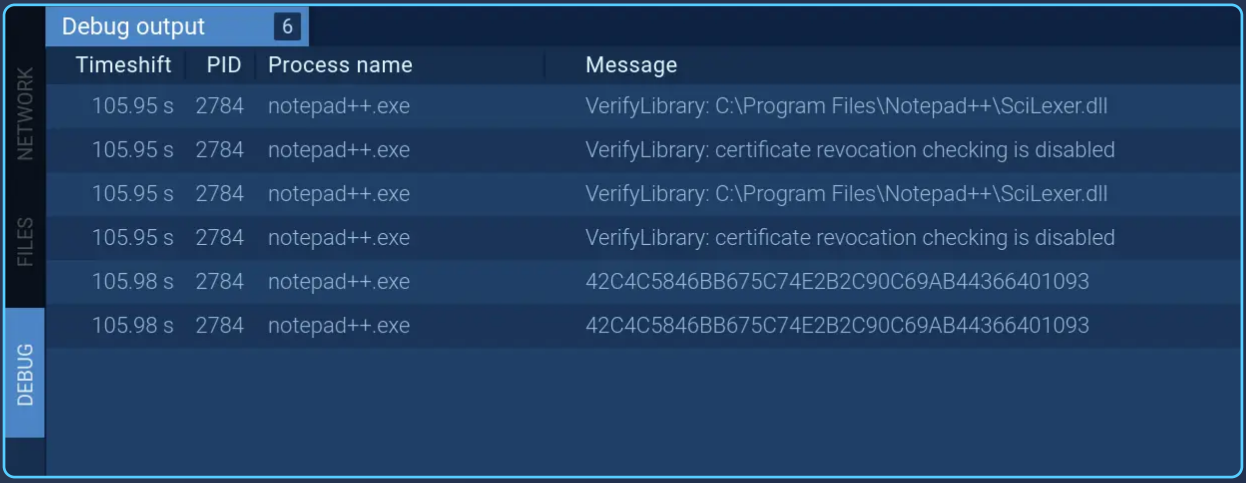
MachineType	AMD AMD64
TimeStamp	2022:11:04 12:59:53+01:00
ImageFileCharacteristics	Executable, Large address aware, DLL
PEType	PE32+
LinkerVersion	14.29
CodeSize	505856
InitializedDataSize	408576
UninitializedDataSize	0
EntryPoint	0x15150
OSVersion	6
ImageVersion	0
SubsystemVersion	6

Static discovering enables you to gain insight into any file

ANY.RUN's Static discovering feature is modular, letting you analyze a wide range of file types including PDF, LNK, ZIP, RAR, Office documents, and others.

Learn more: Static Analysis for Various File Types

Utilize debugging



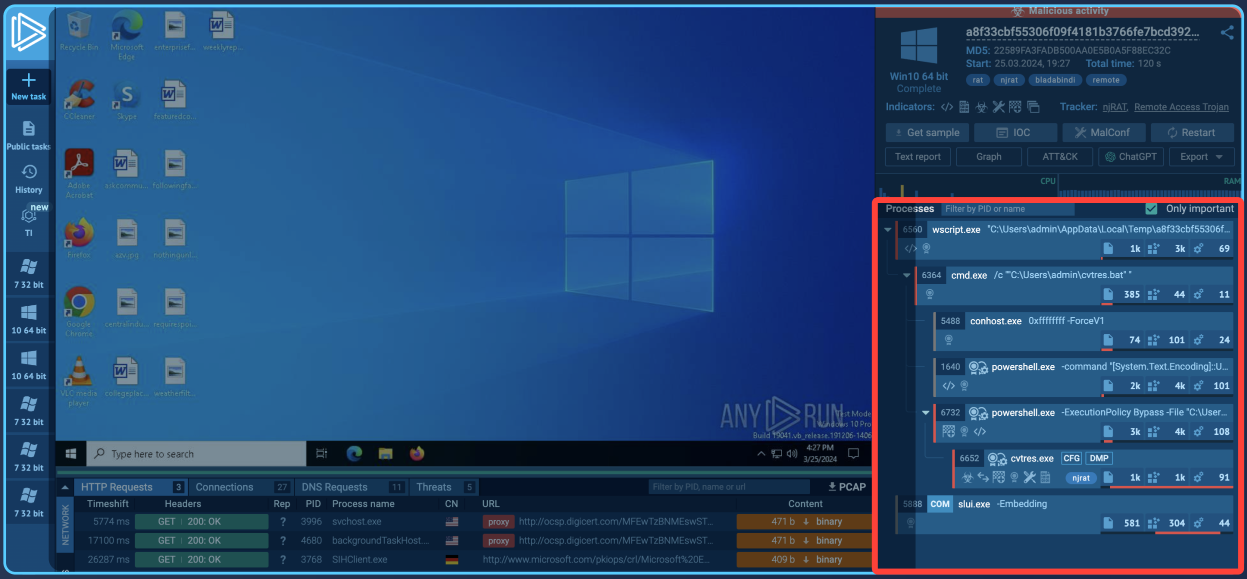
Debug output 6

Timeshift	PID	Process name	Message
105.95 s	2784	notepad++.exe	VerifyLibrary: C:\Program Files\Notepad++\SciLexer.dll
105.95 s	2784	notepad++.exe	VerifyLibrary: certificate revocation checking is disabled
105.95 s	2784	notepad++.exe	VerifyLibrary: C:\Program Files\Notepad++\SciLexer.dll
105.95 s	2784	notepad++.exe	VerifyLibrary: certificate revocation checking is disabled
105.98 s	2784	notepad++.exe	42C4C5846BB675C74E2B2C90C69AB44366401093
105.98 s	2784	notepad++.exe	42C4C5846BB675C74E2B2C90C69AB44366401093

Debugging can come in handy when handling certain malware families

The Debug section displays information on how to debug the program afterward. If you happen to encounter malware like Dridex, debug output messages will be helpful in your investigation.

