Can You Detect This?

Inside The Ransomware Operator's Toolkit

SANS Ransomware Summit 2022

Peter O _pete_0
Yatin Wadhwa yatinwad

Agenda

- Review of common tools and techniques in 2021
- Ransomware attack objectives
- Mapping an attack to detection opportunities
- Understanding human behaviors
- Spotting the adversary... unusual activities
- Useful resources for defenders

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

OPSEC…. Let’s Talk

- CTI dilemma
  - Reveal & share Intel with community vs exposure to the adversary
- Conti leak
  - Chats discussing TheDFIRReport cases
  - Using CTI to track other actors
  - Data-set had usernames, infrastructure etc
- Protect
  - Data – sources, usernames, host…
  - Capability – Infrastructure config, detection…
- Traffic Light Protocol (TLP)


```
{
  "ts": "2020-10-14T14:03:28.371585",
  "from": "buza@q3mcco35auwcstmt.onion",
  "to": "professor@q3mcco35auwcstmt.onion",
  "body": "https://thedfirreport.com/2020/10/08/ryuks-return/"
}
{
  "ts": "2020-10-14T14:06:04.813669",
  "from": "professor@q3mcco35auwcstmt.onion",
  "to": "buza@q3mcco35auwcstmt.onion",
  "body": "well, not much different from our movements"
}
{
  "ts": "2020-10-14T14:06:08.381836",
  "from": "professor@q3mcco35auwcstmt.onion",
  "to": "buza@q3mcco35auwcstmt.onion",
  "body": "yes, practically nothing"
}
```


https://www.cisa.gov/tlp

Briefing is **TLP WHITE**
Data & Capabilities is **TLP RED**

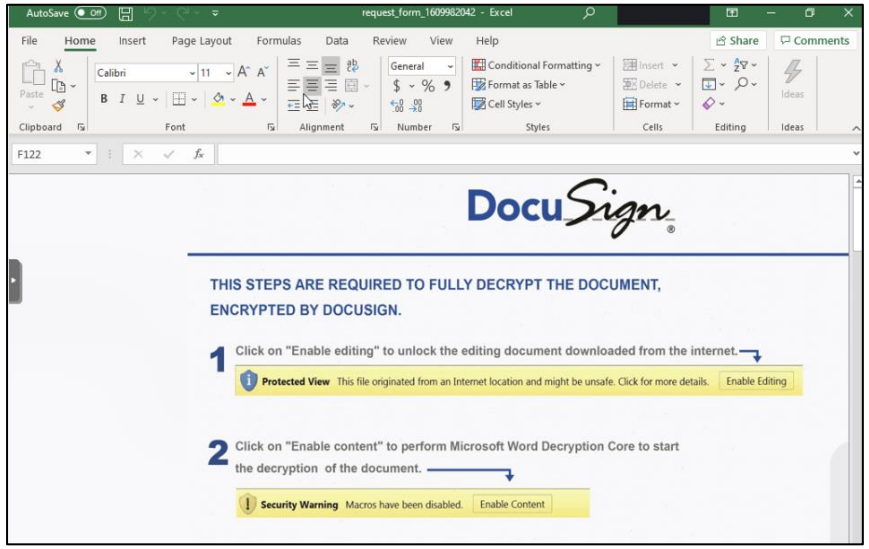
Adversary Trends – Initial Access

- Phishing is the primary initial access vector for delivery of malware.
  - Trickbot
  - Bazar
  - IcedID
  - Hancitor

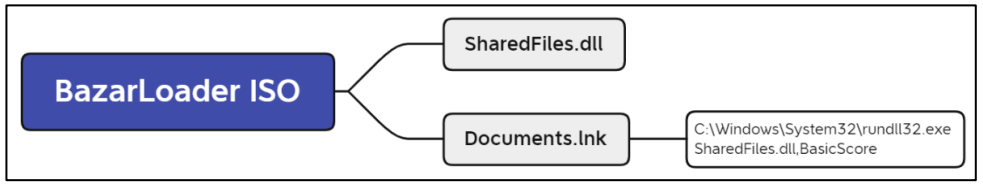
- Increase in use of "**.ISO**" images as compared to macro-based Office documents. [T1553.005]

- Serve as "**Access Brokers**" for various Ransomware Groups.
  - Conti
  - Sodinokibi

