LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

AZORult Malware

OVERALL CLASSIFICATION IS

TLP:WHITE

04/16/2020

Report #: 202004161000

Agenda

Image source: NJCCIC

- 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)

Introduction

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

Image source: Bleeping Computer

AZORult – Attack Vectors

Image source: Ad Astra Games

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

Image source: LinkedIn

Mapping AZORult against the MITRE ATT&CK Framework

MITRE ATT&CK Techniques used by AZORult:

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

Source: https://attack.mitre.org/software/S0344/

AZORult – Infection and compromise

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

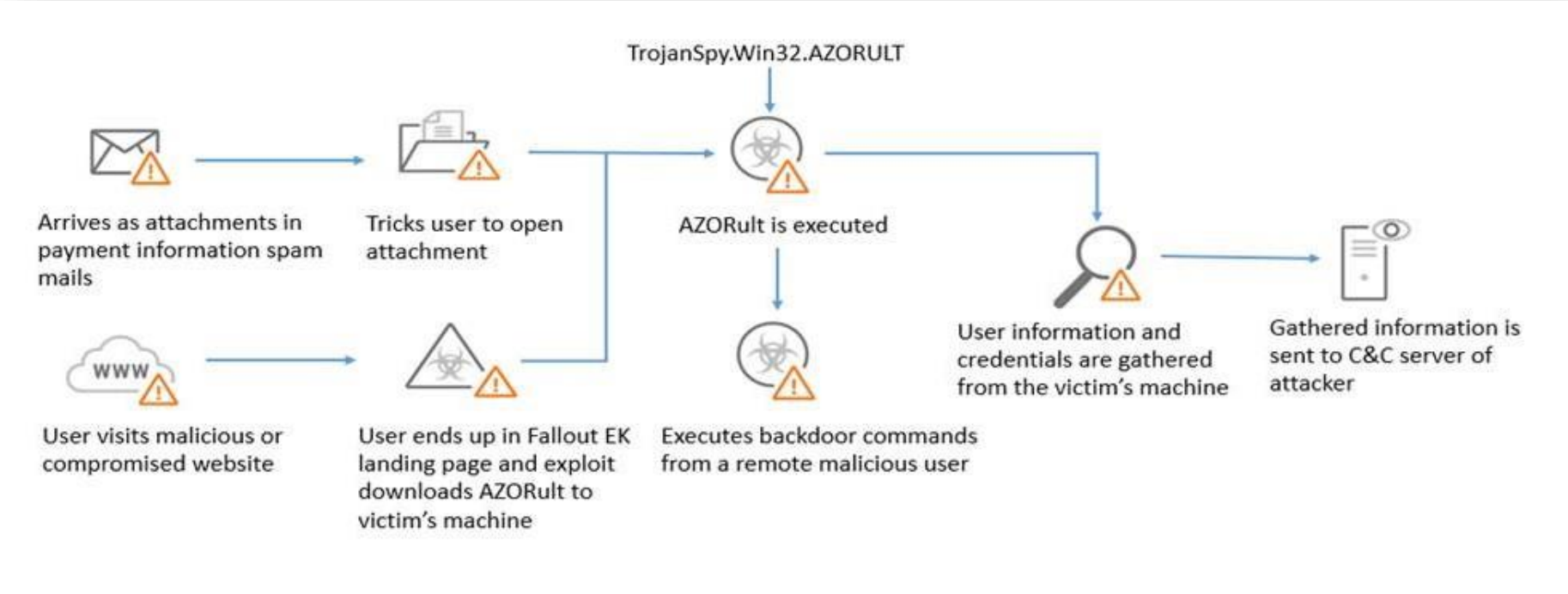
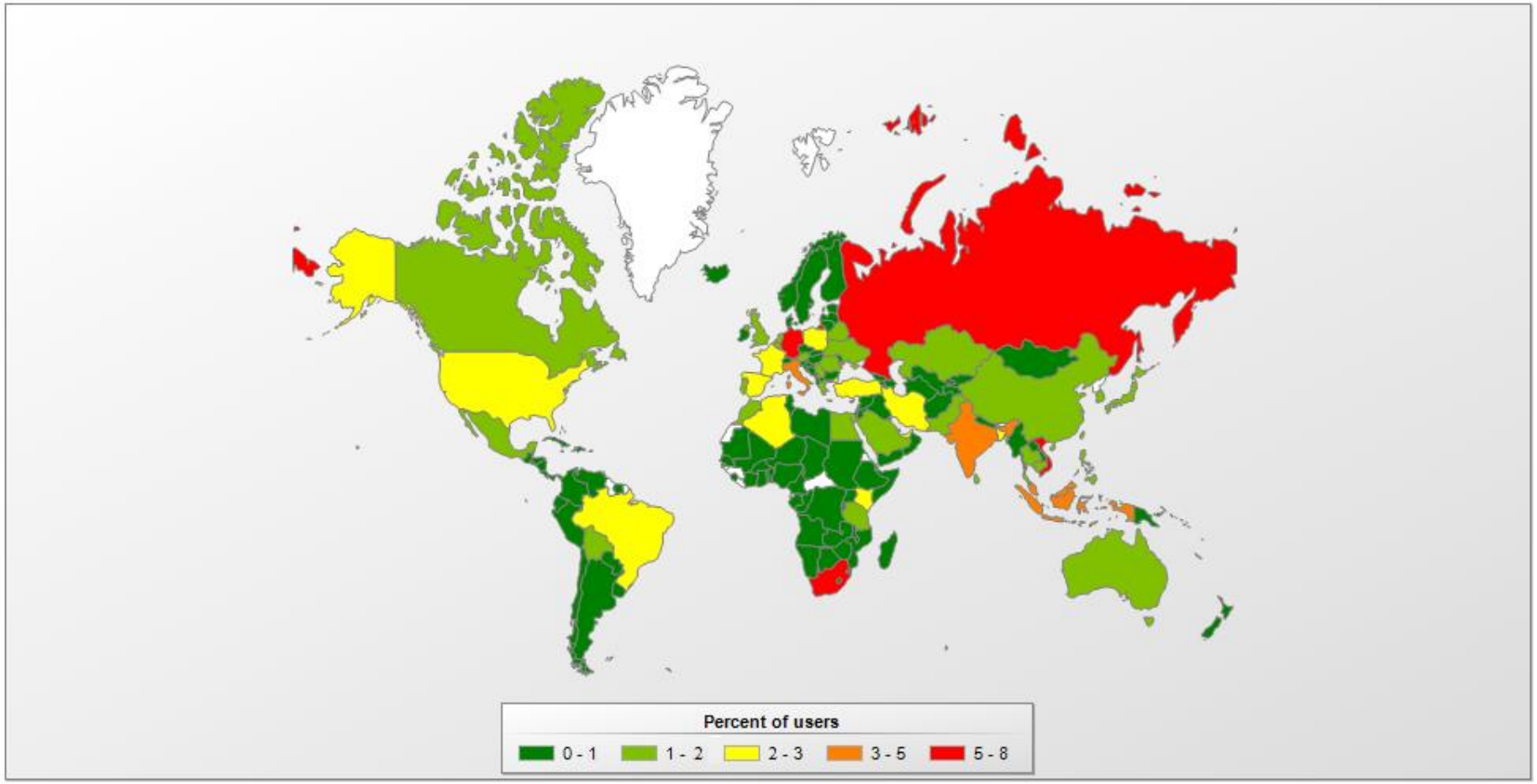


