CS 5202-Threat intelligence

Lab# 1

AZORult Malware Analysis

Study of Yara rules

Aswin Vijay V L

MT20ACS500

Table of Contents

[**Introduction** 3](#_Toc81238736)

[**Attack Vectors** 3](#_Toc81238737)

[**Origination of attacks** 4](#_Toc81238738)

[**Recent AZORult usage – Fake Coronavirus map** 5](#_Toc81238739)

[**Functionality overview** 6](#_Toc81238740)

[**Infection and compromise** 7](#_Toc81238741)

[**Persistence** 8](#_Toc81238742)

[**Yara Rules** 9](#_Toc81238743)

[**Mitigation Practices** 10](#_Toc81238744)

[**References** 11](#_Toc81238745)

### **Introduction**

AZORult

• Malware – Information stealer and cryptocurrency theft

• Initially detected in 2016 when dropped by the Chthonic banking trojan

• Latest version: 3.2; Used to target Windows

• AKA PuffStealer, Ruzalto

• Easy to operate (user friendly)

• Very common; Sold on Russian hacker forums for ~$100

• Can both be dropped or serve as a dropper (first or second stage)

• Constantly changing/evolving infection vectors and attack stages and capabilities

• Especially relevant during the Coronavirus pandemic

• Used in Coronavirus-themed attacks

### **Attack Vectors**

How is AZORult delivered?

• Common:

• Exploit Kits (especially Fallout Exploit Kit)

• Other malware that acts as a dropper

• Ramnit

• Emotet

• Phishing

• Malspam

• Infected websites

• Malvertisements

• Fake installers

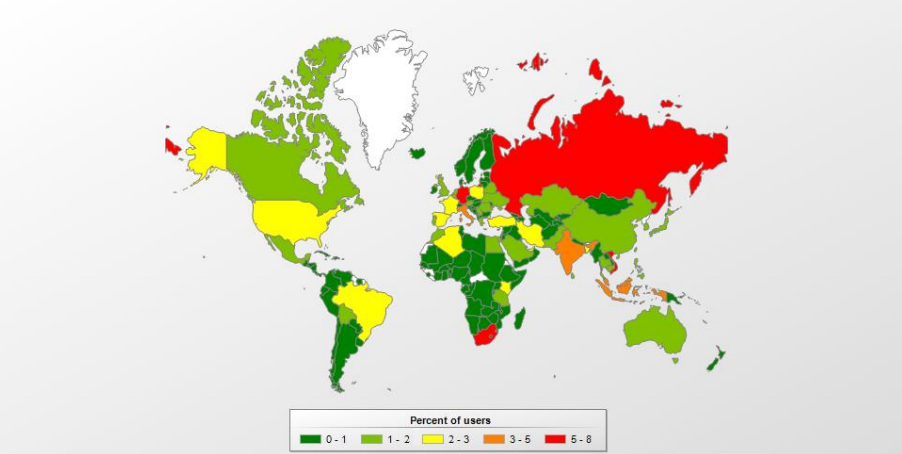
• On occasion:

• .iso file

• Remote Desktop Protocol (RDP) exploitation

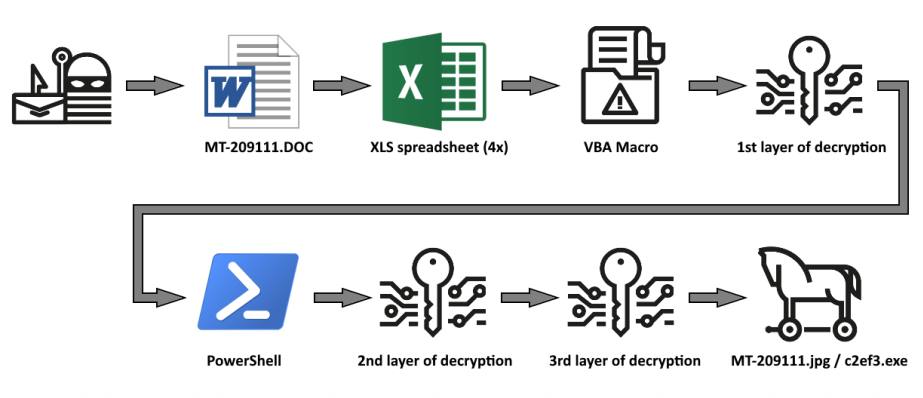
### **Origination of attacks**

Geographical distribution of AZORult attacks: December 2017 through December 2018



