






General Info

File name:	AdwereCleaner.exe
Full analysis:	<a href="https://app.any.run/tasks/7eb52e8d-98c1-4cbb-98b1-9f9ea413b4ba">https://app.any.run/tasks/7eb52e8d-98c1-4cbb-98b1-9f9ea413b4ba</a>
Verdict:	Malicious activity
Analysis date:	September 05, 2024 at 22:56:53
OS:	Windows 10 Professional (build: 19045, 64 bit)
Indicators:	  
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
MD5:	248AADD395FFA7FFB1670392A9398454
SHA1:	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5
SHA256:	51290129CCCCA38C6E3B4444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC
SSDEEP:	3072:15TDpNFVbxDXJFFGhcBR1WLZ37p73G8Wn7GID0g+ELqdSxo5XtlZjnvxRJgghaR:157TcfFPB63GL7g+me5aZjn5VII9T/

Software environment set and analysis options

Launch configuration

Task duration:	150 seconds	Heavy Evasion option:		Network geolocation:	off
Additional time used:	none	MITM proxy:	on	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
- DotNetRollup
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face 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
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- QuickAssist Package
- RollupFix
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- TabletPCMath Package
- UserExperience Desktop Package
- WordPad 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)

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
<p>Changes the autorun value in the registry</p> <ul style="list-style-type: none"><li>• 6AdwCleaner.exe (PID: 6296)</li></ul>	<p>Reads security settings of Internet Explorer</p> <ul style="list-style-type: none"><li>• AdwereCleaner.exe (PID: 6808)</li><li>• 6AdwCleaner.exe (PID: 6296)</li></ul> <p>Executable content was dropped or overwritten</p> <ul style="list-style-type: none"><li>• AdwereCleaner.exe (PID: 6808)</li></ul>	<p>Creates files or folders in the user directory</p> <ul style="list-style-type: none"><li>• AdwereCleaner.exe (PID: 6808)</li></ul> <p>Checks supported languages</p> <ul style="list-style-type: none"><li>• AdwereCleaner.exe (PID: 6808)</li><li>• 6AdwCleaner.exe (PID: 6296)</li></ul> <p>Reads the computer name</p> <ul style="list-style-type: none"><li>• AdwereCleaner.exe (PID: 6808)</li><li>• 6AdwCleaner.exe (PID: 6296)</li></ul> <p>Process checks computer location settings</p> <ul style="list-style-type: none"><li>• AdwereCleaner.exe (PID: 6808)</li></ul> <p>Reads Environment values</p> <ul style="list-style-type: none"><li>• 6AdwCleaner.exe (PID: 6296)</li></ul> <p>The process uses the downloaded file</p> <ul style="list-style-type: none"><li>• AdwereCleaner.exe (PID: 6808)</li></ul> <p>Reads the machine GUID from the registry</p> <ul style="list-style-type: none"><li>• 6AdwCleaner.exe (PID: 6296)</li></ul> <p>Disables trace logs</p> <ul style="list-style-type: none"><li>• 6AdwCleaner.exe (PID: 6296)</li></ul> <p>Checks proxy server information</p> <ul style="list-style-type: none"><li>• 6AdwCleaner.exe (PID: 6296)</li></ul>

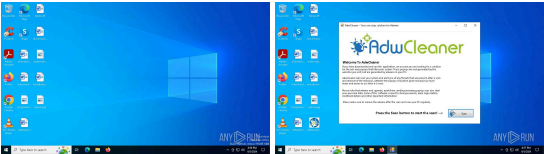
Malware configuration

No Malware configuration.

Static information

TRiD	EXIF																										
<div><p>.exe   NSIS - Nullsoft Scriptable Install System (91.9)</p><p>.exe   Win32 Executable MS Visual C++ (generic) (3.3)</p><p>.exe   Win64 Executable (generic) (3)</p><p>.dll   Win32 Dynamic Link Library (generic) (0.7)</p><p>.exe   Win32 Executable (generic) (0.4)</p></div>	<div><p>EXE</p><table><tr><td>MachineType:</td><td>Intel 386 or later, and compatibles</td></tr><tr><td>TimeStamp:</td><td>2013:12:25 05:01:41+00:00</td></tr><tr><td>ImageFileCharacteristics:</td><td>No relocs, Executable, No line numbers, No symbols, 32-bit</td></tr><tr><td>PEType:</td><td>PE32</td></tr><tr><td>LinkerVersion:</td><td>6</td></tr><tr><td>CodeSize:</td><td>24064</td></tr><tr><td>InitializedDataSize:</td><td>162816</td></tr><tr><td>UninitializedDataSize:</td><td>1024</td></tr><tr><td>EntryPoint:</td><td>0x30e4</td></tr><tr><td>OSVersion:</td><td>4</td></tr><tr><td>ImageVersion:</td><td>6</td></tr><tr><td>SubsystemVersion:</td><td>4</td></tr><tr><td>Subsystem:</td><td>Windows GUI</td></tr></table></div>	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
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																										