Inspect processes



a8f33cbf55306f09f4181b3766fe7bcd392...
MD5: 22589FA3FADB500AA0E5B0A5F88EC32C
Start: 25.03.2024, 19:27 Total time: 120 s
rat njrat bladabindi remote
Win10 64 bit
Complete
Indicators:
Tracker: njRAT, Remote Access Trojan

Processes Filter by PID or name ☑ Only important

```
6560 wscript.exe "C:\Users\admin\AppData\Local\Temp\a8f33cbf55306f...        1k   3k   69
  6364 cmd.exe /c ""C:\Users\admin\cvtres.bat" "                            385   44   11
    5488 conhost.exe 0xffffffff -ForceV1                                     74  101   24
    1640 powershell.exe -command "[System.Text.Encoding]::U...               2k   4k  101
    6732 powershell.exe -ExecutionPolicy Bypass -File "C:\User...            3k   4k  108
      6652 cvtres.exe CFG DMP njrat                                          1k   1k   91
5888 COM slui.exe -Embedding                                                581  304   44
```

HTTP Requests 3 | Connections 27 | DNS Requests 11 | Threats 5 | Filter by PID, name or url | PCAP

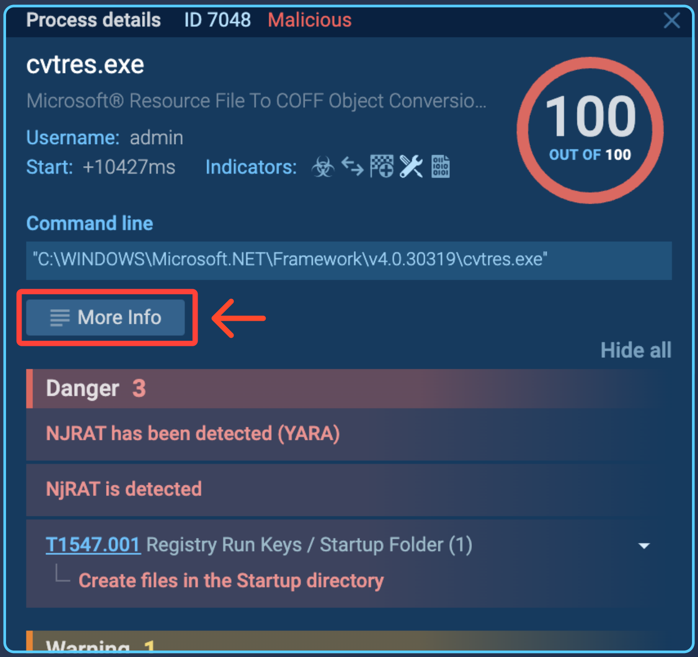
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5774 ms	GET 200: OK	?	3996	svchost.exe		proxy http://ocsp.digicert.com/MFEwTzBNMEswST...	471 b binary
17100 ms	GET 200: OK	?	4680	backgroundTaskHost....		proxy http://ocsp.digicert.com/MFEwTzBNMEswST...	471 b binary
26287 ms	GET 200: OK	?	3768	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20E...	409 b binary

The process tree depicts processes taking place in real time

The Processes section lays out a hierarchical view of all processes, accompanied by corresponding indicators.

Learn more: Indicators and Tags Used in ANY.RUN

To investigate a specific process, simply click on it. This will bring up the Process details window, from which you can navigate to the Advanced details by pressing the “More Info” button.



Process details ID 7048 Malicious

cvtres.exe

Microsoft® Resource File To COFF Object Conversio...

Username: admin

Start: +10427ms Indicators:

100 OUT OF 100

Command line

"C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\cvtres.exe"

Danger 3

NJRAT has been detected (YARA)

NjRAT is detected

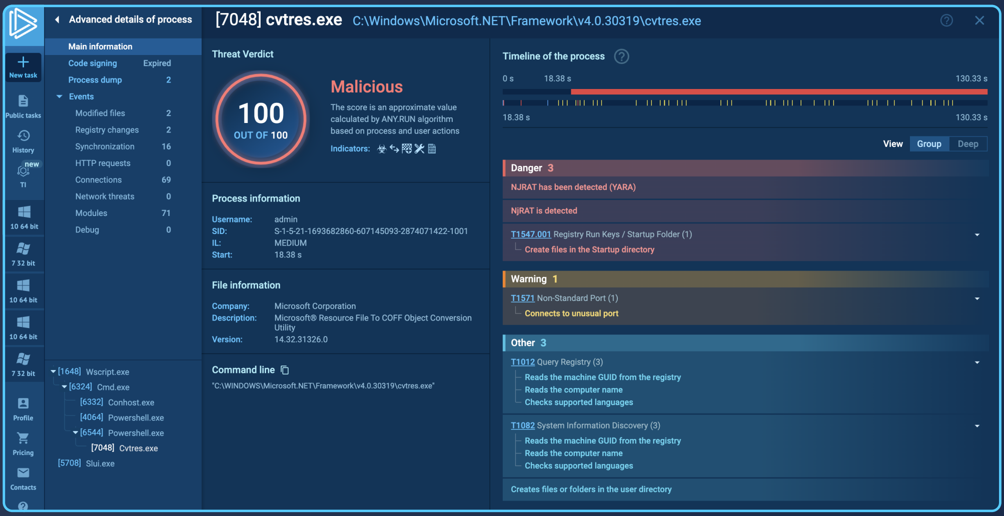
T1547.001 Registry Run Keys / Startup Folder (1)

Create files in the Startup directory

Warning 1

By clicking on a process, you can discover more information on it

The Advanced details menu can help you track the timeline of any process.