- External Facing Vulnerabilities – **ProxyShell** [T1190]
  - Exchange Exploit Leads to Domain Wide Ransomware
  - APT35 Automates Initial Access Using ProxyShell



DocuSign Themed Excel Document



Contents of Malicious ISO

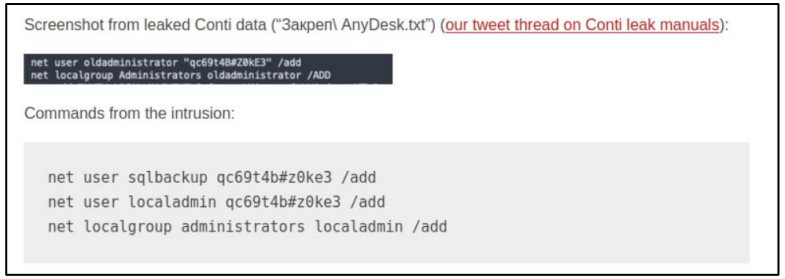
Detection Opportunity

Office applications spawning unusual child processes
- Living of the Land Binaries
- Windows Shell Command

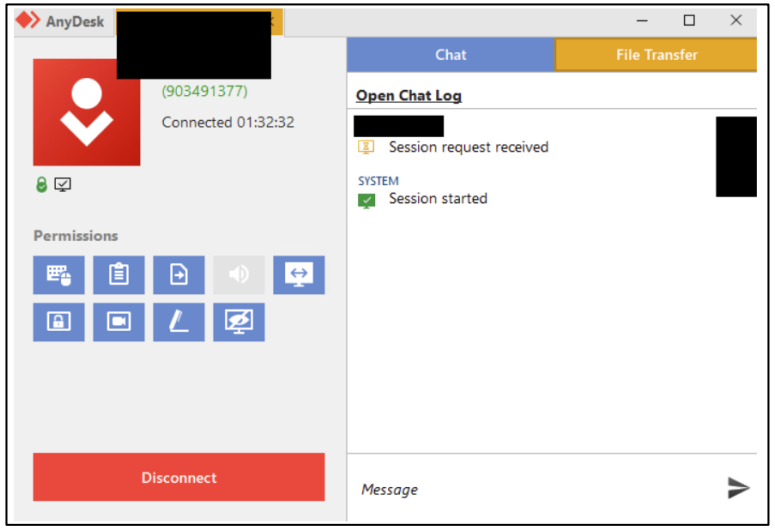
Adversary Trends – Maintain Foothold

"Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access." – MITRE ATT&CK

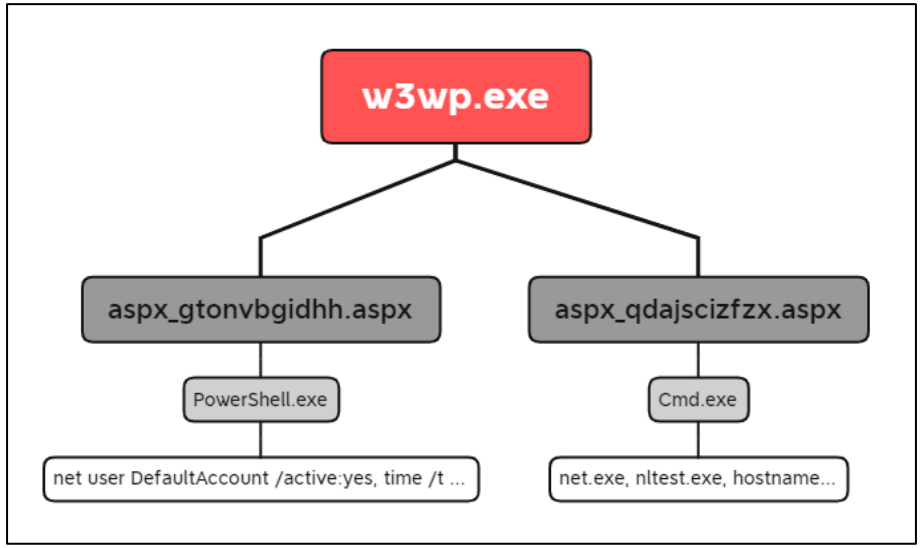
Techniques
Scheduled Task [T1053.005]
BITS Jobs [T1197]
Addition of new user [T1136.002]
Web Shells [T1505.003]
Remote Access Applications [T1219]
Run Keys [T1547.001]



User Addition



Usage of AnyDesk



Web Severs Spawning Web Shells

Detection Opportunity

- Usage of remote management tools such as "**AnyDesk**", "**Atera Agent**", "**TeamViewer**".
- Web servers spawning shells
  - **Example:** w3wp.exe -> cmd.exe or powershell.exe
- Monitor creation of scheduled tasks.