Image source: Trend Micro

AZORult – Origination of attacks

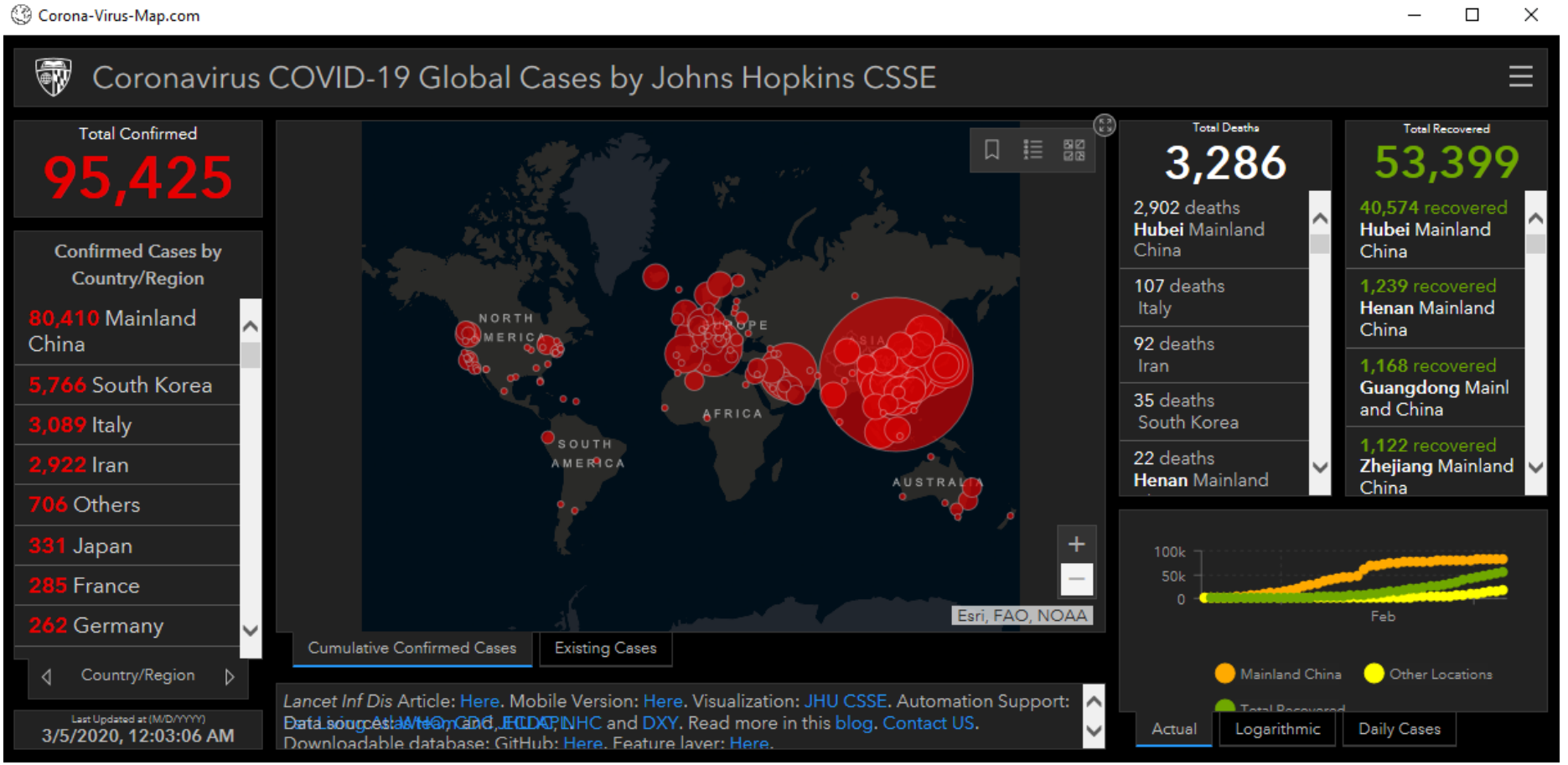
Geographical distribution of AZORult attacks: December 2017 through December 2018