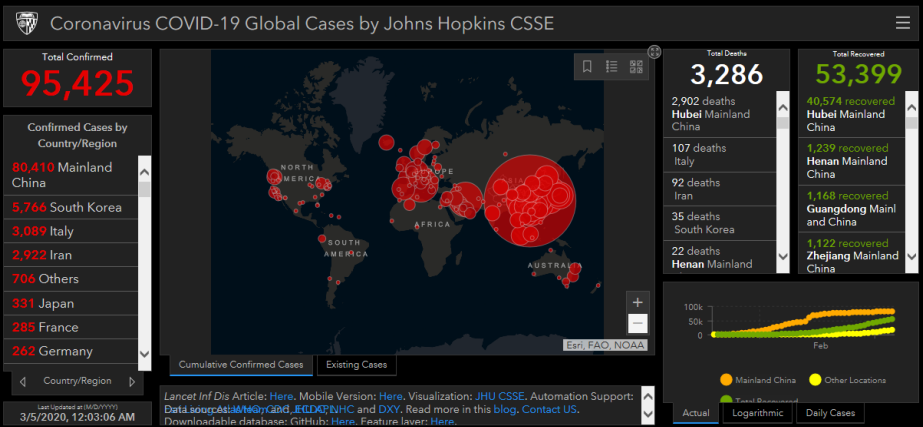
Recent AZORult technique – triple encryption

• Observed in a February 2020 phishing campaign:

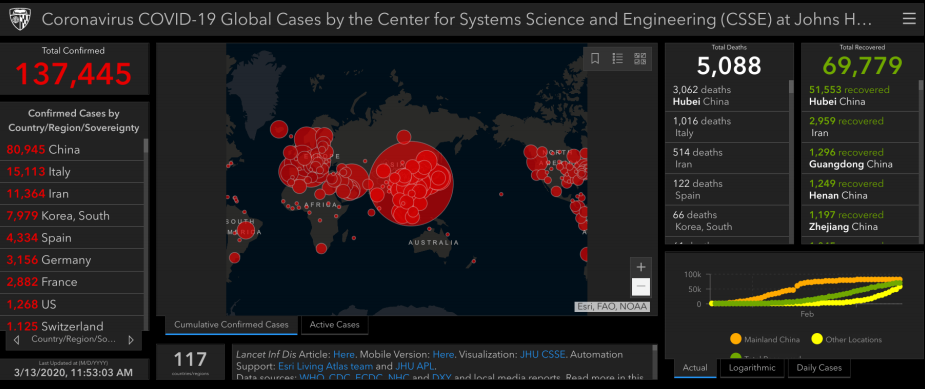


### **Recent AZORult usage – Fake Coronavirus map**

Fake Coronavirus tracking map drops AZORult on victim systems:



Legitimate Johns Hopkins Coronavirus Map :



### **Functionality overview**

AZORult possesses the following capabilities:

• Steals:

• System login credentials

• System reconnaissance info (GUID, system architecture and language, username and computer name,

operating system version, system IP address

• Cryptocurrency wallets

• Monero, uCoin, and bitcoin cryptocurrencies

• Electrum, Electrum-LTC, Ethereum, Exodus, Jaxx and Mist wallets

• Steam and Telegram credentials; Skype chat history and credentials

• Payment card numbers

• Cookies and other sensitive browser-based data (especially autofill)

• Data Exfiltration/Communication

• Pushes to a command-and-control server.

• Screenshots

• Executes files via remote backdoor commands

### **Infection and compromise**

MITRE ATT&CK Techniques used by AZORult:

* Access Token Manipulation

AZORult can call WTSQueryUserToken and CreateProcessAsUser to start a new process with local system privileges.

* Credentials from Web Browsers

AZORult can steal credentials from the victim's browser.

* Credentials in Files

AZORult can steal credentials in files belonging to common software such as Skype, Telegram, and Steam.

* Deobfuscate/Decode Files or Information

AZORult uses an XOR key to decrypt content and uses Base64 to decode the C2 address.

* File and Directory Discovery

AZORult can recursively search for files in folders and collects files from the desktop with certain extensions.

* File Deletion

AZORult can delete files from victim machines.

* Process Discovery

AZORult can collect a list of running processes by calling CreateToolhelp32Snapshot.

* Process Hollowing

AZORult can decrypt the payload into memory, create a new suspended process of itself, then inject a decrypted payload to the new process and resume new process execution.

* Query Registry

AZORult can check for installed software on the system under the Registry key Software\Microsoft\Windows\CurrentVersion\Uninstall

* Remote File Copy

AZORult can download and execute additional files. Azorult has also downloaded a ransomware payload called Hermes.

* Screen Capture

AZORult can capture screenshots of the victim’s machines.

* Standard Cryptographic Protocol

AZORult can encrypt C2 traffic using XOR.

* System Information Discovery

AZORult can collect the machine information, system architecture, the OS version, computer name, Windows product name, the number of CPU cores, video card information, and the system language.

* System Network Configuration Discovery

AZORult can collect host IP information from the victim’s machine.