Adversary Trends – Escalate, Harvest & Evade

Phase	Techniques
Escalate	• UAC Bypass [T1548.002] • Named Pipe Impersonation
Harvest	• Registry Hive Access [T1003.002] • Browser Password Enumeration • Dumping LSASS [T1003.001] • Zerologon Exploit [T1210] • Accessing LSASS Process
Evade	• Process Injection [T1055.002] • Disabling Security Tools [T1562.001] • Masquerading [T1036.005] • Post-exploit payload Obfuscation

Image: “C:\Windows\System32\cmd.exe”
CommandLine: “C:\Windows\system32\cmd.exe /c echo 4d64fbbbf34 > \\.\pipe\b4312c”
ParentImage: “C:\Windows\System32\runonce.exe”
ParentCommandLine: “C:\Windows\system32\runonce.exe”

Escalation via GetSystem

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

Usage of ProcDump

```
PowerShell -nop -exec bypass -EncodedCommand
UwBlAHQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARABpAHMAYQBiAGwAZQBSA
GUAYQBsAHQ AaQBtAGUATQBvAG4AaQB0AG8AcgBpAG4AZwAgACQAdAByAHUAZQA=
```

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

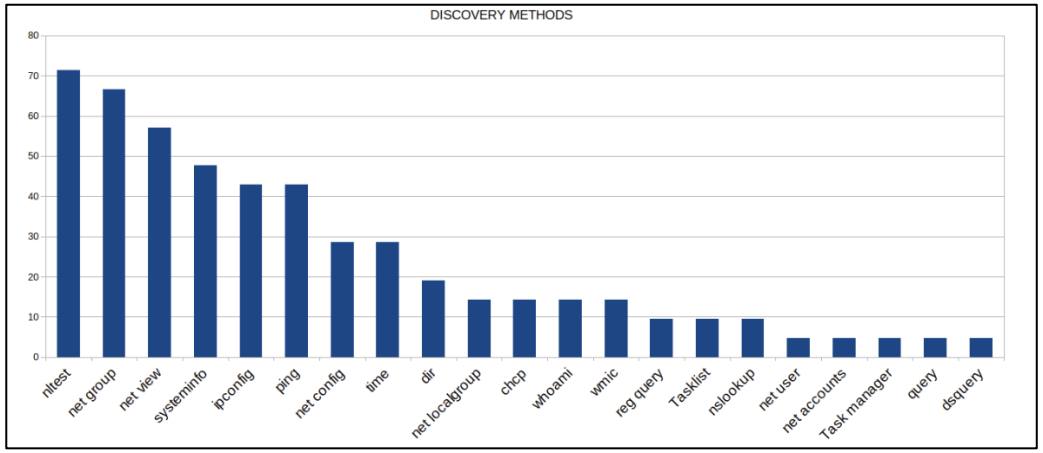
Disabling of Windows AV

Detection Opportunity

- Monitoring default named pipes.
- Creation of *.dmp files on the disk using Task Manager and Procdump.
- Disabling of Windows Defender AV

Adversary Trends – Discovery & Lateral Movement

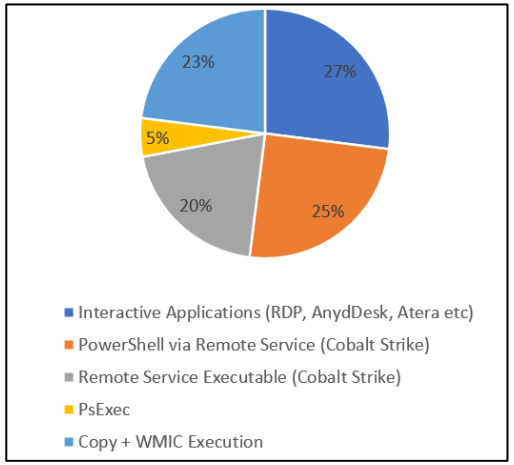
- Reliance on windows in-built utilities for performing internal reconnaissance.



