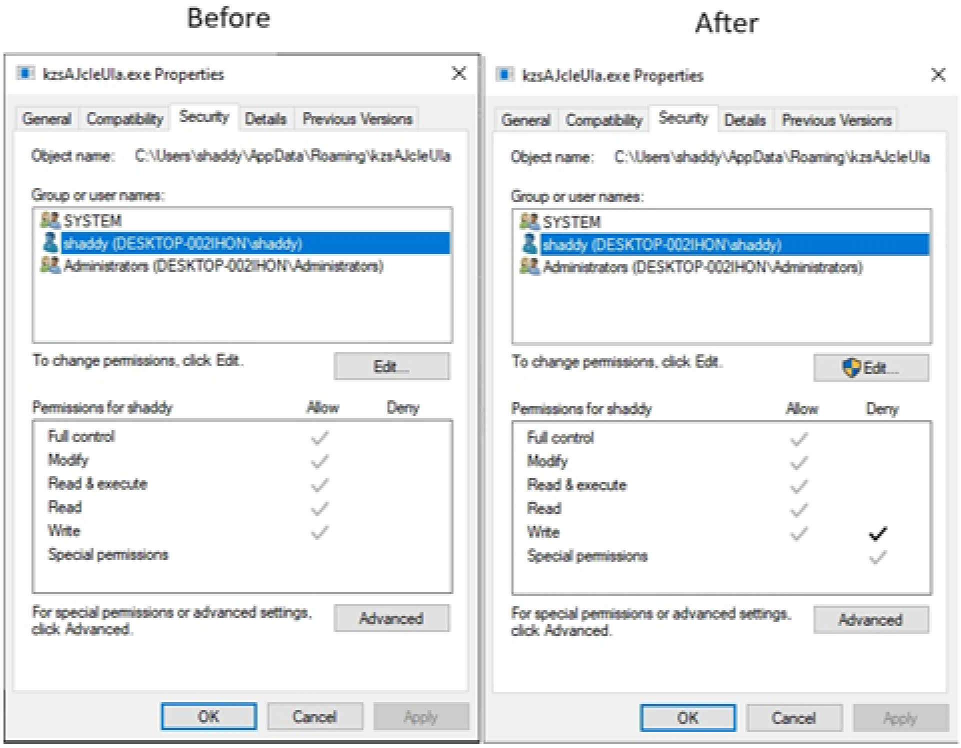
Unfolding Agent Tesla: The Art of Credentials Harvesting. Dropper Analysis

osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-f1a988cfd137

Osama Ellahi

February 16, 2024



Before

Object name: C:\Users\shaddy\AppData\Roaming\kzsAJcleUla

Group or user names:
SYSTEM
shaddy (DESKTOP-002IHON\shaddy)
Administrators (DESKTOP-002IHON\Administrators)

To change permissions, click Edit.

Permissions for shaddy	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

After

Object name: C:\Users\shaddy\AppData\Roaming\kzsAJcleUla

Group or user names:
SYSTEM
shaddy (DESKTOP-002IHON\shaddy)
Administrators (DESKTOP-002IHON\Administrators)

To change permissions, click Edit.

Permissions for shaddy	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	✓
Special permissions		✓

For special permissions or advanced settings, click Advanced.

Osama Ellahi

--

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.

Malware Composition

2877f7995c2735d9f3776a49b6b28f9af850446b023821833c94581ce2b689c4

First stage -exe

```
SHA-
2562877f7995c2735d9f3776a49b6b28f9af850446b023821833c94581ce2b689c4MD5431c41bf81aabdb9
```

Ben — dll {Second Stage}

```
SHA-
256bc419893a2948f85aa53af290eca67dc626ab1467b72a45419385d0fe709fd58MD5febba18c6714fcec
```

ReactionDiffusion - dll {Third Stage}

```
SHA-
256d01f3dea3851602ba5a0586c60430d286adf6fcc7e17aab080601a66630606e5MD5579197d4f760148a
```

Tyrone — dll {Fouth Stage}

```
SHA-
2568b76c98384c6c3adc45bccab7569d9c9683c322c20934b03cda24c84b76fb70dMD588d10653202e2cfc
```

Agent Tesla — exe {Final Stage}

```
SHA-
256bc419893a2948f85aa53af290eca67dc626ab1467b72a45419385d0fe709fd58MD57911215edc491695
```

Loader

Agent tesla in this variant comes in a very famous loader which is written in c#. This loader has been seen with so much malware like formbook, remcos and njrat etc. It have the malicious code inside the InitializeComponent() and it is a form application.

It starts with initializing a string with obfuscated binary content.

It de-obfuscates the content by replacing **"|" with "00".** Then it loads the assembly by the name **Ben i**n modules. Ben is same obfuscated binary which it has in string JFDJ after de obfuscation, it loads in its module for further processing.

After that it loads a second DLL **ReactionDiffusion** in modules extracting from resources.

And then the third DLL is loaded in modules with name of "**Tyrone**". It invoke "**INeFsQJBtN**()" method from "**xmUvG0atRoqU5DT6Sy.mCFjRgCR32aHEMMYFO**"

It checks if the file exits "**C:\Users\%username%\AppData\Roaming\kzsAJcleUla.exe**" if it does not exist **it copies itself there**. It is doing this for persistence purposes.

It changes the permission of the copied file so that no one could be able to change it or delete it.

As we can see clear difference in the following picture, the left picture shows before executing this function and right picture was recorded after the execution. After this the user cannot delete or write anything in the file.

Then it loads the encoded string from modules of **tyrone** binary and decode it. The decoded string looks like an xml, let's explore it further.

Persistence

This variant of agent tesla performs persistence by using task scheduler method, it runs a PowerShell command which takes a temporary **xml file** that contains configuration of task.

It performs the following steps.

- loads string from modules.
- creates a new process.
- Assign those strings to this new process as an argument.
- Make window style hidden of process.
- Start the process.

Defense Evasion

It adds an exclusion for a specific file (in this case, **kzsAJcIeUIa.exe** located in a user's **AppData\Roaming** directory) to Windows Defender's scanning process. This command tells Windows Defender not to scan or consider this file as a potential threat.

Powershell.exe

@"Add-MpPreference -ExclusionPath
""C:\Users\%username%\AppData\Roaming\kzsAJcIeUIa.exe"""

After that **it alter information of xml** and save it in **tmp folder**
@"C:\Users\%username%\AppData\Local\Temp\tmp95EB.tmp"

This xml contains the configuration about the persistent task. It is triggered **on every Log on of user**, when user starts the system, it will execute an application which is saved in roaming.

The next command utilizes the Windows Task Scheduler tool, schtasks.exe, to create a scheduled task named "**kzsAJcIeUIa**" within the "Updates" folder. The task's properties and settings are defined in an XML file located at "**C:\Users%username%\AppData\Local\Temp\tmp95EB.tmp**," with %username% serving as a placeholder for the currently logged-in user's username.

"schtasks.exe"

@"/Create /TN ""Updates\kzsAJcIeUIa"" /XML
""C:\Users\%username%\AppData\Local\Temp\tmp95EB.tmp"""

It sets the process windows style hidden to run this command in background, so that user would not see any command pop up.

Injection

It creates read write and executable memory and then writes whole new extracted binary from resources. It injects the final stage malware in same process, this is process hollowing because a whole binary is injected into same process.

Parts

Part — 1 — Dropper Analysishttps://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 Credentialshttps://osamaellahi.medium.com/unfolding-agent-tesla-the-art-of-credentials-harvesting-55e7b2c64d60

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

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

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

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

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