• Example attack:

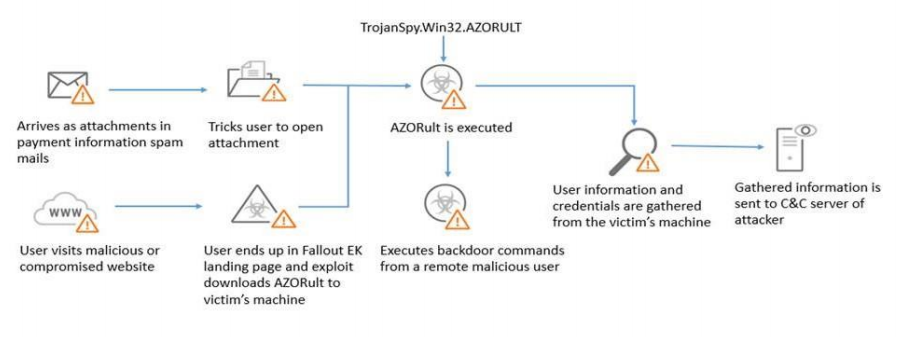
• Infection vector

• Execution

• Persistence

• Reconnaissance

• Exfiltration



### **Persistence**

AZORult can establish persistence:

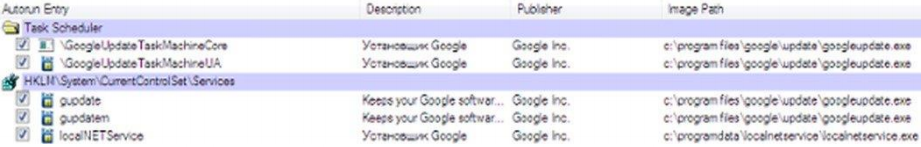
• Install standard backdoors

• Creates hidden admin account to set registry key to establish Remote

Desktop Protocol (RDP) connection

• Camouflages as legitimate application (registry and scheduled tasks)

• See example of fake Google update binary below which contained AZORult Trojan



### **Yara Rules**

rule azorult

{

meta:

description = "2019-03-AZORult"

author = "MT20ACS500"

category = "Lab Practical"

strings:

$a1 = "!This program cannot be run in DOS mode." /\* exe header \*/

$c = "http://" wide /\* check for any http urls\*/

$d = "NetUserAdd" /\* func to add a new user\*/

$e = "NetLocalGroupAddMembers" /\* func to add a new usergroup\*/

$f = "CredEnumerate" /\* enumerates the user creds\*/

$h = "CryptUnprotectData" /\* decrypt the creds\*/

$i = "LookupAccountSid" /\* security identifier lookup\*/

$j = "Reg" wide

condition:

all of ($a\*) and

$c or

($d and $f) or

($e and $f) or

($f and $h) or

($j and $i)

}

References for Yara rules

<https://malpedia.caad.fkie.fraunhofer.de/yara/win.azorult>

https://github.com/YaraRules/rules/blob/master/malware/MALW\_AZORULT.yar

<https://malware.lu/articles/2018/05/04/azorult-stealer.html>

<https://yoroi.company/research/gootkit-unveiling-the-hidden-link-with-azorult/>

<https://neonprimetime.blogspot.com/2019/02/malware-yara-rules.html>

<https://tccontre.blogspot.com/2019/01/interesting-azorult-mutex-name-that.html>

### **Mitigation Practices**

* Provide social engineering and phishing training to employees.
* Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported
* Ensure emails originating from outside the organization are automatically marked before received.
* Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.
* Implement Intrusion Detection System (IDS); Keep signatures and rules updated.
* Implement spam filters at the email gateways; Keep signatures and rules updated.
* Block suspicious IP addresses at the firewall; Keep firewall rules are updated.
* Implement whitelisting technology to ensure that only authorized software is allowed to execute.
* Implement access control based on the principal of least privilege.
* Implement and maintain anti-malware solution.
* Conduct system hardening to ensure proper configurations.

### **References**

• Analyzing an AZORult Attack – Evasion in a Cloak of Multiple Layers

<https://blog.minerva-labs.com/analyzing-an-azorult-attack-evasion-in-a-cloak-of-multiple-layers>

• Let's Learn: Reversing Credential and Payment Card Information Stealer 'AZORult V2'

<https://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html>

• Kaspersky Threats: TROJAN-PSW.WIN32.AZORULT

<https://threats.kaspersky.com/en/threat/Trojan-PSW.Win32.Azorult/campaign>

• AZORult Malware - HHS cybersecurity Program

[https://securityintelligence.com/news/azorult-trojan-uses-fake-protonvpn-installer-to-disguise-attacks/](https://www.hhs.gov/sites/default/files/azorult-malware.pdf)

• AZORULT Malware Information

<https://success.trendmicro.com/solution/000146108-azorult-malware-information-kAJ4P000000kEK2WAM>

• New version of AZORult stealer improves loading features, spreads alongside ransomware in new campaign

<https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside>