### Agent-Tesla-Open-Directory

Agent Tesla is a malware family written in .NET for Microsoft Windows systems and has much in common with spyware in its capabilities. It has many spyware like capabilities such as :

* Stealing credentials,
* Keylogging,
* Collecting screenshots,
* Capturing web camera images, and
* Gathering clipboard data,

but it is often seen in more standard malware campaigns and uses common malware techniques for obfuscation, unpacking, and data collection. Recently, Agent Tesla has been distributed in the wild through phishing emails and malicious Word documents containing macros to drop and execute the malware.

Recent research has identified Agent Tesla being delivered within email attachments by the names of “COVID 19 NEW ORDER FACE MASKS.doc.rtf”, “COVID-19 Supplier Notice.zip” or something along those lines. When a user clicks to download the file, the malware can execute within the impacted device without additional user interaction. If an attacker is able to fully deliver this RAT onto your device, they will have achieved full computer and network access.

The following yara rule is created for the detection of this malware. Let us look at it in detail.

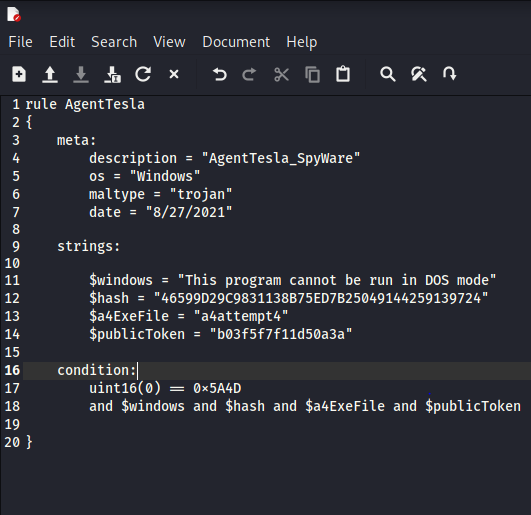


Fig. 1.1 Yara rule

**Metadata**

Metadata doesn’t affect what the YARA rule will search for, instead, it provides useful information about the rule itself.

* **Description** – A brief overview of the rule’s purpose and malware it aims to detect.
* **Os** – This tells the OS targeted by this malware
* **MalType –** Shows what type of malware it is
* **Date -** Date rule was created.

### Strings

It is common to find unique and interesting strings within a malware sample, these are ideal for building out a YARA rule. To define a string within a rule, the string itself needs to be declared as a variable.

* $windows = "This program cannot be run in DOS mode"
  + This string shows this malware cannot run in DOS mode. This is for windows.
* $hash = "46599D29C9831138B75ED7B25049144259139724"
  + This is the hash value which is common to this malware family.
* $a4ExeFile = "a4attempt4"
  + This is for malware executable
* $publicToken = "b03f5f7f11d50a3a"
  + This is the public token common for this malware family.
  + QSystem.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a

**Conditions**

The strings section defines the search criteria that will be used for a YARA rule, the conditions section defines the criteria for the rule to trigger a successful match. There are multiple conditions that can be used which I will outline.

* **uint16(0) == 0x5A4D** – Checking the header of a file is a great condition to include in your YARA rules. This condition is stipulating that the file must be a Windows executable, this is because the hex values 4D 5A are always located at the start of an executable file header. This is reversed in YARA due to endianness.
* And $windows and $hash and $a4ExeFile and $publicToken – This includes all the string mentioned in above section with and condition.

**Output**

Now the Yara rule created above should identify the Agent tesla malware files as malicious. See the screenshot below.

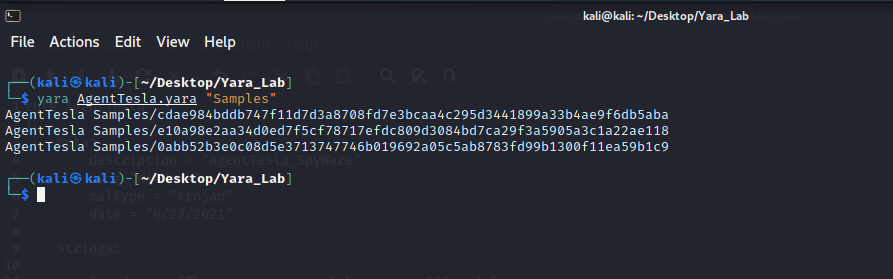


Fig. 1.2 Yara output for Agent Tesla malware

The same Yara rule is not detecting the other malwares. See the screenshot below:

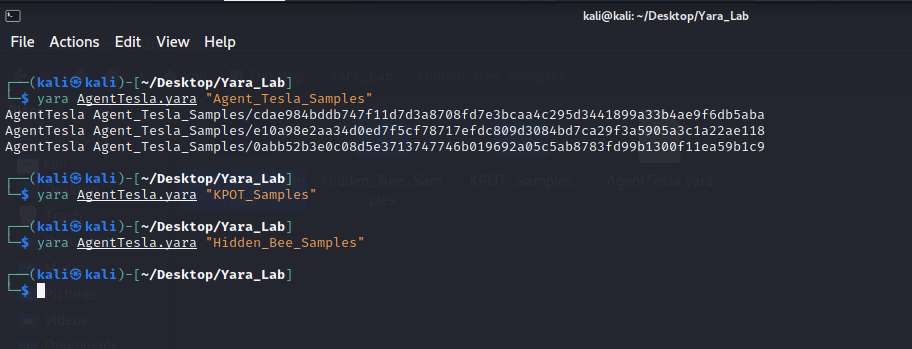


Fig. 1.3 Yara Output for other malwares

References

<https://www.varonis.com/blog/yara-rules/>

<https://www.riskiq.com/blog/external-threat-management/agent-tesla-trend-analysis/#:~:text=Agent%20Tesla%20is%20an%20extremely,information%20from%20its%20operators'%20targets>.

<https://howtofix.guide/trojanwin32-agentteslaml/>

<https://en.wikipedia.org/wiki/Endianness>

<https://inquest.net/2018/05/22/field-notes-agent-tesla-open-directory>