Advanced details of process

[7048] cvtres.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Main information	
Code signing	Expired
Process dump	2
Events	
Modified files	2
Registry changes	2
Synchronization	16
HTTP requests	0
Connections	69
Network threats	0
Modules	71
Debug	0

[1648] Wscript.exe
[6324] Cmd.exe
[6332] Conhost.exe
[4064] Powershell.exe
[6544] Powershell.exe
[7048] Cvtres.exe
[5708] Slui.exe

Threat Verdict

100 OUT OF 100

Malicious

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 18.38 s

File information

Company: Microsoft Corporation
Description: Microsoft® Resource File To COFF Object Conversion Utility
Version: 14.32.31326.0

Command line

"C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\cvtres.exe"

Timeline of the process

Danger 3

NJRAT has been detected (YARA)

NjRAT is detected

T1547.001 Registry Run Keys / Startup Folder (1)
Create files in the Startup directory

Warning 1

T1571 Non-Standard Port (1)
Connects to unusual port

Other 3

T1012 Query Registry (3)
Reads the machine GUID from the registry
Reads the computer name
Checks supported languages

T1082 System Information Discovery (3)
Reads the machine GUID from the registry
Reads the computer name
Checks supported languages

Creates files or folders in the user directory

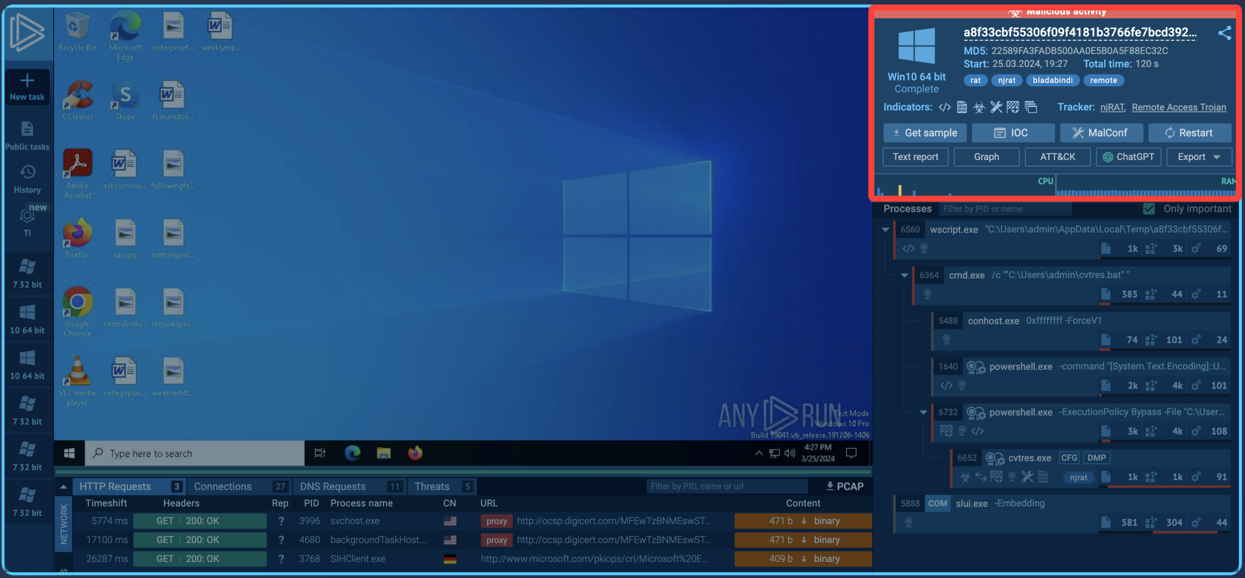
Advanced details let you discover extra information about processes

Additionally, here you can download process dumps. The complete list of process details includes:

- Modified files / Files in a raw view;
- Registry changes / Registry keys;
- Synchronization;
- HTTP Requests;
- Connections;
- Network threats;
- Modules;
- Debug.

Learn more: Fast and Simple Access to Malware Details

Access malware analysis reports



Malicious activity

a8f33cbf55306f09f4181b3766fe7bcd392...

MD5: 22589FA3FADB500AA0E5B0A5F88EC32C
Start: 25.03.2024, 19:27 **Total time:** 120 s

Win10 64 bit
Complete

rat njrat bladabindi remote

Indicators: **Tracker:** njRAT, Remote Access Trojan

```
6560 wscript.exe "C:\Users\admin\AppData\Local\Temp\a8f33cbf55306f...      1k   3k   69
  6364 cmd.exe /c ""C:\Users\admin\cvtres.bat" "                            385  44   11
    5488 conhost.exe 0xffffffff -ForceV1                                     74   101  24
    1640 powershell.exe -command "[System.Text.Encoding]::U...               2k   4k   101
    6732 powershell.exe -ExecutionPolicy Bypass -File "C:\User...            3k   4k   108
      6652 cvtres.exe CFG DMP                                  njrat         1k   1k   91
5888 COM slui.exe -Embedding                                                 581  304  44
```

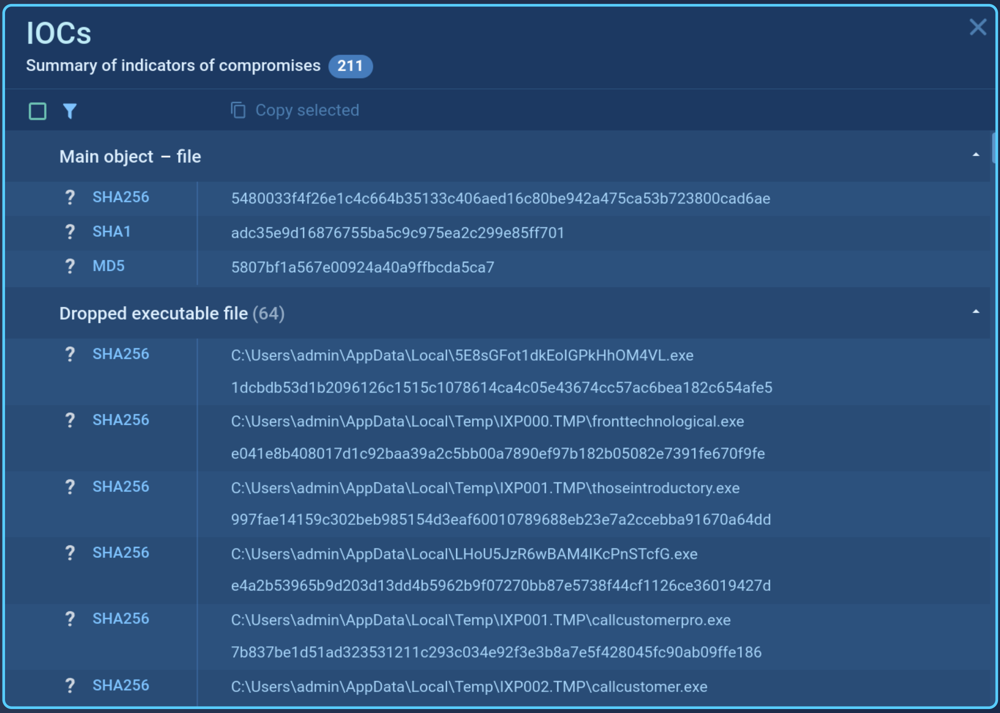
HTTP Requests 3 | Connections 27 | DNS Requests 11 | Threats 5 | Filter by PID, name or url | PCAP