Data and image source: Kaspersky

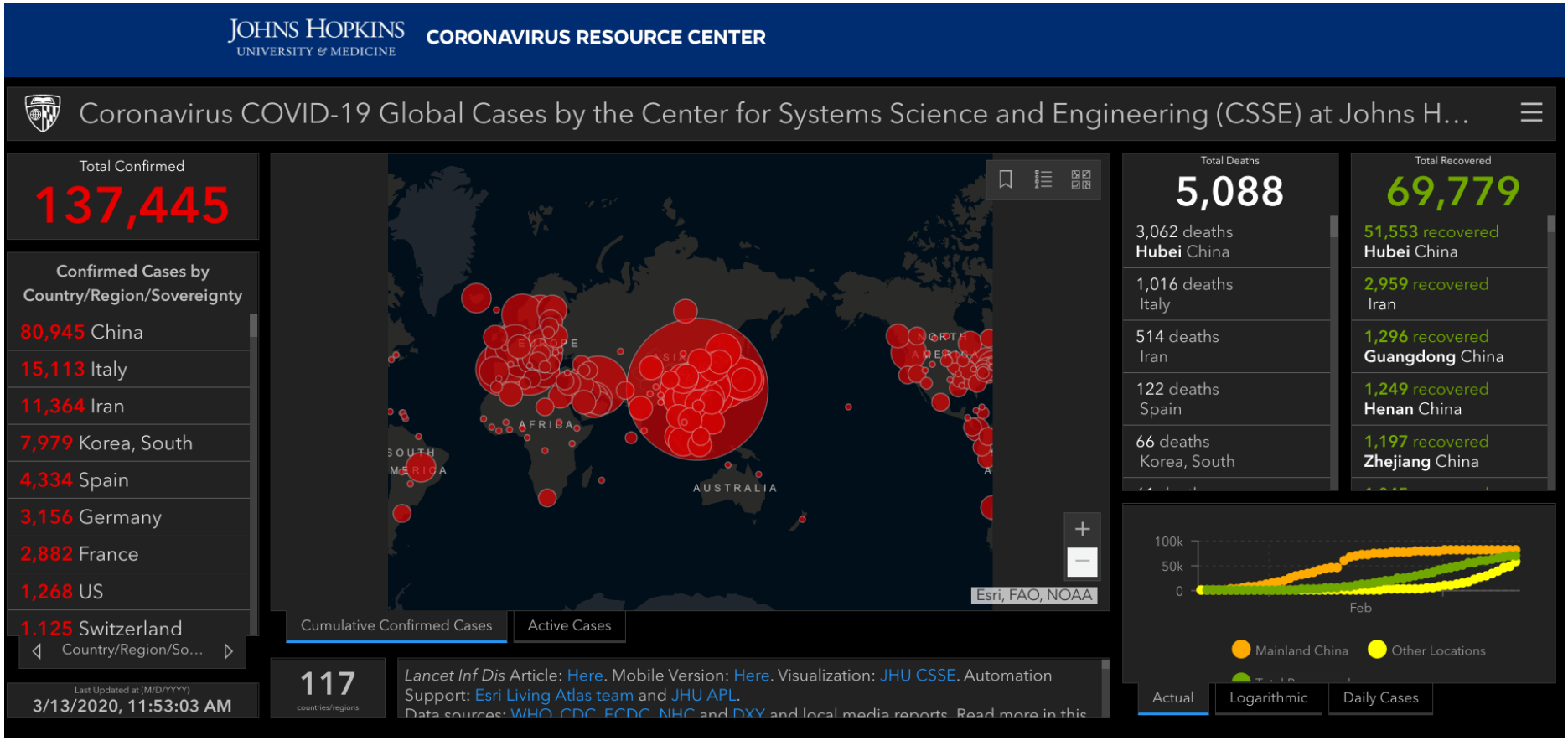
Recent AZORult usage – Fake Coronavirus map

Fake Coronavirus tracking map drops AZORult on victim systems:



