ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	AdwereCleaner.exe
Full analysis:	https://app.any.run/tasks/102bd588-0dc7-4d48-855d-fb42bdaca895
Verdict:	Malicious activity
Analysis date:	October 28, 2024 at 14:34:23
OS:	Windows 10 Professional (build: 19045, 64 bit)
Indicators:	
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive, 5 sections
MD5:	248AADD395FFA7FFB1670392A9398454
SHA1:	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5
SHA256:	51290129CCCCA38C6E3B4444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC
SSDEEP:	3072:15TDpNFVbxDSXJFFGhcBR1WLZ37p73G8Wn7GIDOg+ELqdSxo5XtlZjnvxRJgghaR:157TcfFPB6B3GL7g+me5aZjn5VlI9T/

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- 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 Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package

- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- ProfessionalEdition
- QuickAssist Package
- QuickAssist Package
- RollupFix
- RollupFix
- ServicingStack
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- TabletPCMath Package
- TabletPCMath Package
- UserExperience Desktop Package
- UserExperience Desktop Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package

Behavior activities

MALICIOUS

No malicious indicators.

SUSPICIOUS

Reads security settings of Internet Explorer
- AdwereCleaner.exe (PID: 1176)

Executable content was dropped or overwritten
- AdwereCleaner.exe (PID: 1176)

INFO

Creates files or folders in the user directory
- AdwereCleaner.exe (PID: 1176)

Reads the computer name
- AdwereCleaner.exe (PID: 1176)

The process uses the downloaded file
- AdwereCleaner.exe (PID: 1176)

Checks supported languages
- AdwereCleaner.exe (PID: 1176)

Process checks computer location settings
- AdwereCleaner.exe (PID: 1176)

Malware configuration

No Malware configuration.

Static information

TRiD

.exe | NSIS - Nullsoft Scriptable Install System (91.9)
.exe | Win32 Executable MS Visual C++ (generic) (3.3)
.exe | Win64 Executable (generic) (3)
.dll | Win32 Dynamic Link Library (generic) (0.7)
.exe | Win32 Executable (generic) (0.4)

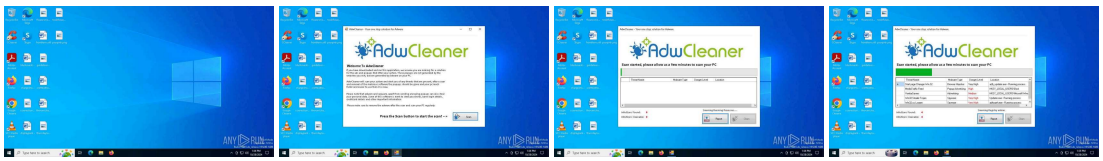
EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2013:12:25 05:01:41+00:00
ImageFileCharacteristics:	No relocs, Executable, No line numbers, No symbols, 32-bit
PEType:	PE32
LinkerVersion:	6
CodeSize:	24064
InitializedDataSize:	162816
UninitializedDataSize:	1024
EntryPoint:	0x30e4
OSVersion:	4
ImageVersion:	6
SubsystemVersion:	4