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
5774 ms	GET 200: OK	?	3996	svchost.exe		proxy http://ocsp.digicert.com/MFEwTzBNMEswST...	471 b binary
17100 ms	GET 200: OK	?	4680	backgroundTaskHost....		proxy http://ocsp.digicert.com/MFEwTzBNMEswST...	471 b binary
26287 ms	GET 200: OK	?	3768	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20E...	409 b binary

This segment contains the malware analysis data that you can download

In the top right corner, you can view the key threat information generated as part of the task, including:

Indicators of compromise (IOCs)



IOCs

Summary of indicators of compromises 211

□ Copy selected

Main object – file

? SHA256	5480033f4f26e1c4c664b35133c406aed16c80be942a475ca53b723800cad6ae
? SHA1	adc35e9d16876755ba5c9c975ea2c299e85ff701
? MD5	5807bf1a567e00924a40a9ffbcda5ca7

Dropped executable file (64)

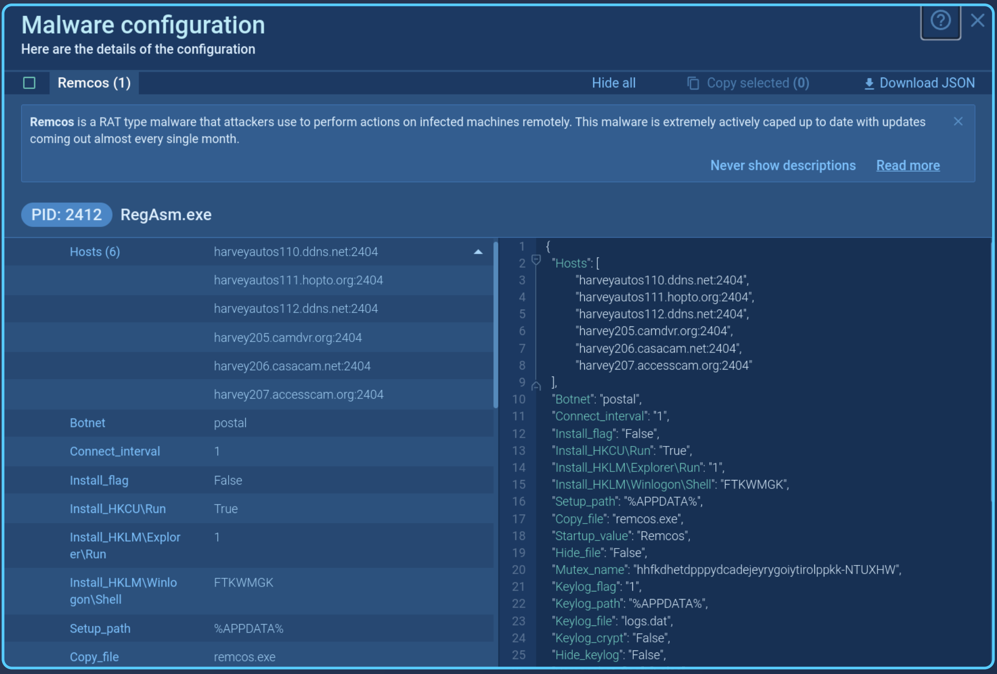
? SHA256	C:\Users\admin\AppData\Local\5E8sGFot1dkEoIGPkHhOM4VL.exe 1dcbdb53d1b2096126c1515c1078614ca4c05e43674cc57ac6bea182c654afe5
? SHA256	C:\Users\admin\AppData\Local\Temp\IXP000.TMP\fronttechnological.exe e041e8b408017d1c92baa39a2c5bb00a7890ef97b182b05082e7391fe670f9fe
? SHA256	C:\Users\admin\AppData\Local\Temp\IXP001.TMP\thoseintroductory.exe 997fae14159c302beb985154d3eaf60010789688eb23e7a2ccebba91670a64dd
? SHA256	C:\Users\admin\AppData\Local\LHoU5JzR6wBAM4IKcPnSTcfG.exe e4a2b53965b9d203d13dd4b5962b9f07270bb87e5738f44cf1126ce36019427d
? SHA256	C:\Users\admin\AppData\Local\Temp\IXP001.TMP\callcustomerpro.exe 7b837be1d51ad323531211c293c034e92f3e3b8a7e5f428045fc90ab09ffe186
? SHA256	C:\Users\admin\AppData\Local\Temp\IXP002.TMP\callcustomer.exe

ANY.RUN helps you collect fresh IOCs of the latest threats

Indicators of compromise are an essential piece of information that you can use for timely detection of malware.

Learn more: Indicators of Compromise

Malware's configuration



Malware configuration

Here are the details of the configuration

□ **Remcos (1)**   Hide all   Copy selected (0)   Download JSON

Remcos is a RAT type malware that attackers use to perform actions on infected machines remotely. This malware is extremely actively caped up to date with updates coming out almost every single month.