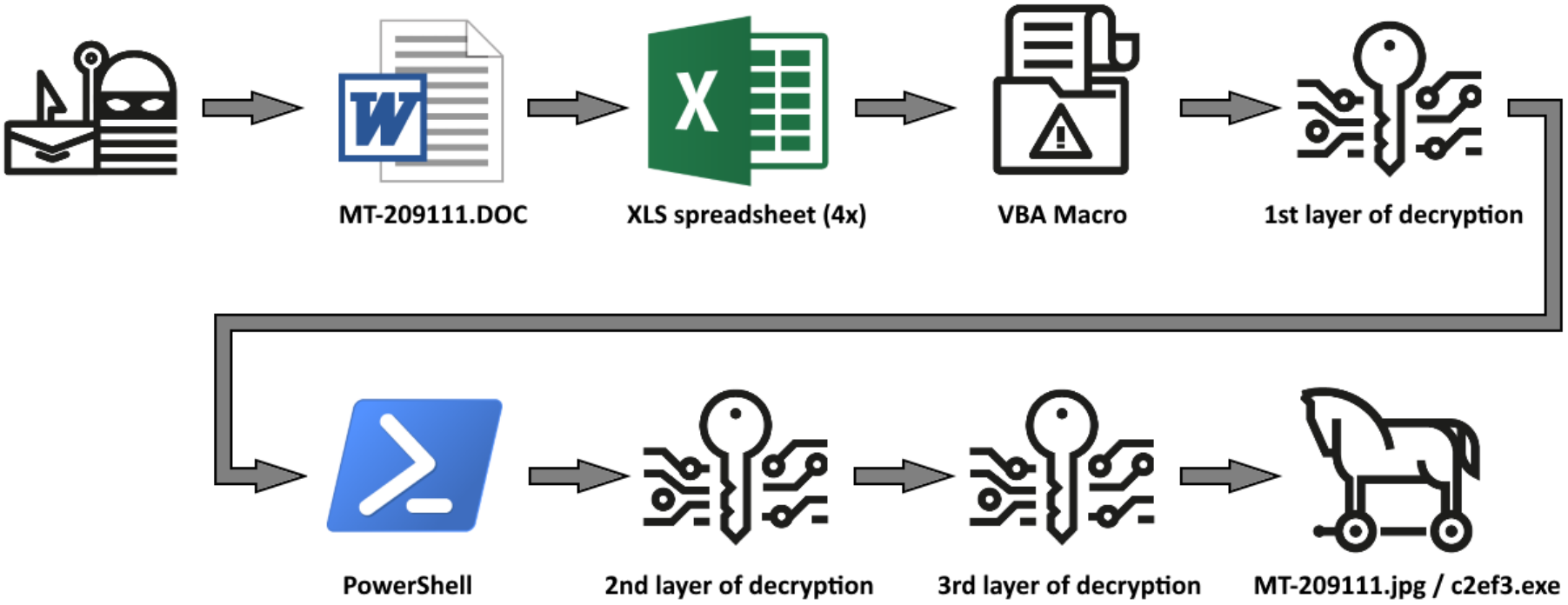
Legitimate Johns Hopkins Coronavirus Map

Legitimate map:



Recent AZORult technique – triple encryption

- Observed in a February 2020 phishing campaign:

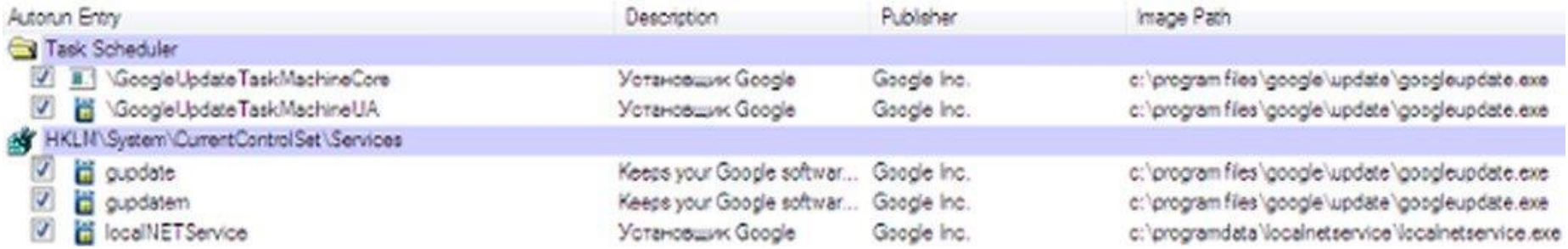


Data and image source: ThreatPost

AZORult - 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:



Autorun Entry	Description	Publisher	Image Path
Task Scheduler			
\GoogleUpdateTaskMachineCore	Установщик Google	Google Inc.	c:\program files\google\update\googleupdate.exe
\GoogleUpdateTaskMachineUA	Установщик Google	Google Inc.	c:\program files\google\update\googleupdate.exe
HKLM\System\CurrentControlSet\Services			
gupdate	Keeps your Google softwar...	Google Inc.	c:\program files\google\update\googleupdate.exe
gupdatem	Keeps your Google softwar...	Google Inc.	c:\program files\google\update\googleupdate.exe
localNETService	Установщик Google	Google Inc.	c:\programdata\localnetservice\localnetservice.exe

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

Mitigation Practices: AZORult

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.