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
```

- TA utilize remote desktop applications, remote service execution among other techniques for moving laterally.



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.

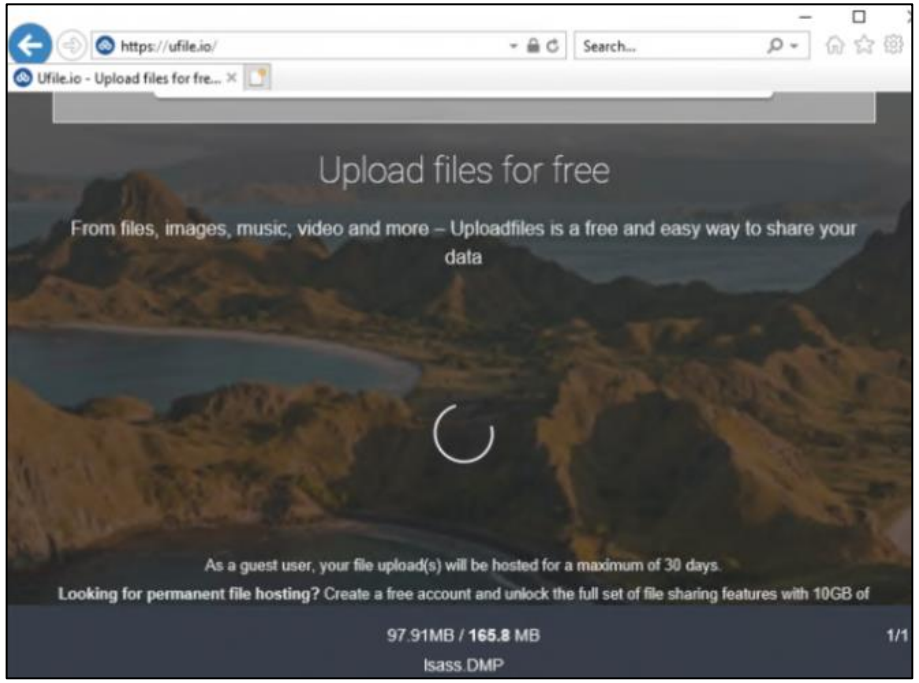
```
cmd.exe /C copy 192145.dll \\<INTERNAL_IP>\ADMIN$ /Y /Z
psexec.exe -accepteula -d -s \\<INTERNAL_IP> rundll32.exe C:\windows\192145.dll,StartW
```

Detection Opportunity

- Execution of utilities such as net.exe, nltest.exe in a short timespan.
- Usage of 3rd party tools (AdFind, BloodHound)
- Usage of Sysinternals PsExec

Adversary Trends – Achieve Objectives

Objectives	Methods
Collection	• Compression of data files using 7z • Dumping of SQL Database using sqlcmd.exe
Exfiltration	• Use of utilities such as WinSCP, Rclone, Filezilla • File sharing services – MEGA, ufile.io
Impact	• Domain wide encryption



Uploading of LSASS dump to "ufile.io"

Detection Opportunity

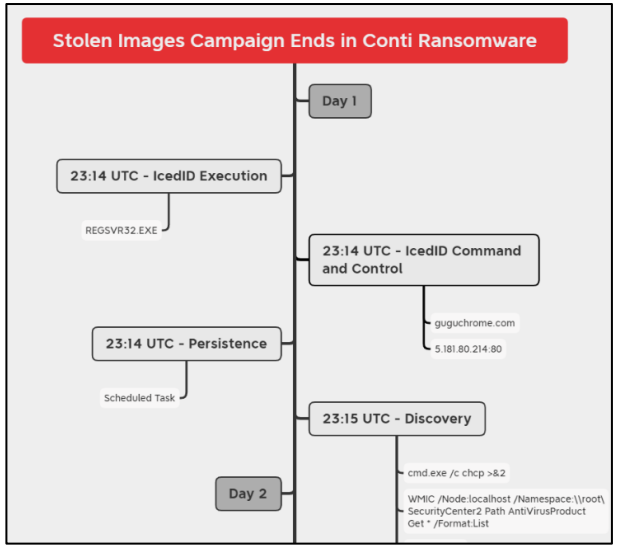
- Connection to cloud storage services.
- Installation of data copy utilities.
- Usage of compression utilities such as 7-zip

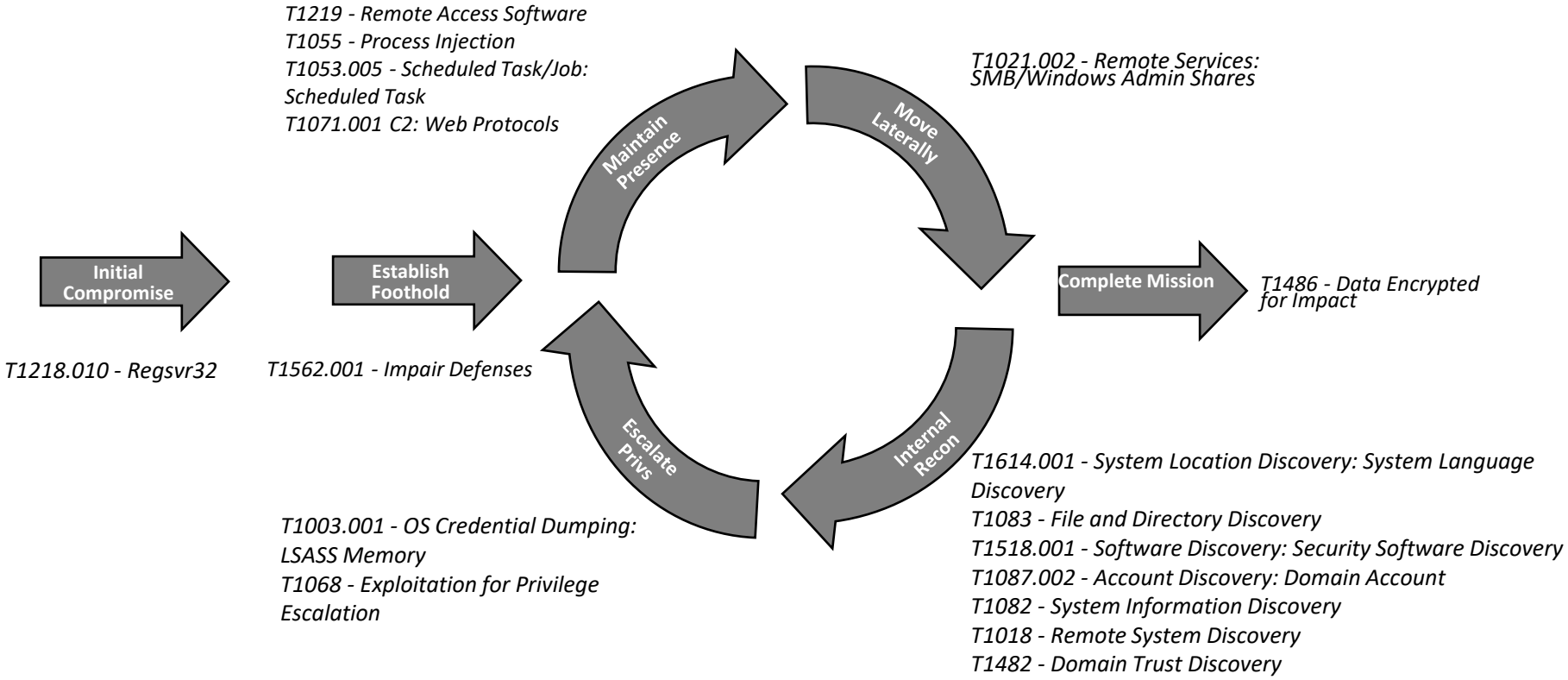
