**Name: Dipendra Kushwah Date: 27-08-2021**

**Enrollment number: MT20ACS507**

**Subject: CS 5202-Threat intelligence**

**Lab 2: Yara rule and static analysis of malware**

**Malware Sample used: 9d6611c2779316f1ef4b4a6edcfdfb5e770fe32b31ec2200df268c3bd236ed75**

**Brief overview:**

AZORult is a credential and payment card information stealer. AZORult is a robust information stealer & downloader that Proofpoint researchers originally identified in 2016 as part of a secondary infection via the Chthonic banking Trojan. We have since observed many instances of AZORult dropped via exploit kits and in fairly regular email campaigns as both a primary and secondary payload. Recently, AZORult authors released a substantially updated version, improving both on its stealer and downloader functionality.

AZORult Version 2 Stealer, written in Borland Delphi (now getting advanced with c and c++) collects information’s, sends a report to the C2 server, then self-deletes. AZORult steals cookies, saved passwords, and saved credit card information from browsers. It also steals XMPP and Bitcoin wallet information Additionally, the malware is able to grab files from Desktop with specified extensions. It supports .bit domain communication.

AZORult v3 always appends the XOR key used to encrypt the following message sent to its C&C at the beginning of the message. Thus, the initial communication always starts with three NUL bytes followed by an XOR encrypted ID hash.

It encodes streams and separates the report information as follows:

* Browsers\AutoComplete\<browser>\_CC.txt
* Browsers\AutoComplete\<browser>\_\_.default
* Browsers\Cookies\<browser>\_\_.default.txt
* IP.txt
* Passwords.txt
* CookieList.txt
* SYSInfo.txt

**AZORult obtains the user and computer information via** usual GetUserName and GetComputerName APIs.

Moreover, AZOrult aslo appear to collect the following cryptocurrency files:

* wallet.dat
* \wallet.dat
* electrum.dat
* \electrum.dat
* .wallet
* \.wallet
* %APPDATA%\MultiBitHD
* mbhd.wallet.aes
* \MultiBitHD\
* \mbhd.wallet.aes
* \mbhd.checkpoints
* mbhd.checkpoints
* \mbhd.spvchain
* mbhd.spvchain
* \mbhd.yaml
* mbhd.yaml
* wallet\_path
* Software\monero-project\monero-core
* \Monero\

Desktop file grabber of files with .txt & .dat extensions.

**Also works as** malware campaigns where both a stealer and ransomware are present. (2018 AZORult downloads Hermes 2.1 ransomware  after it exfiltrates the victim’s data and credentials.)

**Disclosed Log text for version 3.2 Azorult:**

*Change log text:*

* UPD v3.2
* [+] Added stealing of history from browsers (except IE and Edge)
* [+] Added support for cryptocurrency wallets: Exodus, Jaxx, Mist, Ethereum, Electrum, Electrum-LTC
* [+] Improved loader. Now supports unlimited links. In the admin panel, you can specify the rules for how the loader works. For example: if there are cookies or saved passwords from mysite.com, then download and run the file link[.]com/soft.exe. Also there is a rule "If there is data from cryptocurrency wallets" or "for all"
* [+] Stealer can now use system proxies. If a proxy is installed on the system, but there is no connection through it, the stealer will try to connect directly (just in case)
* [+] Reduced the load in the admin panel.
* [+] Added to the admin panel a button for removing "dummies", i.e. reports without useful information
* [+] Added to the admin panel guest statistics
* [+] Added to the admin panel a geobase

\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Static (only strings) Analysis of above sample:**

**Filetype**

window64 executable

**Strings found in the binary may indicate undesirable behavior:**

1. May have dropper capabilities: %temp%
2. Contains domain names: http://ravor.ac.ug
3. This program cannot be run in DOS mode

In order to achieve back compatible to DOS program, the PE file format contains the DOS stub, which can be run in DOS real mode. In most case, the PE executable has the DOS stub that simply displays a string "This program cannot be run in DOS mode".

[Reference: https://sites.google.com/site/bletchleypark2/network-attack-and-defense/ctf/-mma-ctf-2015-reverse-notrunindos]

**Dll requiring internet connection**

wininit.dll

Cryptographic algorithms detected in the binary:

Uses constants related to CRC32

Uses constants related to SHA1

**The PE contains functions mostly used by malware.**

**Functions related to the privilege level:**

1. OpenProcessToken

**Enumerates local disk drives:**

1. GetVolumeInformationW

**Can take screenshots:**

1. GetDC
2. CreateCompatibleDC
3. BitBlt

**VirusTotal score**: 58/70

**Basic Info**

Referenced File F:\orders\cpp\azorult\_new\Release\azorult\_new.pdb

TimeDateStamp 2019-Mar-02 09:08:41

**Total imports**: 90

**Description for the Strings used to create Yara rule: (Yara rule file attached separately)**

**$mz = {4D 5A}**

* **Specify the file type as executable**

**$string2 = "SYSInfo.txt"**

* **Selected assuming malware might be trying to write System info**

**$string3 = "CookieList.txt"**

* **Selected assuming malware might be trying to write System info**

**$string4 = "PasswordsList.txt"**

* **Selected assuming malware might be trying to write password list**

**$string5 =** [**http://ravor.ac.ug**](http://ravor.ac.ug)

* **Redirection to Unknown domain**

**$string6 = "%s\\Ethereum\\keystore"**

* **Trying to get in Crypto wallet key**

**$string7 = "%S\\r\\nUSER:"**

* **Reading User name**

**$string8 = "%s\\r\\nPASS:"**

* **Reading Password**

**$string9 = "wininet.dll"**

* **Dll used for internet connection. Malware must require internet connection**

**Pending:**

**Have to add Mutex string**   
A mutex is a locking mechanism used to synchronize access to a resource. Only one task (can be a thread or process based on OS abstraction) can acquire the mutex. It means there is ownership associated with a mutex, and only the owner can release the lock (mutex).

**Constants string values for**

Azorult functions that grabs .txt and .dat files from Desktop

And Portion of code from Azorult self-delete function

**Reference:**

* https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside
* [**https://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html**](https://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html)
* CVE-2018-4878 (Flash Player up to 28.0.0.137) and Exploit Kits [**https://malware.dontneedcoffee.com/2018/03/CVE-2018-4878.html#gf-sundown**](https://malware.dontneedcoffee.com/2018/03/CVE-2018-4878.html#gf-sundown)
* Virus Total
* https://www.vmray.com/analyses/5ff8a87fd762/report/behavior\_grouped.html
* <https://www.vmray.com/cyber-security-blog/azorult-delivered-by-guloader-malware-analysis-spotlight/>
* <https://malpedia.caad.fkie.fraunhofer.de/details/win.azorult>
* <https://blog.minerva-labs.com/analyzing-an-azorult-attack-evasion-in-a-cloak-of-multiple-layers>