

General Info

File name: 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.zip

Full analysis: <https://app.any.run/tasks/e4979ab7-3145-4121-a042-ea91d7e2c86b>

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.

Analysis date: January 26, 2021 at 20:39:47

OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Tags: rat agenttesla trojan

Indicators: 

MIME: application/zip

File info: Zip archive data, at least v5.1 to extract

MD5: E0C049B213F76DC3A9133B78EBEB18B8

SHA1: F33E372DE178076C3476322E97C0E80F9E36BFE2

SHA256: 1D4C38DAEAA29E6AF28D94B4C50711DB0FCD74ED356E191B231F3CA871362FFC

SSDEEP: 12288:cAHNvuO1yx3JiNsKpTR9kRPwqK94zj+L2:cMNvuOKZ+xTR9mPlij9

Software environment set and analysis options

Launch configuration

| | | | | | |
|-----------------------|-------------|-----------------------|-----|--------------------------|-------------------|
| Task duration: | 240 seconds | Heavy Evasion option: | off | Network geolocation: | off |
| Additional time used: | 180 seconds | MITM proxy: | off | Privacy: | Public submission |
| Fakenet option: | off | Route via Tor: | off | Autoconfirmation of UAC: | on |
| Network: | on | | | | |

Software preset

- Internet Explorer 11.0.9600.17843 KB3058515
- Adobe Acrobat Reader DC MUI (15.023.20070)
- Adobe Flash Player 26 ActiveX (26.0.0.131)
- Adobe Flash Player 26 NPAPI (26.0.0.131)
- Adobe Flash Player 26 PPAPI (26.0.0.131)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.35)
- FileZilla Client 3.36.0 (3.36.0)
- Google Chrome (75.0.3770.100)
- Google Update Helper (1.3.34.7)
- Java 8 Update 92 (8.0.920.14)
- Java Auto Updater (2.8.92.14)
- Microsoft .NET Framework 4.7.2 (4.7.03062)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)

Hotfixes

- Client LanguagePack Package
- Client Refresh LanguagePack Package
- CodecPack Basic Package
- Foundation Package
- IE Hyphenation Parent Package English
- IE Spelling Parent Package English
- IE Troubleshooters Package
- InternetExplorer Optional Package
- InternetExplorer Package TopLevel
- KB2533623
- KB2534111
- KB2639308
- KB2729094
- KB2731771
- KB2786081
- KB2834140
- KB2882822
- KB2888049
- KB2999226
- KB4019990
- KB976902
- LocalPack AU Package
- LocalPack CA Package
- LocalPack GB Package
- LocalPack US Package
- LocalPack ZA Package
- PlatformUpdate Win7 SRV08R2 Package TopLevel
- ProfessionalEdition
- UltimateEdition

- Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office IME (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)
- Microsoft Office O MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Professional 2010 (14.0.6029.1000)
- Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)
- Microsoft Office Proof (English) 2010 (14.0.6029.1000)

- Microsoft Office Proof (French) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)
- Microsoft Office Proof (German) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
- Microsoft Office Proofing (French) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (German) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Single Image 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)

- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
- Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
- Mozilla Firefox 68.0.1 (x86 en-US) (68.0.1)
- Notepad++ (32-bit x86) (7.5.1)
- Opera 12.15 (12.15.1748)
- Skype version 8.29 (8.29)
- Update for Microsoft .NET Framework 4.7.2 (KB4087364) (1)
- VLC media player (2.2.6)
- WinRAR 5.60 (32-bit) (5.60.0)
- srvpost (2.12.72)

Behavior activities

| MALICIOUS | SUSPICIOUS | INFO |
|--|--|--|
| Uses Task Scheduler to run other applications <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 2680) | Executable content was dropped or overwritten <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 2680) | Manual execution by user <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 2680) |
| Loads the Task Scheduler COM API <ul style="list-style-type: none">• schtasks.exe (PID: 2616) | Creates files in the user directory <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 2680)• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 3140) | |
| Application was dropped or rewritten from another process <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 2680)• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 3140) | Drops a file with too old compile date <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 2680) | |
| Actions looks like stealing of personal data <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 3140) | Reads the cookies of Google Chrome <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 3140) | |
| Steals credentials from Web Browsers <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 3140) | Application launched itself <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 2680) | |
| AGENTTESLA was detected <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 3140) | Reads the cookies of Mozilla Firefox <ul style="list-style-type: none">• 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe (PID: 3140) | |

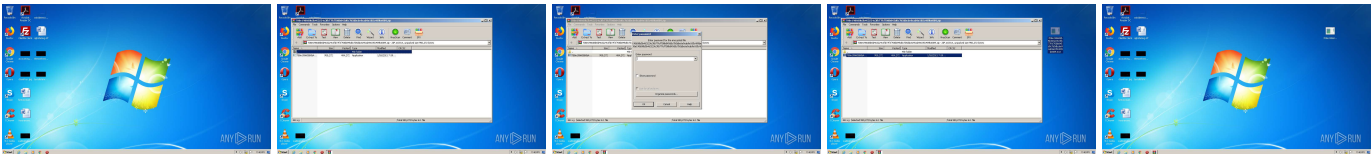
Malware configuration

No Malware configuration.