Adversary Trends Overview– MITRE ATT&CK FRAMEWORK

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, T1482, T1124, T1016]	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]	7-zip [T1560.001]		Rclone [T1567.002]	BitLocker [T1486]
Hancitor [T1566.001 & T1566.002]		Run Keys [T1547.001]	UAC-TokenMagic.ps1	Masquerading [T1036.005]	Rubeus [T1558.003 & T1558.004]	AdFind (Batch Script: adf.bat) [T1087.002, T1482, T1018]	WMIC [T1047]			WinSCP [T1048.003]	DiskCryptor [T1486]
IcedID [T1566.001 & T1566.002]		Create Account [T1136.002]	FilelessUACBypass.ps1		Dumping of LSASS using Task Manager,Process Hacker and ProcDump [T1003.001]	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]				
		Web Shells [T1505.003]			esentutl: To gather MSEdge history and webcache [T1555.003]	Exchange Commandlets[T1114]: Get-MailboxRegionalConfiguration Get-Mailbox Get-ExchangeServer Get-InboxRule	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					

Mapping The Attack Lifecycle

Stolen Images Campaign case timeline





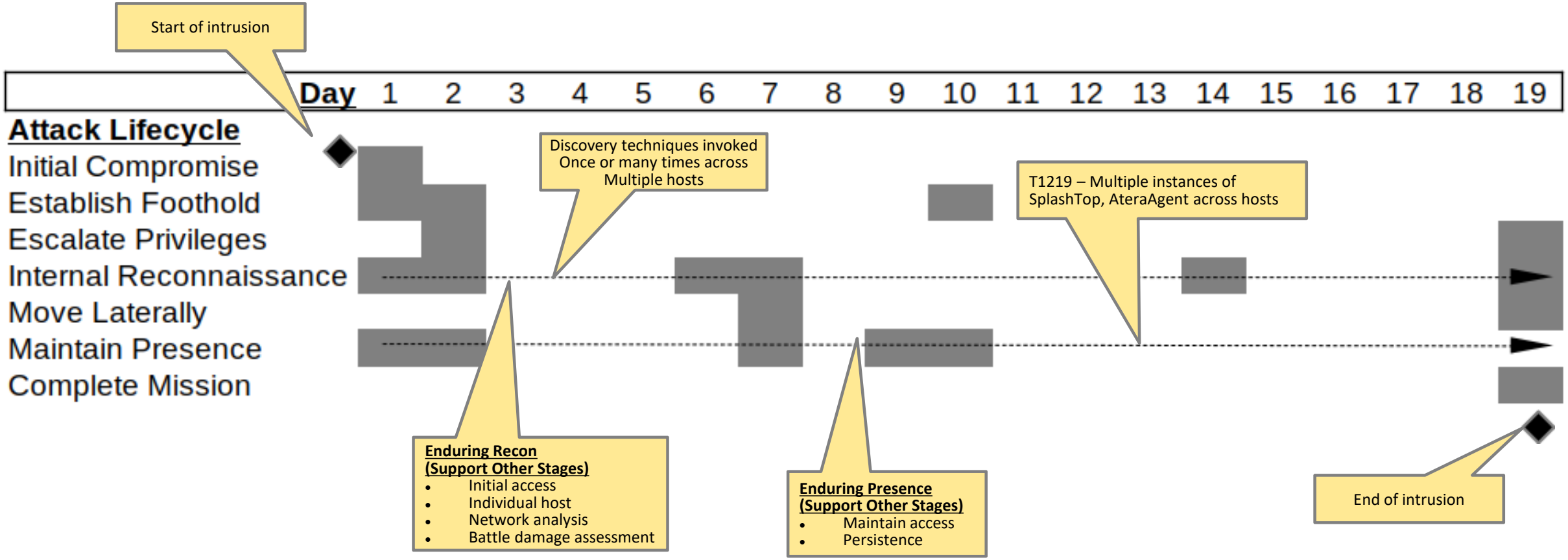
Detection Opportunity

- Adversary actions repeated during Internal Recon & Maintain Presence stages
- Focus detection early on in the attack lifecycle