Subsystem:	Windows GUI

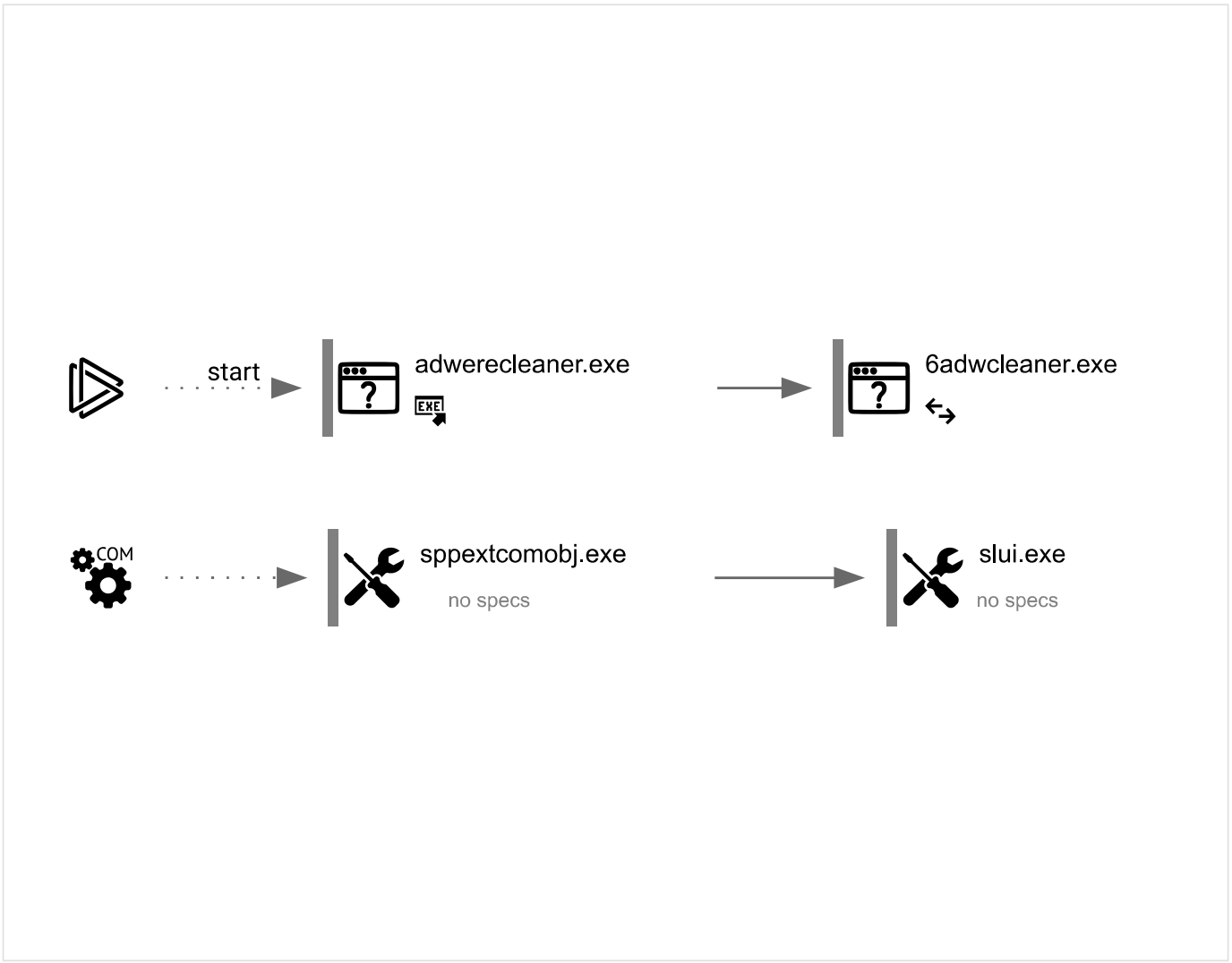
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
132	4	0	0

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
1176	"C:\Users\admin\AppData\Local\Temp\AdwereCleaner.exe"	C:\Users\admin\AppData\Local\Temp\AdwereCleaner.exe		explorer.exe
Information				
User: admin	Integrity Level: MEDIUM			
Exit code: 0				
6592	"C:\Users\admin\AppData\Local\6AdwCleaner.exe"	C:\Users\admin\AppData\Local\6AdwCleaner.exe		AdwereCleaner.exe

Information

User:	admin	Integrity Level:	MEDIUM
Description:	AdwareBooC	Version:	1.0.0.0

6504 C:\WINDOWS\system32\SppExtComObj.exe -Embedding C:\Windows\System32\SppExtComObj.Exe – svchost.exe

Information

User:	NETWORK SERVICE	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	KMS Connection Broker
Version:	10.0.19041.3996 (WinBuild.160101.0800)		

5896 "C:\WINDOWS\System32\SLUI.exe" RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Action=AutoActivate;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=4de7cb65-cdf1-4de9-8ae8-e3cce27b9f2c;NotificationInterval=1440;Trigger=TimerEvent C:\Windows\System32\slui.exe – SppExtComObj.Exe

