



PROFILE

AGENT TESLA MALWARE

ZEROFOX INTELLIGENCE

P-2022-12-15a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Malware

December 15, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 8:00 AM (EST) on December 15, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Agent Tesla Malware

Executive Summary

Agent Tesla is a malware typically used to steal sensitive information from infected computers. It is a remote access trojan (RAT) used by hackers to gain unauthorized access to a victim's computer and has been operating since 2014.¹ Once a computer is infected, Agent Tesla can record keystrokes, take screenshots, steal account credentials, and target other applications to steal sensitive data. Agent Tesla is typically distributed through malicious spam emails; good cyber hygiene practices may combat the risks posed to individuals and organizations.

Capabilities

Obfuscated Files or Information: Software Packing [T1027.002]

Agent Tesla samples are often packed or obfuscated to hinder analysis efforts.

System Owner/User Discovery [T1033]

With each check-in to the command and control (C2) server, Agent Tesla sends the victim's username, computer name, operating system (OS) version, and total physical memory (RAM).

User Execution: Malicious File [T1204.002]

Some Agent Tesla samples are configured to download and execute secondary payloads.

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]

Agent Tesla can persist on a victim's computer by copying itself into the startup folder or by adding itself to the registry run key
(\Software\Microsoft\Windows\CurrentVersion\Run).

¹

[hXXps://www.splunk\[.\]com/en_us/blog/security/inside-the-mind-of-a-rat-agent-tesla-detection-and-analysis.html](https://www.splunk.com/en_us/blog/security/inside-the-mind-of-a-rat-agent-tesla-detection-and-analysis.html)



Credentials from Password Stores: Credentials from Web Browsers [T1555.003]

Agent Tesla targets a large number of web browsers to obtain credentials and other sensitive data.

Targeted browsers:

- 360 Browser
- 7Star
- Amigo
- BlackHawk
- Brave
- CentBrowser
- Chedot
- Chrome
- Chromium
- Citrio
- Coccoc
- Comodo Dragon
- CoolNovo
- Coowon
- CyberFox
- Elements Browser
- Epic Privacy
- Firefox
- Flock
- IceCat
- IceDragon
- Iridium Browser
- K-Meleon
- Kometa
- Liebao Browser
- Opera
- Orbitum
- PaleMoon
- Postbox
- QIP Surf
- QQ Browser
- SRWare Iron
- SeaMonkey
- Sleipnir 6
- Sputnik
- Thunderbird
- Torch Browser

- UC Browser
- Uran
- Vivaldi
- WaterFox
- Yandex
- uCozMedia

Credentials from Password Stores: Password Managers [T1555.005]

In addition to credentials stored by web browsers, Agent Tesla also attempts to steal credentials from a variety of other applications such as OpenVPN, NordVPN, Microsoft Outlook, VNC, Mozilla Thunderbird, MySQL Workbench, and FileZilla.

Input Capture: Keylogging [T1056.001]

Agent Tesla can log a victim's keystrokes using functionality built into the Windows API.

Proxy: Multi-hop Proxy [T1090.003]

Some samples may attempt to download TOR to proxy HTTP requests.

Screen Capture [T1113]

Agent Tesla is capable of taking screenshots of a victim's desktop.

Exfiltration Over C2 Channel [T1041]

Exfiltration with Agent Tesla can be configured to happen over HTTP, FTP, and SMTP.

Recommendations

Agent Tesla is typically distributed through malicious spam emails. ZeroFox Intelligence highly recommends that email administrators block uncommon attachment file types such as (but not limited to) .chm, .js, .iso, .lnk, .vbs, and .vhd, which are not likely to be needed by the average office worker. Administrators should also perform anti-virus scans where possible on email attachments, removing any deemed malicious. Employees should also exercise caution when receiving emails from unknown senders with attachments.

ZeroFox Intelligence also recommends proactively utilizing the unique data sets available within ZeroFox's Threat Intelligence Feeds to correlate alerts in your environment with indicators of attack/compromise and prepare appropriate security team responses in order to get ahead of threat actor activity. More information about which feeds are offered on the [API Data Feeds](#) page is available in the ZeroFox platform.



Appendix 1: Indicators of Compromise (IOCs)

SHA256 Hashes

- 0640def3b6583af894d0f82789fff7400cda2ef359b3abeddf5f90a9df22416d
- 136234391a1f9fe15747d3d96035307657e18f46da60c847a1095de151db453a
- 274f50756eae9c356cd50c5d9101e4fbff8cad0cbb748500d1dac9bc845ad43d
- 4517cd01082e995cbe8baf5a4220a2f88e82657f00ab1f2b663e4c9148be8c74
- 5a6aalfdb77e7cd11c2c562bb812f0172880317d8bdde447f383976b0d187edc
- 662b0273e19dd3d9ad7d7579eba2c398b2a202195a5a8079ee525dcce3720278
- 683fb58ed87ad8bafec143c69fa5b09aa40cf02b3fb7c111277fc542281d3b3
- 916d57e0a893256adc18959aeead518bbcbba58ad8929e57751a943a96266bb
- 938b0b8074db906112a6567f4f0a22229ca344e338eb23586b2f560bff1f770f
- a4a93882eebffc57433742517438c5d56a6d67470a674558f4db52ff4306c9a
- c6de5b7bdb4200dec311343c0f98f417fde523580d4dd8537d24fd8c1e7940e7
- e430b2f55c0ac827593bec378510ba9d2aa486c72620deef9dbf7a5164b7a88d



Appendix 2: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.