AZORult Malware

OVERALL CLASSIFICATION IS
TLP:WHITE

04/16/2020
Agenda

• Introduction
• Attack vectors
• Functionality overview
• Mapping against the MITRE ATT&CK Framework
• Infection and Compromise
• Origination of Attacks
• Fake Coronavirus map
• Triple Encryption
• Persistence
• Intrusion Detection Rules/Signatures
• Mitigation practices
• Indicators of Compromise
• References
• Questions

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
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

- Especially relevant during the Coronavirus pandemic
  - Used in Coronavirus-themed attacks
AZORult – 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
AZORult – 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
Mapping AZORult against the MITRE ATT&CK Framework

MITRE ATT&CK Techniques used by AZORult:

<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>T1134</td>
<td>Access Token Manipulation</td>
<td>AZORult can call WTSQueryUserToken and CreateProcessAsUser to start a new process with local system privileges.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1503</td>
<td>Credentials from Web Browsers</td>
<td>AZORult can steal credentials from the victim’s browser.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1081</td>
<td>Credentials in Files</td>
<td>AZORult can steal credentials in files belonging to common software such as Skype, Telegram, and Steam.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1140</td>
<td>Deobfuscate/Decode Files or Information</td>
<td>AZORult uses an XOR key to decrypt content and uses Base64 to decode the C2 address.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1083</td>
<td>File and Directory Discovery</td>
<td>AZORult can recursively search for files in folders and collects files from the desktop with certain extensions.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1107</td>
<td>File Deletion</td>
<td>AZORult can delete files from victim machines.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1057</td>
<td>Process Discovery</td>
<td>AZORult can collect a list of running processes by calling CreateToolhelp32Snapshot.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1093</td>
<td>Process Hollowing</td>
<td>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.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1012</td>
<td>Query Registry</td>
<td>AZORult can check for installed software on the system under the Registry key Software\Microsoft\Windows\CurrentVersion\Uninstall.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1105</td>
<td>Remote File Copy</td>
<td>AZORult can download and execute additional files. Azorult has also downloaded a ransomware payload called Hermes.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1113</td>
<td>Screen Capture</td>
<td>AZORult can capture screenshots of the victim’s machines.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1032</td>
<td>Standard Cryptographic Protocol</td>
<td>AZORult can encrypt C2 traffic using XOR.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1082</td>
<td>System Information Discovery</td>
<td>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.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1016</td>
<td>System Network Configuration Discovery</td>
<td>AZORult can collect host IP information from the victim’s machine.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1033</td>
<td>System Owner/User Discovery</td>
<td>AZORult can collect the username from the victim’s machine.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1124</td>
<td>System Time Discovery</td>
<td>AZORult can collect the time zone information from the system.</td>
</tr>
</tbody>
</table>

Source: [https://attack.mitre.org/software/S0344/](https://attack.mitre.org/software/S0344/)
AZORult – Infection and compromise

- Example attack:
  - Infection vector
  - Execution
  - Persistence
  - Reconnaissance
  - Exfiltration

Image source: Trend Micro
Geographical distribution of AZORult attacks: December 2017 through December 2018

Data and image source: Kaspersky
Recent AZORult usage – Fake Coronavirus map

Fake Coronavirus tracking map drops AZORult on victim systems:
Legitimate Johns Hopkins Coronavirus Map

Legitimate map:
Recent AZORult technique – triple encryption

- Observed in a February 2020 phishing campaign:

  1. MT-209111.DOC
  2. XLS spreadsheet (4x)
  3. VBA Macro
  4. 1st layer of decryption
  5. PowerShell
  6. 2nd layer of decryption
  7. 3rd layer of decryption
  8. MT-209111.jpg / c2ef3.exe