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Provide social engineering and phishing training to employees.	[10.S.A], [1.M.D]
Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.	[10.S.A], [10.M.A]
Ensure emails originating from outside the organization are automatically marked before received.	[1.S.A], [1.M.A]
Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.	[7.S.A], [7.M.D]
Implement Intrusion Detection System (IDS); Keep signatures and rules updated.	[6.S.C], [6.M.C], [6.L.C]
Implement spam filters at the email gateways; Keep signatures and rules updated.	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall; Keep firewall rules are updated.	[6.S.A], [6.M.A], [6.L.E]
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	[2.S.A], [2.M.A], [2.L.E]
Implement access control based on the principal of least privilege.	[3.S.A], [3.M.A], [3.L.C]
Implement and maintain anti-malware solution.	[2.S.A], [2.M.A], [2.L.D]
Conduct system hardening to ensure proper configurations.	[7.S.A], [7.M.D]
Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.	[7.S.A], [7.M.D]

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

AZORult: Indicators of Compromise

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.

INDICATOR	TYPE	DESCRIPTION
http://daticho.ac[.]ug	Domain	Command and control server
http://ravor.ac[.]ug	Domain	Command and control server
ssl[.admin[.itybuy[.it	Domain	Command and control server
hairpd[.]com/stat/stella.exe	Domain	Malware storage
hairpd[.]com/stat/sputik.exe	Domain	Malware storage
ivanzakharov91[.]example.com	Domain	Malware storage
Driverconnectsearch[.]info	Domain	Malware storage
host.colocrossing[.]com	Domain	Malware storage
Driverconnectsearch[.]info	Domain	Malware storage
185.154.21[.]208	IP address	Malware storage
192.3.179[.]203	IP address	Malware storage
08EB8F2E441C26443EB9ABE5A93CD942	MD5	Executable
5B26880F80A00397BC379CAF5CADC564	MD5	Executable
B0EC3E594D20B9D38CC8591BAFF0148B	MD5	Executable
FE8938F0BAAF90516A90610F6E210484	MD5	Executable
2274174ed24425f41362aa207168b491e6fb55cab208116070f91c049946097a	MD5	Executable
6f51bf05c9fa30f3c7b6b581d4bbf0194d1725120b242972ca95c6ecc7eb79bc	MD5	Executable
a75b318eb2ae6678fd15f252d6b33919203262eb59e08ac32928f8bad54ca612	MD5	Executable
12791e14ba82d36d434e7c7c0b81c7975ce802a430724f134b7e0cce5a7bb185	MD5	Executable
97c016bab36a85ca830376ec48c7e70ee25edbb55f626aee6219ade7468cee19	MD5	Executable
f291c822ee0c5655b2900f1c8881e415	MD5	Executable

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
- Seamless Campaign Delivers Ramnit via RIG EK at 188.225.82.158. Follow-up Malware is AZORult Stealer.
  - https://malwarebreakdown.com/2017/11/12/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.
  - https://malwarebreakdown.com/2017/07/24/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'
  - https://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html
- Threat Actors Using Legitimate PayPal Accounts To Distribute Chthonic Banking Trojan
  - https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
- Kaspersky Threats: TROJAN-PSW.WIN32.AZORULT
  - https://threats.kaspersky.com/en/threat/Trojan-PSW.Win32.Azorult/campaign
- AZORult Trojan Uses Fake ProtonVPN Installer to Disguise Attacks
  - https://securityintelligence.com/news/azorult-trojan-uses-fake-protonvpn-installer-to-disguise-attacks/
- 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
- Malpedia: Azorult
  - https://malpedia.caad.fkie.fraunhofer.de/details/win.azorultcampaign
- Trend Micro: AZORULT Malware Information
  - https://success.trendmicro.com/solution/000146108-azorult-malware-information-kAJ4P000000kEK2WAM

References

- Malicious coronavirus map hides AZORult info-stealing malware
  - https://www.scmagazine.com/home/security-news/news-archive/coronavirus/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
  - https://securityintelligence.com/news/azorult-trojan-uses-fake-protonvpn-installer-to-disguise-attacks/
- Azorult Trojan Steals Passwords While Hiding as Google Update
  - https://www.bleepingcomputer.com/news/security/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
  - https://www.carbonblack.com/2019/09/24/cb-tau-threat-intelligence-notification-common-to-russian-underground-forums-azorult-aims-to-connect-to-cc-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
  - https://cysinfo.com/azorult-version-2-atrocious-spyware-infection-using-3-1-rtf-document/
- AZORult++: Rewriting history
  - https://securelist.com/azorult-analysis-history/89922/
- TROJAN-PSW.WIN32.AZORULT
- https://threats.kaspersky.com/en/threat/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.**