Never show descriptions   Read more

PID: 2412   RegAsm.exe

Hosts (6)	harveyautos110.ddns.net:2404
	harveyautos111.hopto.org:2404
	harveyautos112.ddns.net:2404
	harvey205.camdvr.org:2404
	harvey206.casacam.net:2404
	harvey207.accesscam.org:2404
Botnet	postal
Connect_interval	1
Install_flag	False
Install_HKCU\Run	True
Install_HKLM\Explorer\Run	1
Install_HKLM\Winlogon\Shell	FTKWMGK
Setup_path	%APPDATA%
Copy_file	remcos.exe

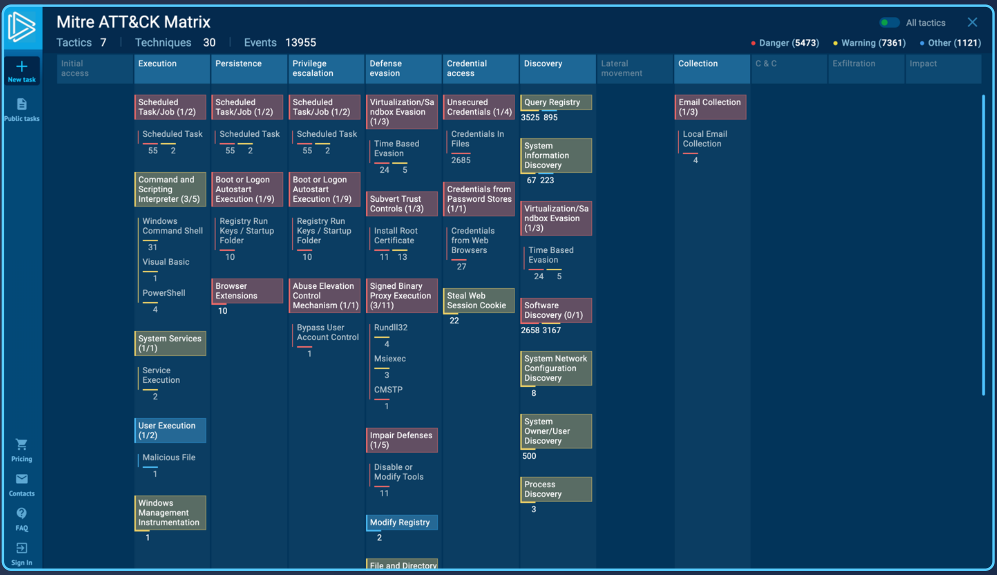
```
{
 "Hosts": [
      "harveyautos110.ddns.net:2404",
      "harveyautos111.hopto.org:2404",
      "harveyautos112.ddns.net:2404",
      "harvey205.camdvr.org:2404",
      "harvey206.casacam.net:2404",
      "harvey207.accesscam.org:2404"
 ],
 "Botnet": "postal",
 "Connect_interval": "1",
 "Install_flag": "False",
 "Install_HKCU\Run": "True",
 "Install_HKLM\Explorer\Run": "1",
 "Install_HKLM\Winlogon\Shell": "FTKWMGK",
 "Setup_path": "%APPDATA%",
 "Copy_file": "remcos.exe",
 "Startup_value": "Remcos",
 "Hide_file": "False",
 "Mutex_name": "hhfkdhetdpppydcadejeyrygoiytirolppkk-NTUXHW",
 "Keylog_flag": "1",
 "Keylog_path": "%APPDATA%",
 "Keylog_file": "logs.dat",
 "Keylog_crypt": "False",
 "Hide_keylog": "False",
```

ANY.RUN offers configurations for dozens of malware families

Malware configurations can include a variety of information, such as IP addresses and ports of C2 servers, malware family name, type, and version, encryption keys, anti-debugging, anti-sandbox, and other evasion methods, and much more.

Learn more: [Dive into Analysis with Malware Configuration]

MITRE ATT&CK Matrix



Mitre ATT&CK Matrix

Tactics 7 | Techniques 30 | Events 13955

● Danger (5473) ● Warning (7361) ● Other (1121)

Initial access

Execution
- Scheduled Task/Job (1/2)
  - Scheduled Task 55 2
- Command and Scripting Interpreter (3/5)
  - Windows Command Shell 31
  - Visual Basic 1
  - PowerShell 4
- System Services (1/1)
  - Service Execution 2
- User Execution (1/2)
  - Malicious File 1
- Windows Management Instrumentation 1

Persistence
- Scheduled Task/Job (1/2)
  - Scheduled Task 55 2
- Boot or Logon Autostart Execution (1/9)
  - Registry Run Keys / Startup Folder 10
- Browser Extensions 10

Privilege escalation
- Scheduled Task/Job (1/2)
  - Scheduled Task 55 2
- Boot or Logon Autostart Execution (1/9)
  - Registry Run Keys / Startup Folder 10
- Abuse Elevation Control Mechanism (1/1)
  - Bypass User Account Control 1

Defense evasion
- Virtualization/Sandbox Evasion (1/3)
  - Time Based Evasion 24 5
- Subvert Trust Controls (1/3)
  - Install Root Certificate 11 13
- Signed Binary Proxy Execution (3/11)
  - Rundll32 4
  - Msiexec 3
  - CMSTP 1
- Impair Defenses (1/5)
  - Disable or Modify Tools 11
- Modify Registry 2
- File and Directory

Credential access
- Unsecured Credentials (1/4)
  - Credentials In Files 2685
- Credentials from Password Stores (1/1)
  - Credentials from Web Browsers 27
- Steal Web Session Cookie 22

Discovery
- Query Registry 3525 895
- System Information Discovery 67 223
- Virtualization/Sandbox Evasion (1/3)
  - Time Based Evasion 24 5
- Software Discovery (0/1) 2658 3167
- System Network Configuration Discovery 8
- System Owner/User Discovery 500
- Process Discovery 3

