A Report on AZORult malware Yara rule and static analysis

CS 5202-Threat intelligence

Submitted by:
Name: Dipendra Kushwah
Enrollment number: MT20ACS507

Under guidance of:
Dr. Ashu Sharma
Faculty – NIIT University

Table of Contents

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.[2]

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 – What is it?

• 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

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

AZORult obtains the user and computer information via usual GetUserName and GetComputerName APIs.
Moreover, AZOrult also 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.)

Example attack:

• Infection vector
• Execution
•Persistence
•Reconnaissance
• Exfiltration

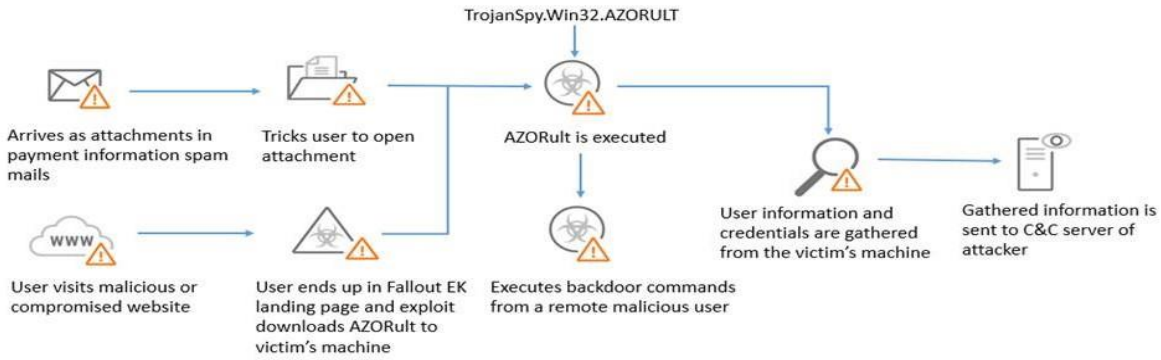


Image source: Trend Micro

Sample Spam - Shipping Inquiry Spam

From : ctnprincipal@inscape.co.za Date Time : 9/4/2019 10:05:07 PM
To : [redacted]
Cc :
Bcc :
Subject : Re: As Agreed
Attachments : attachedFile.rtf Attachment_747547567546754675090978236327345634 34.img

[EXTERNAL EMAIL] Verify sender before clicking on links or attachments

Good day,

Kindly find the below documents as you requested, Please Sign on the last 3 pages where your initials and Banking informations are then we can proceed with payment.

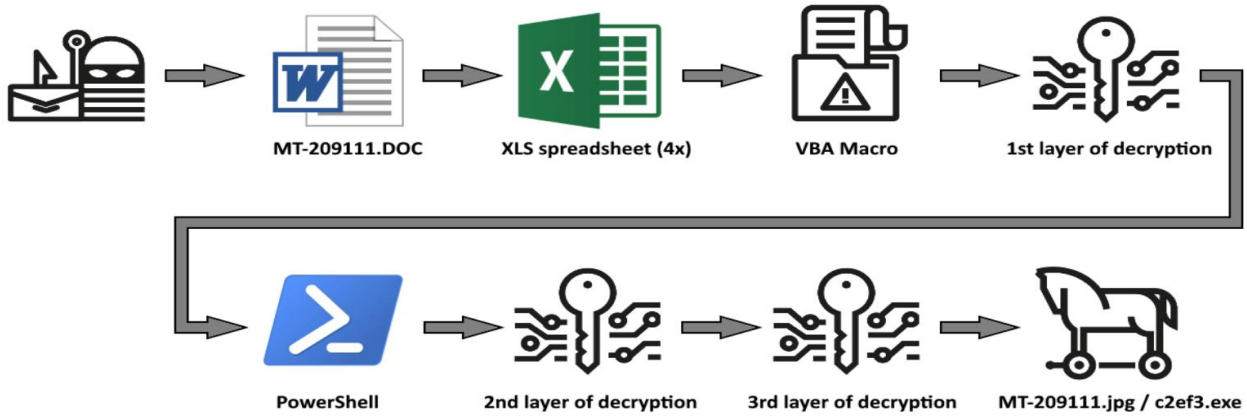
Your soonest response will be highly appreciated.

Best Regards
Njisuh Zebedee
Assistant Manager
1 Forssman Close, Barbeque Downs 16185
Fax: 0822748278

Image source: Trend Micro

Recent AZORult technique – triple encryption

Observed in a February 2020 phishing campaign:



Data and image source: ThreatPost

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)

Updated 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

****

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

Static (only strings) Analysis of above sample:

Filetype
window64 executable

Strings found in the binary that 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:
[2] GetVolumeInformationW
Can take screenshots:
[3] GetDC
[4] CreateCompatibleDC
[5] 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
- Redirection to Unknown domain

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

- Trying to get in Crypto wallet key

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

- Querying User name

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

- Querying Password

$string9 = "wininet.dll"

- Dll used for internet connection. Malware must requires internet connection

```
rule Malware : Azorult
    {
        meta:
            author = "Dipendra Kushwah"
            date = "2021-08-27"
            description = "Match first two bytes for file indentification and strings, Azorult"
            reference = "https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside"
            reference = "https://otx.alienvault.com/indicator/file/b72ba2dd844b6e99088093d22a5110ca4bdbd99922d17ef58403b6e389189c8e/"

        strings:
            $mz = {4D 5A}
            $string2 = "SYSInfo.txt"
            $string3 = "CookieList.txt"
            $string4 = "PasswordsList.txt"
            $string5 = "http://ravor.ac.ug"
            $string6 = "%s\\Ethereum\\keystore"
            $string7 = "%S\\r\\nUSER:"
            $string8 = "%s\\r\\nPASS:"
            $string9 = "wininet.dll"
            $string1 = "ST234LMUV56CklAopq78Brstuvwxyz01NOPQRmGHIJKWXYZabcdefgDEFhijn9+/" wide ascii // Azorult custom base64-like alphabet //analyszed for other samples
            $constant1 = {85 C0 74 40 85 D2 74 31 53 56 57 89 C6 89 D7 8B 4F FC 57} // Azorult grabs .txt and .dat files from Desktop //analyszed for other samples
            $constant2 = {68 ?? ?? ?? ?? FF 75 FC 68 ?? ?? ?? ?? 8D 45 F8 BA 03 00} // Portion of code from Azorult self-delete function //analyszed for other samples
        condition:
            $mz at 0 or $string2 or ($string3 and $string4 and $string9) or $string1 or $string5 or $string6 or $string7 or $string8  or ( $constant1 and $constant2 )

    }
```

Other String parameter that can be specified for a given malware

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:

1. https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside
2. https://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html
3. 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
4. https://www.virustotal.com/gui/home/upload
5. https://www.vmray.com/analyses/5ff8a87fd762/report/behavior_grouped.html
6. https://www.vmray.com/cyber-security-blog/azorult-delivered-by-guloader-malware-analysis-spotlight/
7. https://malpedia.caad.fkie.fraunhofer.de/details/win.azorult
8. https://blog.minerva-labs.com/analyzing-an-azorult-attack-evasion-in-a-cloak-of-multiple-layers