Unfolding Agent Tesla: The Art of Credentials Harvesting. Dropper Analysis

By Osama Ellahi

Published: 2024-08-15 · Archived: 2026-04-05 14:20:07 UTC

Analysis of Agent Tesla, A Close Look at Password Theft Technique

— Part — 1 — Dropper Analysis

Executive Summary

Agent Tesla is a very detailed form of malware that typically infiltrates systems through deceptive emails. Once executed, it goes through multiple stages, using various droppers to disguise its presence. The malware's primary goal is to steal sensitive information, such as passwords, from web browsers, email, VPN, and FTP clients. It then secretly transmits this stolen data to the attacker's email through a compromised email server.

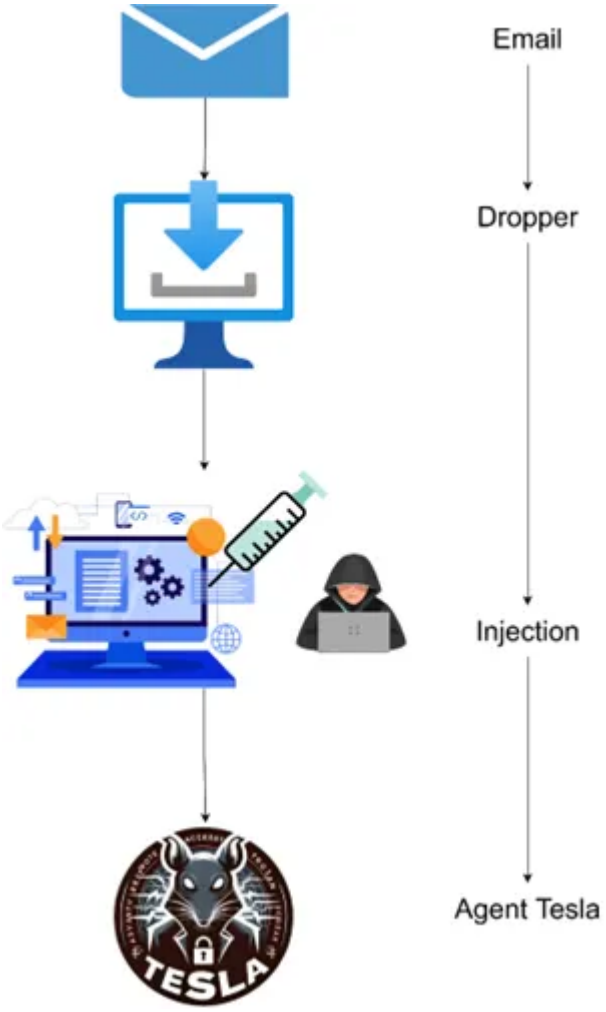
This highlights the importance of being cautious with email attachments to prevent falling victim to such malicious activities.

Malware Flow

Agent Tesla starts its malicious journey through a phishing email. The initial carrier is an {EXE} file, known as the dropper. Inside this executable file, there is a second stage {DLL} that gets loaded into its modules. Subsequently, a third stage {DLL} is loaded, followed by a fourth stage {DLL}. This fourth {DLL} is crucial, as it contains the actual Agent Tesla binary, which is also an {EXE} file.

Upon execution, this fourth-stage binary extracts the **Agent Tesla payload**, decrypts it, and injects the Agent Tesla binary into its own running process. In simpler terms, it activates the malicious code within itself. **The final stage binary is responsible for harvesting credentials from various sources, including browsers, email clients, VPN clients, and FTP clients**.

Once it successfully collects passwords from the system, the malware takes the next step by sending this stolen data to the attacker's email address. To achieve this, it utilizes a compromised email server, completing the malicious cycle initiated by the phishing email.



|

|

To read this full blog click on following link. We shifted this blog to personal blogging website.

https://breachnova.com/blog.php?id=29

|

Get Osama Ellahi's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

|

|

Parts

Part — 1 — Dropper Analysis
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-f1a988cfd137

Part — 2 — Browsers Stealing
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-2d565c68db0d

Part — 3- Discovery & Exfiltration
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-7a77f69435ee

Part — 4 — Stealing FileZilla
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-d30da9c36988

Part — 5 — Stealing The BAT! EMAIL CLIENT
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-c3fe4854775b

Part — 6 — Stealing Outlook Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-de3737f9d66e

Part — 7 — Stealing Trillian Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-afa2dd6e9de7

Part — 8 — Stealing MailBird Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-e5501af1c942

Part — 9 — Stealing WinSCP Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-55e7b2c64d60

Part — 10 — Stealing Core FTP LE Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-cdce40f6a747

Part — 11 — Stealing WinSCP Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-db9bb6698041

Part — 12 — Stealing FTP Navigator Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-59818a3686a3

Part — 13 — Stealing FTP Commander Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-7d01a41d554b

Part — 14 — Stealing FTP Getter Credentials
https://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-fe5ff29cc93c

---