Information

User:	NETWORK SERVICE	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	Windows Activation Client
Version:	10.0.19041.1 (WinBuild.160101.0800)		

Registry activity

Total events	Read events	Write events	Delete events
4 329	4 313	16	0

Modification events

(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableFileTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableAutoFileTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableConsoleTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	FileTracingMask
Value:			
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	ConsoleTracingMask
Value:			
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	MaxFileSize
Value:	1048576		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableFileTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableAutoFileTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableConsoleTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	FileTracingMask
Value:			
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	ConsoleTracingMask

Value:

(PID) Process: (6592) 6AdwCleaner.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation: write Name: MaxFileSize
Value: 1048576

(PID) Process: (6592) 6AdwCleaner.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation: write Name: FileDirectory
Value: %windir%\tracing

(PID) Process: (6592) 6AdwCleaner.exe Key: HKEY_CURRENT_USER\SOFTWARE\AdwCleaner
Operation: write Name: id
Value: 0

(PID) Process: (6592) 6AdwCleaner.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation: write Name: AdwCleaner
Value: "C:\Users\admin\AppData\Local\6AdwCleaner.exe" -auto

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	6	0	0

Dropped files

PID	Process	Filename	Type
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F MD5: ABFA2E894B4479D44DEE722D520492D1 SHA256: 4DF7CA15EE8FD8AAEA113F6DA6CE752B5E2ECFEAB4673878ED56476A1A120466	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F4D9C889B7AEBCF4E1A2DAABC5C3628A_77D782D611E65A2A81EA974847CB0C84 MD5: 5E8CA0A2FE32380587F51F8C1A17E693 SHA256: 906FAEB2DA09C0A88200DF01E365E23A70CA5DF38C894C9F5D7830D523AE6424	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1F356F4D07FE8C483E769E4586569404 MD5: C6680BC4DFC37EB388A992DC25BE6D97 SHA256: 229F7DB821AE0B3B901BC9FB04739B6D4E2B17FF797FFE7197A869735485DDAF	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F MD5: 9F886DF6518081483BD277BB2926D56F SHA256: 7701277481103526O7DBBF4D962E7302282B45C4F480B2EA32A9F274B4DD43D4	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F4D9C889B7AEBCF4E1A2DAABC5C3628A_77D782D611E65A2A81EA974847CB0C84 MD5: 36F43D8EB4DCB4C4B31E0665B6305B52 SHA256: BE76D817AA4B8027F36E4E9C373546742A65478791154984B339D25711432DC3	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1F356F4D07FE8C483E769E4586569404 MD5: A6DDBCCF4CEDE94A5EA0BA756C30EA33 SHA256: 3B122677ED438603E184AB3EC9A5C74AF281D4312B38B3380CD91E5933093C10	binary
1176	AdwereCleaner.exe	C:\Users\admin\AppData\Local\6AdwCleaner.exe MD5: 87E4959FEFEC297EBBF42DE79B5C88F6 SHA256: 4F0033E811FE2497B38F0D45DF958829D01933EBE7D331079EEFC8E38FBEAA61	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
11	49	26	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
–	–	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	–	–	unknown
–	–	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	unknown
–	–	GET	200	2.16.164.106:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	unknown
4376	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	unknown
6592	6AdwCleaner.exe	GET	200	104.18.38.233:80	http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRtl6lMY2%2BiPob4twryIF%2BFfgUdvwQUK8NGq7oOyWUqRtF5R8Ri4uHa%2FLgCEBBwnU%2F1VAjXMGAB2OqRdbs%3D	unknown	–	–	unknown