* Observable – An event (benign or malicious) on a network or system (NIST SP 800-150)

https://www.mandiant.com/resources/targeted-attack-lifecycle
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/

Attack Lifecycle Analysis



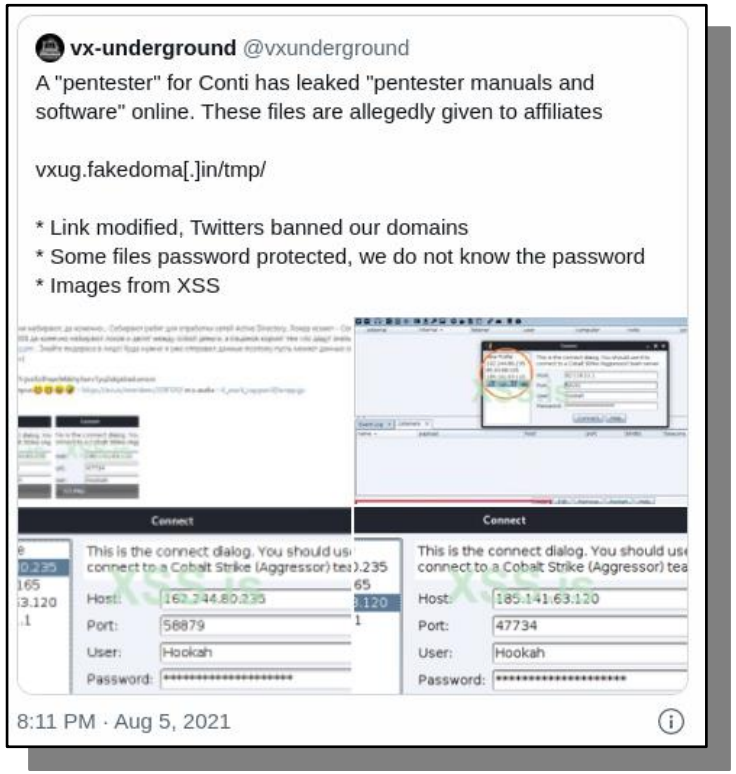
Detection Opportunity

- Correlate multiple discovery actions
- Focus on atomic actions
- Avoid general WMI,CMD use

https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/

Attack Lifecycle & Playbooks

- **Human behaviors**
- **Evidence of playbooks being followed**
  - Familiar scripts and applications
  - Same malware deployed
  - Hands-on keyboard actions (commands)
- **'Conti leak' confirmed existence of playbooks**
- **Playbooks provide tried and battle tested TTPs**
  - Repeatable & does the job != advanced
- **Mistakes and odd actions observed**



Detection Opportunity

- Use of unmodified OST scripts (exploits etc)
- Rarely change default Cobalt Strike malleable profile
- Consistent use of CLI LOLBAS procedures followed

Playbooks – Operator Errors

- Hands-on keyboard actions increase risk of errors!

Cobalt Strike AV_Query aggressor script. Beacon interaction

```
beacon> AV_Query
[+] Determining what AntiVirus is installed...
[+] host called home, sent: 1437 bytes
[+] received output:

PID|Name|Path

1820|McTray|C:\Program Files (x86)\McAfee\Common Framework\McTray.exe
2380|shstat|C:\Program Files (x86)\McAfee\VirusScan Enterprise\SHSTAT.EXE
4796|UdaterUI|C:\Program Files (x86)\McAfee\Common Framework\UdaterUI.exe
```

AV_Query entered in the shell on host

```
c:\windows\system32\cmd.exe /c av_query
```

- Others, "*tasklist /s ip*" - IP should be the remote computer
  - Likely a copy/paste error

Detection Opportunity

- Tool commands being entered directly on the host
- Copy & paste of commands/keywords

https://github.com/harleyQu1nn/AggressorScripts

Playbooks - Tools

- **Adf.bat**
  - AdFind – collection script
  - Observed in a number of cases ~2 years
  - Shared tool/re-used between groups (Ryuk and Conti)

```
adfind.exe -f "(objectcategory=person)"
adfind.exe -f "objectcategory=computer"
adfind.exe -f "(objectcategory=organizationalUnit)"
adfind.exe -sc trustdmp
adfind.exe -subnets -f (objectCategory=subnet)
adfind.exe -f "(objectcategory=group)"
adfind.exe -gcb -sc trustdmp
```

```
"ts": "2020-10-14T14:06:24.230768",
"from": "professor@q3mcco35auwcstmt.onion",
"to": "buza@q3mcco35auwcstmt.onion",
"body": "adf.bat - this is my f[redacted] batch file"
```

- **SAMTHEADMIN**
  - Active Directory vulnerabilities
  - CVE-2021-42278 and CVE-2021-42287