Lateral movement

Collection
- Email Collection (1/3)
  - Local Email Collection 4

C & C

Exfiltration

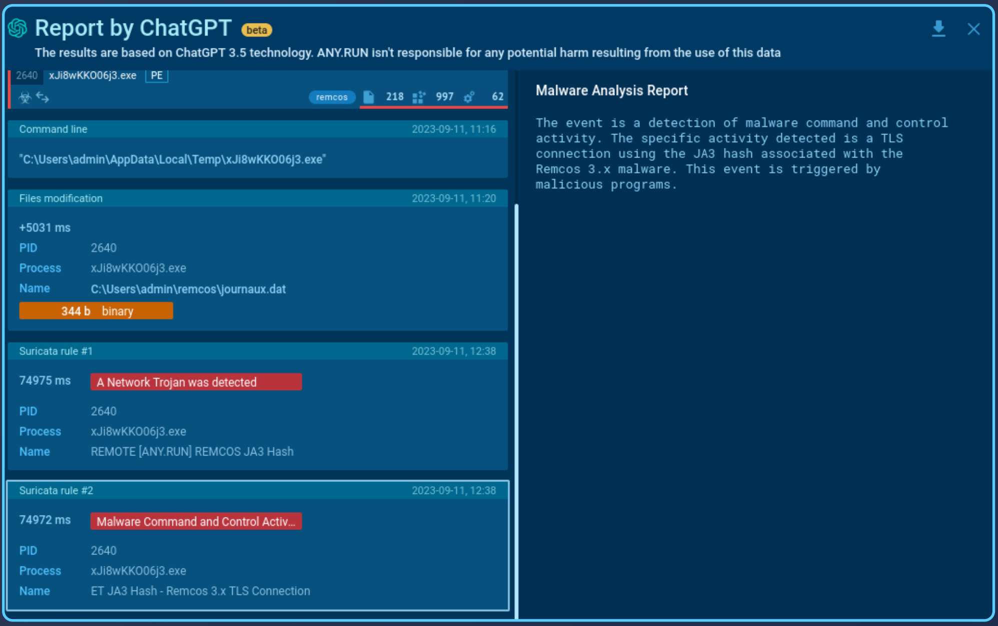
Impact

Analyze malware and see which tactics it employs

The built-in MITRE ATT&CK Matrix allows you to view the techniques utilized by the malware with action mapping and explore each of them.

Learn more: [MITRE ATT&CK Matrix]

ChatGPT insights (Available only for public tasks)



Report by ChatGPT beta

The results are based on ChatGPT 3.5 technology. ANY.RUN isn't responsible for any potential harm resulting from the use of this data

2640 xJi8wKKO06j3.exe PE

remcos 218 997 62

Command line 2023-09-11, 11:16

"C:\Users\admin\AppData\Local\Temp\xJi8wKKO06j3.exe"

Files modification 2023-09-11, 11:20

+5031 ms

PID	2640
Process	xJi8wKKO06j3.exe
Name	C:\Users\admin\remcos\journaux.dat

344 b binary

Suricata rule #1 2023-09-11, 12:38

74975 ms A Network Trojan was detected

PID	2640
Process	xJi8wKKO06j3.exe
Name	REMOTE [ANY.RUN] REMCOS JA3 Hash

Suricata rule #2 2023-09-11, 12:38

74972 ms Malware Command and Control Activ...

PID	2640
Process	xJi8wKKO06j3.exe
Name	ET JA3 Hash - Remcos 3.x TLS Connection

Malware Analysis Report

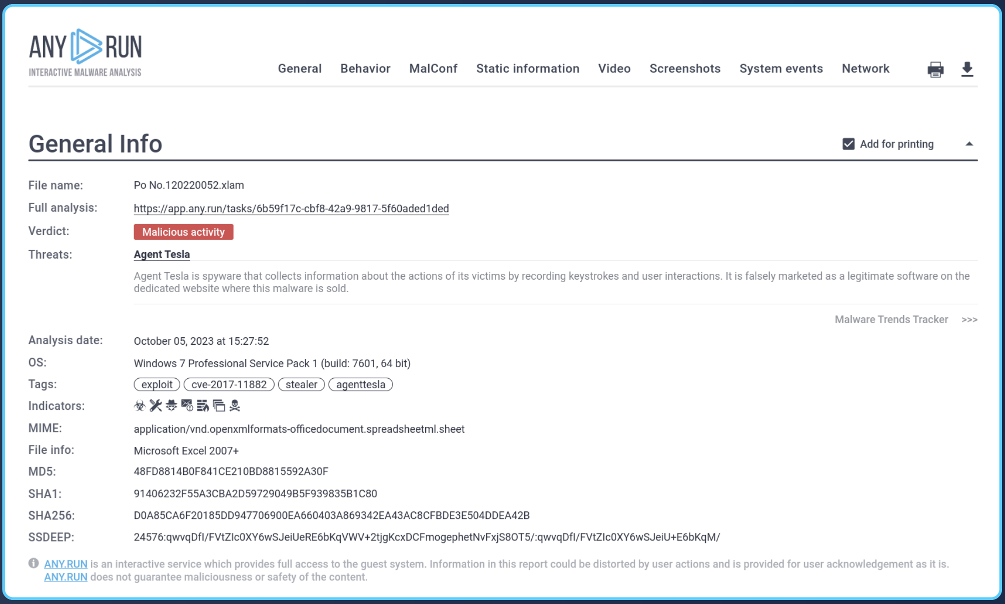
```
The event is a detection of malware command and control
activity. The specific activity detected is a TLS
connection using the JA3 hash associated with the
Remcos 3.x malware. This event is triggered by
malicious programs.
```

Discover AI-generated explanations of different elements detected by ANY.RUN

This feature provides you with a deeper understanding of malware's behavior by providing AI-powered explanations of important elements, such as processes, rules, and connections. To use this feature, simply click on the ChatGPT icon next to any important element in your report.