Static information

| TRiD | EXIF |
|--|---|
| <p>.zip ZIP compressed archive (100)</p> | <p>ZIP</p> <p>ZipFileName: 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe</p> <p>ZipUncompressedSize: 950272</p> <p>ZipCompressedSize: 484272</p> <p>ZipCRC: 0xbba1382e</p> <p>ZipModifyDate: 2021:01:26 19:39:05</p> <p>ZipCompression: Unknown (99)</p> <p>ZipBitFlag: 0x0003</p> <p>ZipRequiredVersion: 51</p> |

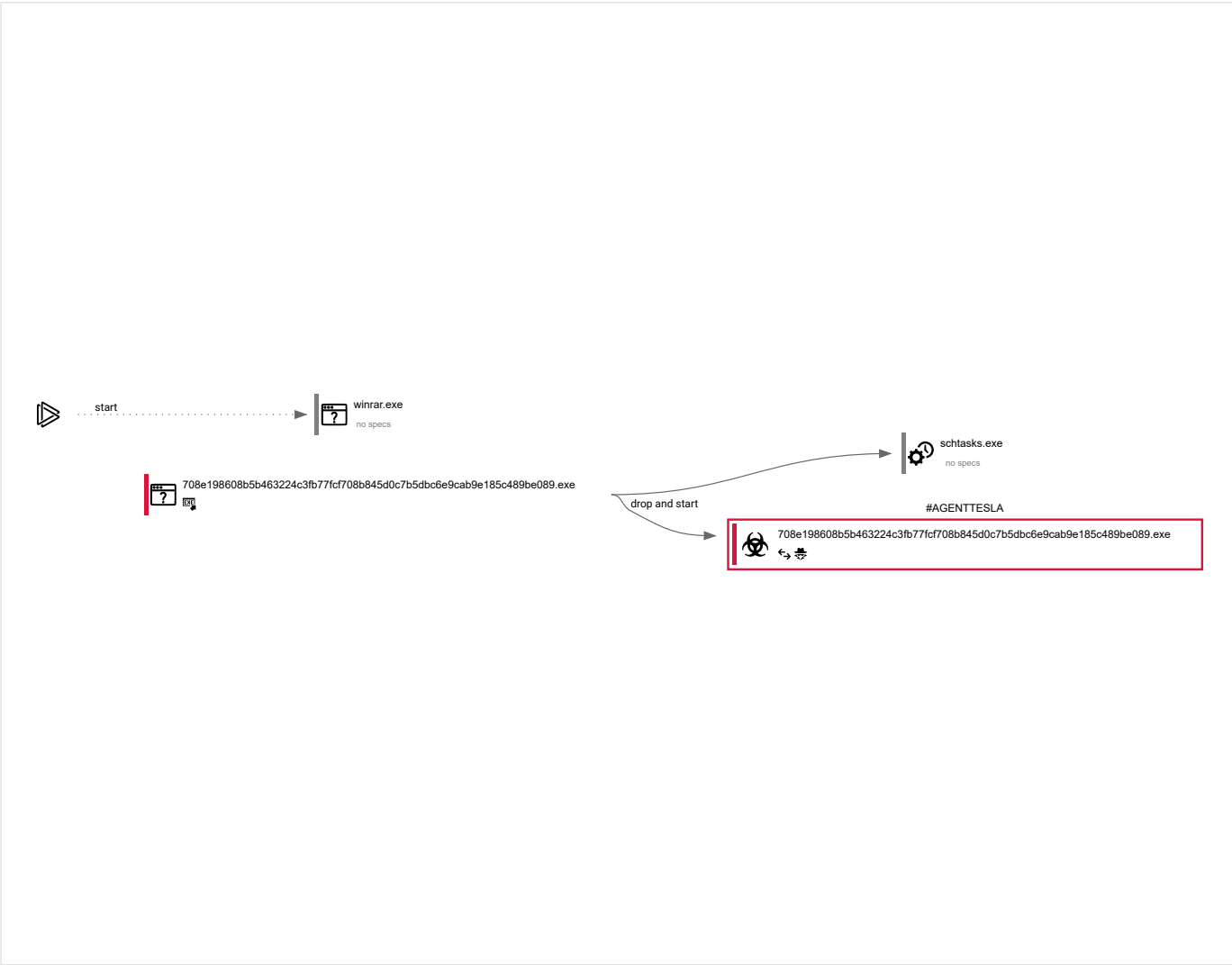
Video and screenshots



Processes

| | | | |
|-----------------|---------------------|---------------------|----------------------|
| Total processes | Monitored processes | Malicious processes | Suspicious processes |
| 40 | 4 | 2 | 0 |