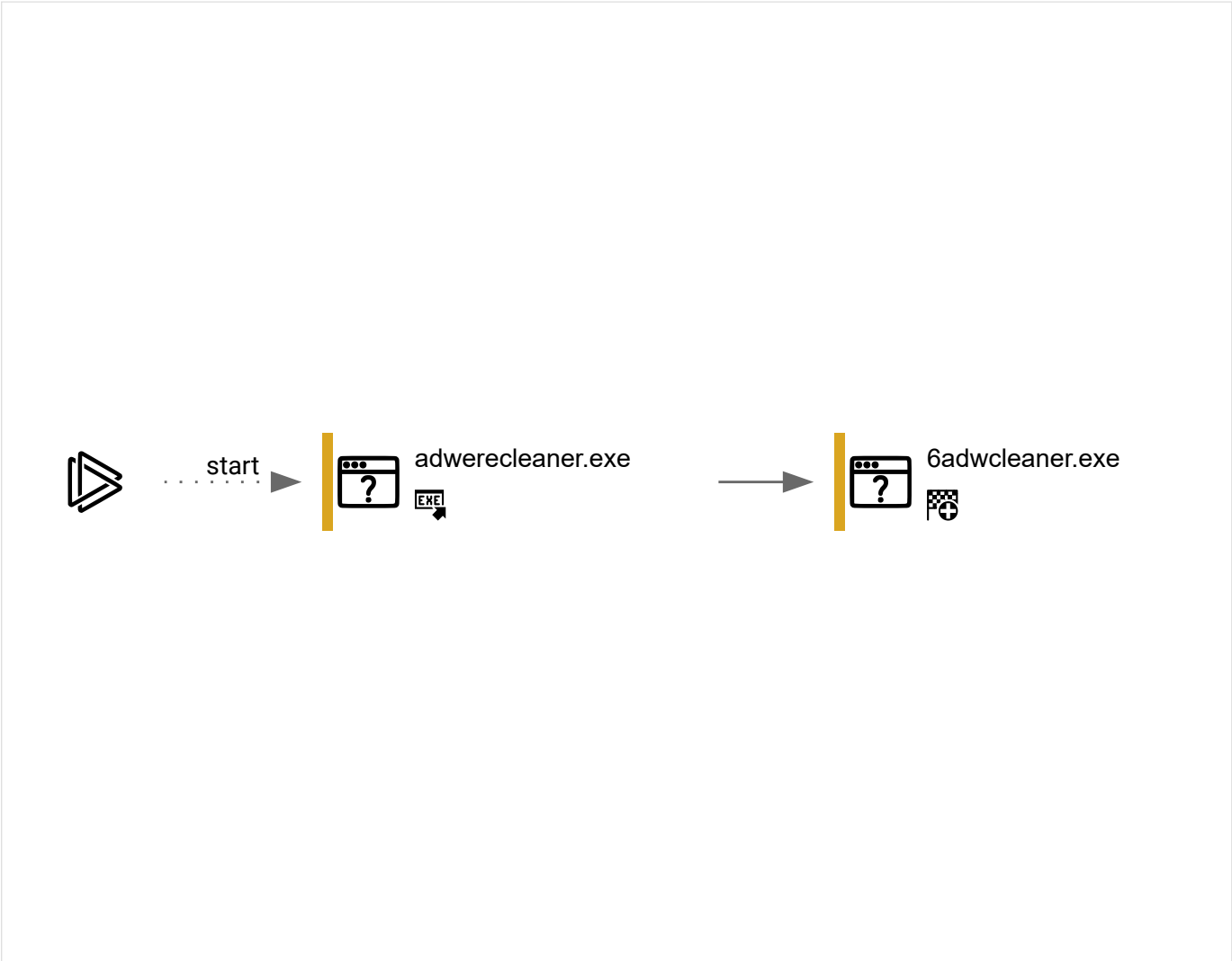
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
122	2	0	2

Behavior graph



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

Process information

PID	CMD	Path	Indicators	Parent process
6296	"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		
6808	"C:\Users\admin\Desktop\AdwereCleaner.exe"	C:\Users\admin\Desktop\AdwereCleaner.exe		explorer.exe

Information			
User:	admin	Integrity Level:	MEDIUM
Exit code:	0		

Registry activity

Total events	Read events	Write events	Delete events
1 042	1 026	16	0

Modification events

(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableFileTracing
Value:	0		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableAutoFileTracing
Value:	0		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableConsoleTracing
Value:	0		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	FileTracingMask
Value:			
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	ConsoleTracingMask
Value:			
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	MaxFileSize
Value:	1048576		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableFileTracing
Value:	0		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableAutoFileTracing
Value:	0		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableConsoleTracing
Value:	0		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	FileTracingMask
Value:			
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	ConsoleTracingMask
Value:			
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	MaxFileSize
Value:	1048576		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		
(PID) Process:	(6296) 6AdwCleaner.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\AdwCleaner
Operation:	write	Name:	id
Value:	0		
(PID) Process:	(6296) 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	0	0	0

Dropped files

PID	Process	Filename	Type
6808	AdwreCleaner.exe	C:\Users\admin\AppData\Local\6AdwCleaner.exe MD5: 87E4959FEFEC297EBBF42DE79B5C88F6	SHA256: 4F0033E811FE2497B38F0D45DF958829D01933EBE7D331079EEFC8E38FBEEA61 executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
3	17	5	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6456	RUXIMICS.exe	GET	200	184.30.21.171:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	—	—	whitelisted
568	svchost.exe	GET	200	184.30.21.171:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	—	—	whitelisted
2120	MoUsoCoreWorker.exe	GET	200	184.30.21.171:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
—	—	192.168.100.255:138	—	—	—	whitelisted
568	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
2120	MoUsoCoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6456	RUXIMICS.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
568	svchost.exe	184.30.21.171:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6456	RUXIMICS.exe	184.30.21.171:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
2120	MoUsoCoreWorker.exe	184.30.21.171:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
3888	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
4324	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	51.104.136.2	whitelisted
google.com	142.250.186.174	whitelisted
www.vikingwebscanner.com	—	malicious
www.microsoft.com	184.30.21.171	whitelisted

Threats

No threats detected

Debug output strings

No debug info