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)
  - See example of fake Google update binary below which contained AZORult trojan:

```
<table>
<thead>
<tr>
<th>Autorun Entry</th>
<th>Description</th>
<th>Publisher</th>
<th>Image Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Scheduler</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Update TaskMachineCore</td>
<td>Установщик Google</td>
<td>Google Inc.</td>
<td>c:\program files\google\update\googleupdate.exe</td>
</tr>
<tr>
<td>GoogleUpdateTaskMachineUA</td>
<td>Установщик Google</td>
<td>Google Inc.</td>
<td>c:\program files\google\update\googleupdate.exe</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gupdate</td>
<td>Keeps your Google software...</td>
<td>Google Inc.</td>
<td>c:\program files\google\update\googleupdate.exe</td>
</tr>
<tr>
<td>gupdate</td>
<td>Keeps your Google software...</td>
<td>Google Inc.</td>
<td>c:\program files\google\update\googleupdate.exe</td>
</tr>
<tr>
<td>localNETService</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Image source: Bleeping Computer
AZORult Intrusion Detection Rules/Signatures

• Yara Rules:
  • https://malpedia.caad.fkie.fraunhofer.de/yara/win.azorult
  • https://github.com/Yara-Rules/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

• Snort rules:
  • https://www.snort.org/rule_docs/1-47339
  • https://www.snort.org/rule_docs/1-49548
  • https://snort.org/rule_docs/1-47602
The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate AZORult.

<table>
<thead>
<tr>
<th>DEFENSE/MITIGATION/COUNTERMEASURE</th>
<th>405(d) HICP REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide social engineering and phishing training to employees.</td>
<td>[10.S.A], [1.M.D]</td>
</tr>
<tr>
<td>Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.</td>
<td>[10.S.A], [10.M.A]</td>
</tr>
<tr>
<td>Ensure emails originating from outside the organization are automatically marked before received.</td>
<td>[1.S.A], [1.M.A]</td>
</tr>
<tr>
<td>Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
<tr>
<td>Implement spam filters at the email gateways; Keep signatures and rules updated.</td>
<td>[1.S.A], [1.M.A]</td>
</tr>
<tr>
<td>Block suspicious IP addresses at the firewall; Keep firewall rules are updated.</td>
<td>[6.S.A], [6.M.A], [6.L.E]</td>
</tr>
<tr>
<td>Implement whitelisting technology to ensure that only authorized software is allowed to execute.</td>
<td>[2.S.A], [2.M.A], [2.L.E]</td>
</tr>
<tr>
<td>Conduct system hardening to ensure proper configurations.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
<tr>
<td>Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
</tbody>
</table>

Background information can be found here: [https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf](https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf)
Indicators of Compromise:

- There are instances of obsolete IOCs being reused, so any organization attempting to defend themselves should consider all possibilities.
- New IOCs are constantly being released, especially with a tool as prominent and frequently used as AZORult. It is therefore incumbent upon any organization attempting to defend themselves to remain vigilant, maintain situational awareness and be ever on the lookout for new IOCs to operationalize in their cyberdefense infrastructure.

<table>
<thead>
<tr>
<th>INDICATOR</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://daticho.ac%5B.%5Dug">http://daticho.ac[.]ug</a></td>
<td>Domain</td>
<td>Command and control server</td>
</tr>
<tr>
<td><a href="http://ravor.ac%5B.%5Dug">http://ravor.ac[.]ug</a></td>
<td>Domain</td>
<td>Command and control server</td>
</tr>
<tr>
<td>ssl[.admin[.itybuy[.it</td>
<td>Domain</td>
<td>Command and control server</td>
</tr>
<tr>
<td>hairpdf[.com/stat/stella.exe</td>
<td>Domain</td>
<td>Malware storage</td>
</tr>
<tr>
<td>hairpdf[.com/stat/sputilk.exe</td>
<td>Domain</td>
<td>Malware storage</td>
</tr>
<tr>
<td>ivanzakharov91[.example.com</td>
<td>Domain</td>