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 |
|-------------|---|------------------------------------|------------|----------------|
| 2176 | "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\admin\AppData\Local\Temp\708e198608b5b463224c3fb77fc708b845d0c7b5dbc6e9cab9e185c489be089.zip" | C:\Program Files\WinRAR\WinRAR.exe | — | explorer.exe |
| Information | | | | |

| | | | |
|-----------------|---|---|--------------|
| User: admin | | Company: Alexander Roehal | |
| 2680 | "C:\Users\admin\Desktop\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe" | C:\Users\admin\Desktop\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe | explorer.exe |
| Version: 5.60.0 | | | |
| Information | | | |
| User: | admin | Integrity Level: | MEDIUM |
| Description: | App | Exit code: | 0 |
| Version: | 1.0.0.0 | | |

| | | | | |
|------------------|---|----------------------------------|---------------------------------------|--|
| 2616 | "C:\Windows\System32\schtasks.exe" /Create /TN "Updates\neHneiobyhcr.JJ" /XML "C:\Users\admin\AppData\Local\Temp\tmp5383.tmp" | C:\Windows\System32\schtasks.exe | — | 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe |
| Information | | | | |
| User: | admin | Company: | Microsoft Corporation | |
| Integrity Level: | MEDIUM | Description: | Manages scheduled tasks | |
| Exit code: | 0 | Version: | 6.1.7600.16385 (win7_rtm.090713-1255) | |

| | | | | |
|--------------|---|---|---|--|
| 3140 | "C:\Users\admin\Desktop\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe" | C:\Users\admin\Desktop\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe |   | 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe |
| Information | | | | |
| User: | admin | Integrity Level: | MEDIUM | |
| Description: | App | Version: | 1.0.0.0 | |

Registry activity

| | | | |
|--------------|-------------|--------------|---------------|
| Total events | Read events | Write events | Delete events |
| 552 | 539 | 0 | 0 |

Modification events

No data

Files activity

| | | | |
|------------------|------------------|------------|---------------|
| Executable files | Suspicious files | Text files | Unknown types |
| 1 | 0 | 1 | 0 |

Dropped files

| PID | Process | Filename | Type |
|------|--|---|------------|
| 2176 | WinRAR.exe | C:\Users\admin\AppData\Local\Temp\Rar\$DRb2176.34513\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe MD5: — SHA256: — | — |
| 3140 | 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe | C:\Users\admin\AppData\Roaming\dtcmbvue.dna\Chrome\Default\Cookies MD5: — SHA256: — | — |
| 3140 | 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe | C:\Users\admin\AppData\Roaming\dtcmbvue.dna\Firefox\Profiles\qldyz51w.default\cookies.sqlite MD5: — SHA256: — | — |
| 2680 | 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe | C:\Users\admin\AppData\Local\Temp\tmp5383.tmp MD5: 984EC3A9799C9300727FC04436E9F3A4 SHA256: 16D44F358DBF6AAD7FCACC3B68A0506FFD7395B7887D7847A77D55170BCF02B7 | xml |
| 2680 | 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe | C:\Users\admin\AppData\Roaming\neHneiobyhcr.JJ.exe MD5: 80B51E872031A2BEFEB9A0A13E6FC480 SHA256: 708E198608B5B463224C3FB77FCF708B845D0C7B5DBC6E9CAB9E185C489BE089 | executable |

Network activity

| | | | |
|------------------|---------------------|--------------|---------|
| HTTP(S) requests | TCP/UDP connections | DNS requests | Threats |
| 0 | 2 | 1 | 14 |

HTTP requests

No HTTP requests

Connections

| PID | Process | IP | Domain | ASN | CN | Reputation |
|------|--|--------------------|-------------------|-----|----|-------------------|
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | 208.91.199.225:587 | smtp.godforeu.com | PDR | US | <div>shared</div> |

DNS requests

| Domain | IP | Reputation |
|-------------------|----------------|----------------------|
| smtp.godforeu.com | 208.91.199.225 | <div>malicious</div> |
| | 208.91.198.143 | |
| | 208.91.199.223 | |
| | 208.91.199.224 | |

Threats

| PID | Process | Class | Message |
|------|--|--|--|
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>Generic Protocol Command Decode</div> | SURICATA Applayer Detect protocol only one direction |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>A Network Trojan was detected</div> | SPYWARE [PTsecurity] AgentTesla Exfiltration |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>Generic Protocol Command Decode</div> | SURICATA Applayer Detect protocol only one direction |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>A Network Trojan was detected</div> | SPYWARE [PTsecurity] AgentTesla Exfiltration |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>A Network Trojan was detected</div> | ET TROJAN AgentTesla Exfil Via SMTP |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>A Network Trojan was detected</div> | AV TROJAN Win.Keylogger.AgentTesla SMTP Activity |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>A Network Trojan was detected</div> | SPYWARE [PTsecurity] AgentTesla Exfiltration |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>A Network Trojan was detected</div> | ET TROJAN AgentTesla Exfil Via SMTP |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>A Network Trojan was detected</div> | AV TROJAN Win.Keylogger.AgentTesla SMTP Activity |
| 3140 | 708e198608b5b463224c3fb77f cf708b845d0c7b5dbc6e9cab9 e185c489be089.exe | <div>A Network Trojan was detected</div> | SPYWARE [PTsecurity] AgentTesla Exfiltration |

Debug output strings

No debug info