```
def samtheadmin(options):
    new_computer_name = f"SAMTHEADMIN-{random.randint(1,100)}$"
    new_computer_password = ''.join(random.choice(characters) for _ in range(12))
```

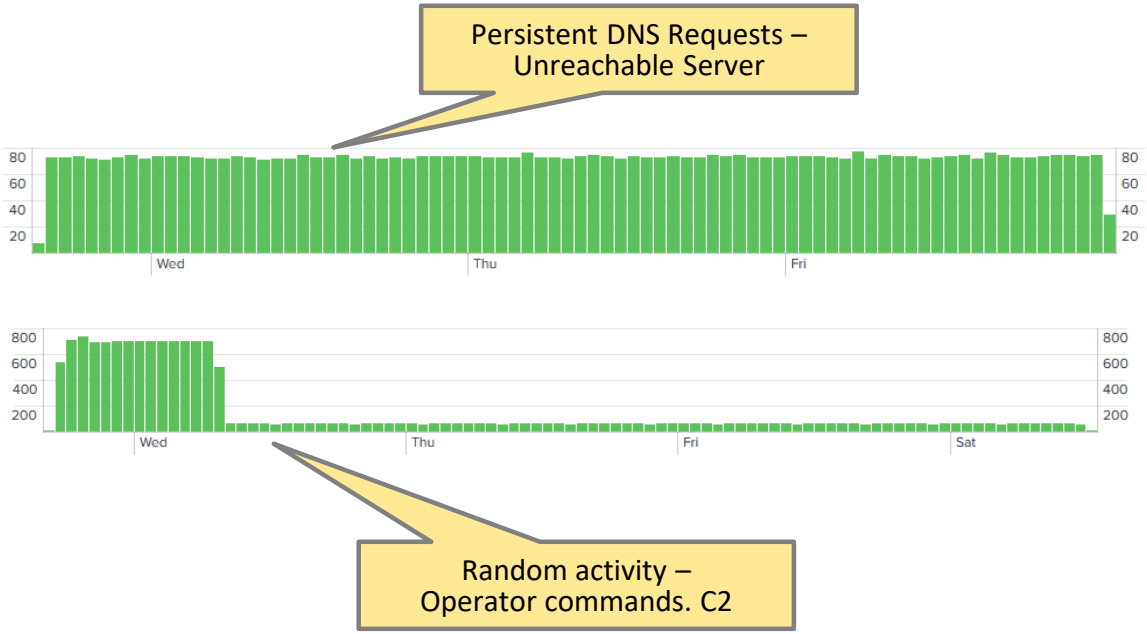
QueryName	QueryStatus
SAMTHEADMIN-92	9003
SAMTHEADMIN-20	9003

Detection Opportunity

- Scripts and binaries dropped in non-standard folders: C:\Windows\Temp, Music etc
- LDAP requests, errors such as 9003

Playbooks – Unusual Activities

- **Errors**
  - Beacon left running
  - Out of band tooling download
  - Remote computers
- **Territorial Dispute**
  - Shared similar techniques
  - Different lateral movement strategies
- **Indirect Actions**
  - Trickbot
  - Different goals and objectives




```
Company: Microsoft Corporation
OriginalFileName: esentutl.exe
CommandLine: "esentutl" /p /o C:\Users\[redacted]\AppData\Local\Temp\grabber_temp.edb
```

https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/

Detection Opportunity

- Unknown computer names
- Abnormal DNS requests
- User agent strings
- Unusual collection

Final Advice for Defenders

- Resources and pointers to help defend against ransomware
- Grugq's Cyber Security principles

1. Increase the cost of the compromise
2. Decrease the value of the compromise
3. Restrict adversarial freedom of movement post compromise
4. Increase ease of detecting a compromise
5. Increase chance of detecting a compromise
6. Audit trails for post compromise analysis
7. Vigilance

Best Practices/Prevention [1,2,3]
US CERT
https://www.cisa.gov/uscert/ncas/alerts/aa20-245a

Mandiant
https://www.mandiant.com/resources/ransomware-protection-and-containment-strategies

Detection [4,5,6]
NCSC (UK)
https://www.ncsc.gov.uk/information/logging-made-easy

https://github.com/The-DFIR-Report

Technique Testing [4,5]
Red Canary
https://github.com/redcanaryco/atomic-red-team

Emulation [5,7]
Scythe
https://github.com/scythe-io/community-threats

Education [7]
US CERT
https://www.cisa.gov/stopransomware

https://medium.com/@thegrugq/security-cyber-and-elections-part-3-9398f639aa28

THANK YOU!!

TheDFIRReport.com

TheDFIRReport

The Team:

kostastsale, RoxpinTeddy, iiamaleks, pigerlin, tas_kmanager, samaritan_o, MetallicHack, ICSNick, v3t0_, 0xtornado, svch0st