6592	6AdwCleaner.exe	GET	200	172.64.149.23:80	http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSOJaE2H4hHYQzP74hlLuO41NG%2BEAQUHsWxLH2H2gJofCW8DAeEP7bP3vECEFGC5bJKS84miWDFSzbnHQI%3D	unknown	–	–	unknown
6720	backgroundTaskHost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDIQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHI3O1J0%3D	unknown	–	–	unknown
6592	6AdwCleaner.exe	GET	200	172.64.149.23:80	http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSOJaE2H4hHYQzP74hlLuO41NG%2BEAQUHsWxLH2H2gJofCW8DAeEP7bP3vECEFGC5bJKS84miWDFSzbnHQI%3D	unknown	–	–	unknown
5284	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	unknown
5284	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	unknown
6592	6AdwCleaner.exe	GET	200	104.18.38.233:80	http://crl.comodoca.com/COMODOCodeSigningCA2.crl	unknown	–	–	unknown

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	–	–	–	whitelisted
6944	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5488	MoUsoCoreWorker.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
–	–	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
–	–	2.16.164.106:80	crl.microsoft.com	Akamai International B.V.	NL	unknown
–	–	88.221.169.152:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
4360	SearchApp.exe	2.23.209.186:443	www.bing.com	Akamai International B.V.	GB	unknown
–	–	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
4376	svchost.exe	40.126.31.73:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
4376	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
4360	SearchApp.exe	2.23.209.144:443	th.bing.com	Akamai International B.V.	GB	unknown
6592	6AdwCleaner.exe	104.18.38.233:80	ocsp.usertrust.com	CLOUDFLARENET	–	shared
6592	6AdwCleaner.exe	172.64.149.23:80	ocsp.usertrust.com	CLOUDFLARENET	US	unknown
780	svchost.exe	23.52.181.141:443	go.microsoft.com	Akamai International B.V.	US	unknown
6944	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2852	svchost.exe	40.113.103.199:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6720	backgroundTaskHost.exe	20.223.35.26:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
6720	backgroundTaskHost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
6720	backgroundTaskHost.exe	20.103.156.88:443	fd.api.iris.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	unknown
4360	SearchApp.exe	92.123.104.45:443	www.bing.com	Akamai International B.V.	DE	unknown
5284	SIHClient.exe	4.245.163.56:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
5284	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
5284	SIHClient.exe	40.69.42.241:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
4020	svchost.exe	239.255.255.250:1900	–	–	–	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	20.73.194.208 40.127.240.158	whitelisted
crl.microsoft.com	2.16.164.106 2.16.164.9	whitelisted
www.microsoft.com	88.221.169.152 23.35.229.160	whitelisted

www.bing.com	2.23.209.186 2.23.209.185 2.23.209.173 2.23.209.182 2.23.209.177 2.23.209.183 2.23.209.178 2.23.209.188 2.23.209.181 92.123.104.45 92.123.104.38 92.123.104.36 92.123.104.44 92.123.104.46 92.123.104.37 92.123.104.40 92.123.104.47 92.123.104.48	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
google.com	142.250.186.78	whitelisted
www.vikingwebscanner.com	–	malicious
login.live.com	40.126.31.73 40.126.31.67 20.190.159.23 20.190.159.4 20.190.159.0 20.190.159.71 40.126.31.69 20.190.159.73	whitelisted
th.bing.com	2.23.209.144 2.23.209.141 2.23.209.140 2.23.209.150 2.23.209.154 2.23.209.149 2.23.209.148 2.23.209.142 2.23.209.143	whitelisted
ocsp.usertrust.com	104.18.38.233 172.64.149.23	whitelisted
ocsp.comodoca.com	172.64.149.23 104.18.38.233	whitelisted
crl.comodoca.com	104.18.38.233 172.64.149.23	whitelisted
go.microsoft.com	23.52.181.141	whitelisted
client.wns.windows.com	40.113.103.199	whitelisted
arc.msn.com	20.223.35.26	whitelisted
fd.api.iris.microsoft.com	20.103.156.88	whitelisted
slscr.update.microsoft.com	4.245.163.56	whitelisted
fe3cr.delivery.mp.microsoft.com	40.69.42.241	whitelisted
nexusrules.officeapps.live.com	52.111.236.22	whitelisted

Threats

No threats detected

Debug output strings

No debug info