Learn more: Sandbox Results with ChatGPT

Malware analysis text report



General Info

☑ Add for printing

File name:	Po No.120220052.xlam
Full analysis:	https://app.any.run/tasks/6b59f17c-cbf8-42a9-9817-5f60aded1ded
Verdict:	Malicious activity
Threats:	Agent Tesla Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold. Malware Trends Tracker >>>
Analysis date:	October 05, 2023 at 15:27:52
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 64 bit)
Tags:	exploit cve-2017-11882 stealer agenttesla
Indicators:	
MIME:	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
File info:	Microsoft Excel 2007+
MD5:	48FD8814B0F841CE210BD8815592A30F
SHA1:	91406232F55A3CBA2D59729049B5F939835B1C80
SHA256:	D0A85CA6F20185DD947706900EA660403A869342EA43AC8CFBDE3E504DDEA42B
SSDEEP:	24576:qwvqDfI/FVtZIc0XY6wSJeiUeRE6bKqVWV+2tjgKcxDCFmogephetNvFxjS8OT5/:qwvqDfI/FVtZIc0XY6wSJeiU+E6bKqM/

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Each task contains an analytical report on the sample you provide

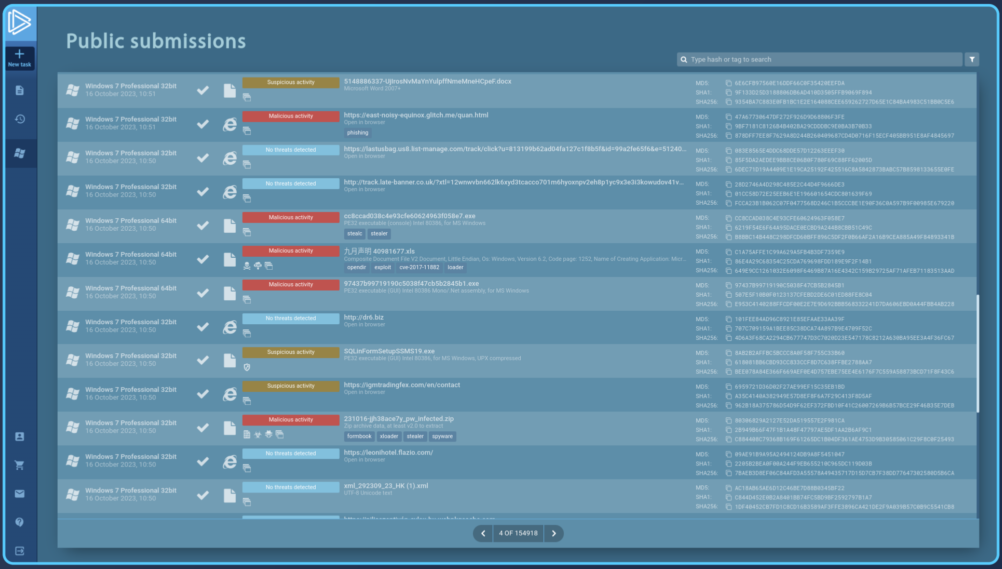
The sandbox generates a comprehensive report for each file and URL you analyze. It includes all of the details we mentioned earlier. The report can be exported in your preferred format, including JSON and HTML.

Learn more: Malware Analysis Report in One Click

Restart the task

You can always restart any task with different VM settings to test a sample in a new environment.