<td>Malware storage</td>
</tr>
<tr>
<td>Driverconnectsearch[.info</td>
<td>Domain</td>
<td>Malware storage</td>
</tr>
<tr>
<td>host.colocrossing[.com</td>
<td>Domain</td>
<td>Malware storage</td>
</tr>
<tr>
<td>Driverconnectsearch[.info</td>
<td>Domain</td>
<td>Malware storage</td>
</tr>
<tr>
<td>185.154.21[.]208</td>
<td>IP address</td>
<td>Malware storage</td>
</tr>
<tr>
<td>192.3.179[.]203</td>
<td>IP address</td>
<td>Malware storage</td>
</tr>
<tr>
<td>08EB8F2E441C26443EB9ABE5A93CD942</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>5B2680F80A003976C379CAF5CAD6564</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>B0EC3E594D20B9D38CC8591BAFF0148B</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>FE8938F0BAAAF90516A80610F6EE210484</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>2274174ed24425f41362aa207168b491e6fb55cab208116070f91c049946097a</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>6f1bf0f05c9a30f3c7b6b581d4bfb0194d1725120b242972ca95c6ecc7eb79bc</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>a75b318e2ae6678fd1f252d6b33919203262eb59e08ac3292b8bad54ca612</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>12791e14ba82d36d434e7c7c0b81c7975ce802a430724134b7e0cce5a7bb185</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>97c016bab36a85ca830376ec4c8c7e0e25edbb55f626aaee6219ade7468cee19</td>
<td>MD5</td>
<td>Executable</td>
</tr>
<tr>
<td>f291c822ee00c56655b2900f1c8881e415</td>
<td>MD5</td>
<td>Executable</td>
</tr>
</tbody>
</table>
References

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

- Seamless Campaign Delivers Ramnit via RIG EK at 188.225.82.158. Follow-up Malware is AZORult Stealer.

- The Seamless Campaign Drops Ramnit. Follow-up Malware: AZORult Stealer, Smoke Loader, etc.

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

- Threat Actors Using Legitimate PayPal Accounts To Distribute Chthonic Banking Trojan

- Kaspersky Threats: TROJAN-PSW.WIN32.AZORULT

- AZORult Trojan Uses Fake ProtonVPN Installer to Disguise Attacks

- AZORULT Malware Information

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

- Malpedia: Azorult
  - https://malpedia.caad.fkie.fraunhofer.de/details/win.azorultcampaign

- Trend Micro: AZORULT Malware Information
• Malicious coronavirus map hides AZORult info-stealing malware

• Battling online coronavirus scams with facts
  • https://blog.malwarebytes.com/social-engineering/2020/02/battling-online-coronavirus-scams-with-facts/

• AZORult Campaign Adopts Novel Triple-Encryption Technique
  • https://threatpost.com/azorult-campaign-encryption-technique/152508/

• AZORult Trojan Uses Fake ProtonVPN Installer to Disguise Attacks

• Azorult Trojan Steals Passwords While Hiding as Google Update

• CB TAU Threat Intelligence Notification: Common to Russian Underground Forums, AZORult Aims to Connect to C&C Server, Steal Sensitive Data

• AZORult Malware Abusing RDP Protocol To Steal the Data by Establish a Remote Desktop Connection
  • https://gbhackers.com/azorult-malware-abusing-rdp-protocol/

• Reverse Engineering, Malware Deep Insight
  • https://vk-intel.org/2017/07/

• Azorult loader stages
  • https://maxkersten.nl/binary-analysis-course/malware-analysis/azorult-loader-stages/

• MITRE: AZORult
  • https://attack.mitre.org/software/S0344/

• AZORULT VERSION 2: ATROCIOUS SPYWARE INFECTION USING 3 IN 1 RTF DOCUMENT

• AZORult++: Rewriting history
  • https://securelist.com/azorult-analysis-history/89922/

• TROJAN-PSW.WIN32.AZORULT
Questions

Upcoming Briefs

• COVID-19 Cyber Threats
• Threat Modelling for Mobile Health Systems

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Health Sector Cybersecurity Coordination Center (HC3)

Background

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

**Sector & Victim Notifications**
Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

**White Papers**
Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

**Threat Briefings & Webinar**
Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.