Working with public malware samples



Public submissions

Type hash or tag to search

Windows 7 Professional 32bit 16 October 2023, 10:51	Suspicious activity	5148886337-UjIrosNvMaYnYulpffNmeMneHCpeF.docx Microsoft Word 2007+	MD5: 6E6CFB97560E16DDF66C0F35420EEFDA SHA1: 9F133D25D3188806DB6AD410D3505FFB9069F894 SHA256: 9354BA7C883E0FB1BC1E2E164088CEE659262727D65E1C84BA4983C51BB0C5E6
Windows 7 Professional 32bit 16 October 2023, 10:51	Malicious activity	https://east-noisy-equinox.glitch.me/quan.html Open in browser phishing	MD5: 47A67730647DF272F926D9D68806F3FE SHA1: 9BF7181C8126B4B402BA29CDDDBC9E0BA3B70B33 SHA256: 878DFF7EE8F7629A8D244B260409687CD4D0716F15ECF405BB951E8AF4845697
Windows 7 Professional 32bit 16 October 2023, 10:50	No threats detected	https://lastusbag.us8.list-manage.com/track/click?u=813199b62ad04fa127c1f8b5f&id=99a2fe65f6&e=51240... Open in browser	MD5: 083E8565E4DDC68DDE57D12263EEEF30 SHA1: 85F5DA2AEDEE9BB8CE06B0F780F69C88FF62005D SHA256: 6DEC71D19A4409E1E19CA25192F425516C8A5842873BABC57B8598133655E0FE
Windows 7 Professional 32bit 16 October 2023, 10:50	No threats detected	http://track.late-banner.co.uk/?xtl=12wnwvbn662lk6xyd3tcacco701m6hyoxnpv2eh8p1yc9x3e3i3kowudov41v... Open in browser	MD5: 28D2746A4D298C485E2C44D4F9666DE3 SHA1: 01CC58D72E25EEB6E1E196601654CDC801639F69 SHA256: FCCA23B1B062C07F0477568D246C1B5CCCBE1E90F36C0A597B9F00985E679220
Windows 7 Professional 64bit 16 October 2023, 10:50	Malicious activity	cc8ccad038c4e93cfe60624963f058e7.exe PE32 executable (console) Intel 80386, for MS Windows stealc stealer	MD5: CC8CCAD038C4E93CFE60624963F058E7 SHA1: 6219F54E6F64A95DACE0ECBD9A244B8CBB51C49C SHA256: B8BBC14B448C298DFCD60BFF896C5DF2F0B66AF2A16B9CEA885A49F84893341B
Windows 7 Professional 64bit 16 October 2023, 10:50	Malicious activity	九月声明 40981677.xls Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Name of Creating Application: Micr... opendir exploit cve-2017-11882 loader	MD5: C1A75AFFE1C99A629A5FB4B3DF7359E9 SHA1: 86E4A29C68354C25CDA769698FDD189E9F2F14B1 SHA256: 649E9CC1261032E6098F6469B87A16E4342C159B29725AF71AFEB71183513AAD
Windows 7 Professional 64bit 16 October 2023, 10:50	Malicious activity	97437b99719190c5038f47cb5b2845b1.exe PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows	MD5: 97437B99719190C5038F47CB5B2845B1 SHA1: 507E5F10B0F0123137CFEBD2DE6C01ED88FE8C04 SHA256: E953C4140288FFCDF00E2E7E9D692BBB568332241D7DA606EBD0A44FBB4AB228
Windows 7 Professional 32bit 16 October 2023, 10:50	No threats detected	http://dr6.biz Open in browser	MD5: 101FEE84AD96C8921E85EFAAE33AA39F SHA1: 707C709159A1BEE85C38DCA74A897B9E4709F52C SHA256: 4D6A3F68CA2294CB677747D3C7020D23E547178C8212A630BA95EE3A4F36FC67
Windows 7 Professional 32bit 16 October 2023, 10:50	Suspicious activity	SQLinFormSetupSSMS19.exe PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed	MD5: 8AB2B2AFFBC5BCCC8A0F58F755C33B60 SHA1: 618081BB6CBD93CC833CCF8D7C638FFBE2788AA7 SHA256: BEE078A84E366F669AEF0E4D757EBE75EE4E6176F7C559A58873BCD71F8F43C6
Windows 7 Professional 32bit 16 October 2023, 10:50	Suspicious activity	https://igmtradingfex.com/en/contact Open in browser	MD5: 6959721D36D02F27AE99EF15C35EB1BD SHA1: A35C4140A382949E57D8EF8F6A7F29C413F8D5AF SHA256: 962B18A375786D54D9F62EF372FBD10F41C26007269B6B57BCE29F46B35E7DEB
Windows 7 Professional 32bit 16 October 2023, 10:50	Malicious activity	231016-jjh38ace7y_pw_infected.zip Zip archive data, at least v2.0 to extract formbook xloader stealer spyware	MD5: 80306829A2127E52DA519557E2F981CA SHA1: 2B949B66F47F1B1A48F47797AE5DF1AA2B6AF9C1 SHA256: C884408C79368B169F61265DC1B04DF361AE4753D9B30585061C29F8C0F25493
Windows 7 Professional 32bit 16 October 2023, 10:50	No threats detected	https://leonihotel.flazio.com/ Open in browser	MD5: 09AE91B9A95A2494124DB9A8F5451047 SHA1: 2205B2BEA0F00A244F9EB655210C965DC119D03B SHA256: 7BAEB3D8EF06C84AFD3A55578A49435717D15D7CB7F38DD77647302580D5B6CA
Windows 7 Professional 32bit 16 October 2023, 10:50	No threats detected	xml_292309_23_HK (1).xml UTF-8 Unicode text	MD5: AC18AB65AE6D12C46BE7D88B0345BF22 SHA1: C844D452E0B2A8401BB74FC5BD9BF2592797B1A7 SHA256: 1DF40452CB7FD1C8CD16B3589AF3FFE3896CA421DE2F9A039B57C0B9C5541CB8

Use the database to stay up-to-date on the latest threats

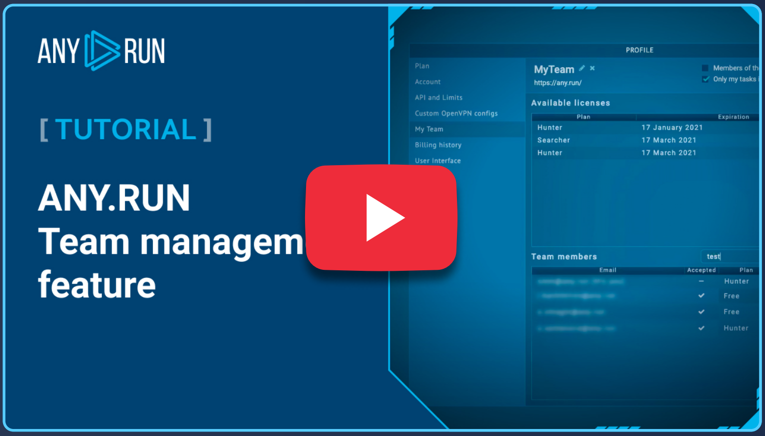
In addition to analyzing your own samples, you can access ANY.RUN's database of over 6 million malware samples submitted by users from around the world.

Learn more: How to Get Free Malware Samples and Reports

Managing a team

All Enterprise-plan users can take advantage of the Teamwork feature that allows analysts to work together on different samples in real time.

It makes it easy to monitor your team's activities and train junior analysts. It is also a great way to track productivity and manage large, dynamic teams.



Available licenses

Plan	Expiration
Hunter	17 January 2021
Searcher	17 March 2021
Hunter	17 March 2021

Team members test

Email	Accepted	Plan
[redacted]	–	Hunter
[redacted]	✓	Free
[redacted]	✓	Free
[redacted]	✓	Hunter

Teamwork can significantly improve the efficiency of your team.

Here are some of its benefits:

- **Real-time collaboration:** Analysts can join their forces, saving time and improving accuracy.
- **Common task history:** Team history can be configured to show all tasks, only the leader's tasks, or only links to the leader's tasks.
- **Employee activity tracking:** Team leaders can view employee activity, which can help them identify areas where training or extra resources are needed.
- **Subscription management:** Team leaders can manage subscriptions and assign licenses to team members.

Learn more: Teamwork

Conclusion

ANY.RUN is your best tool for both static and dynamic malware analysis. Run an unlimited number of tasks, explore millions of reports and malware samples, and collect valuable data by studying the ins and outs of malicious programs and links. With our cloud-based sandbox, your threat investigations will become a walk in the park.

Unlock the full potential of ANY.RUN with a 14-day free trial!