

CTRL + ALT + DEFEND

IT Admins vs. the World

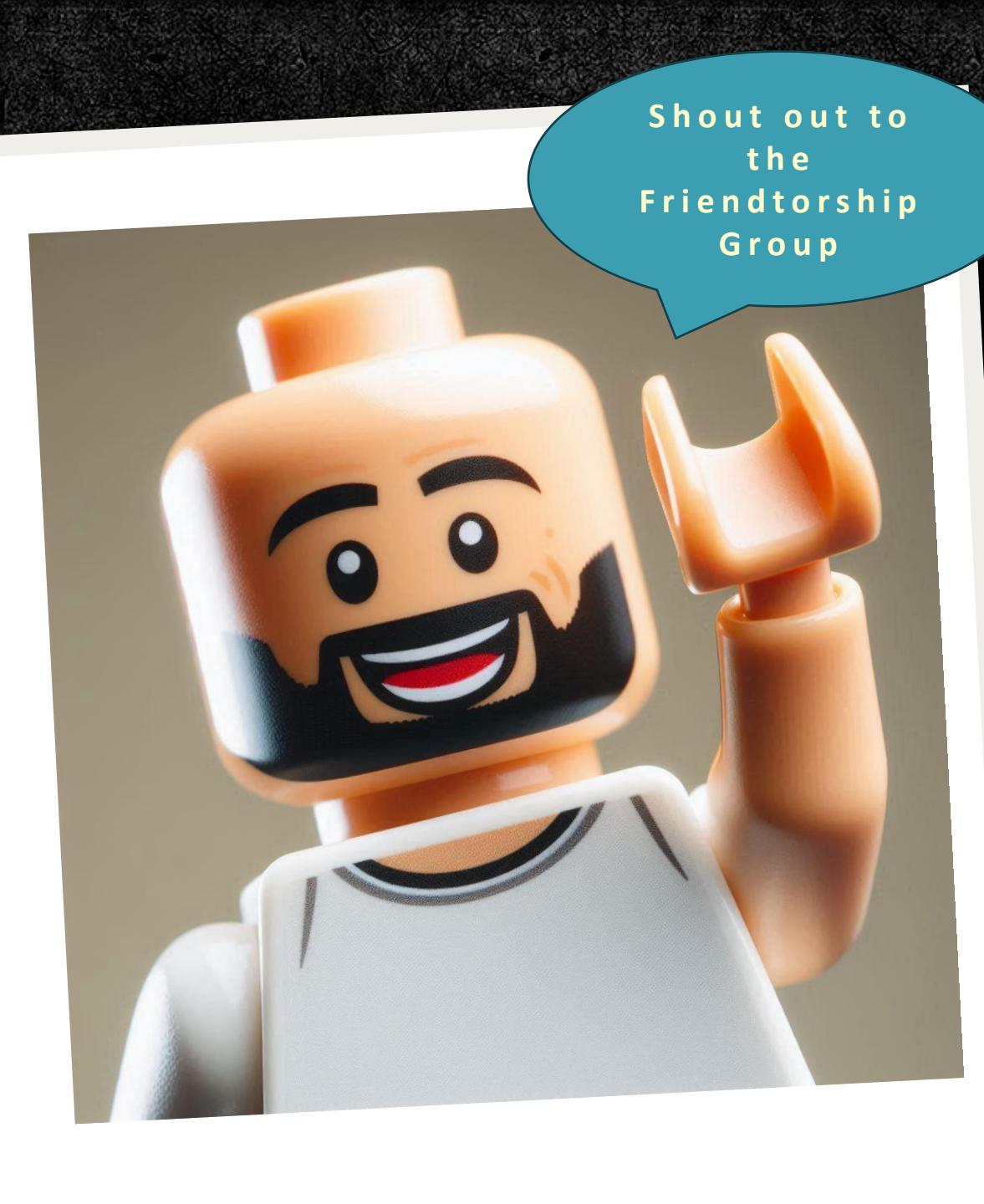
In an era where bad actors have mastered living off the land techniques and exploit simple vulnerabilities in technology to achieve their goals, understanding these tactics is more crucial than ever. This discussion will explore practical, real-world examples to enhance defenses against such attacks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





**Shout out to
the
Friendtorship
Group**

About Me

J.A. Medina

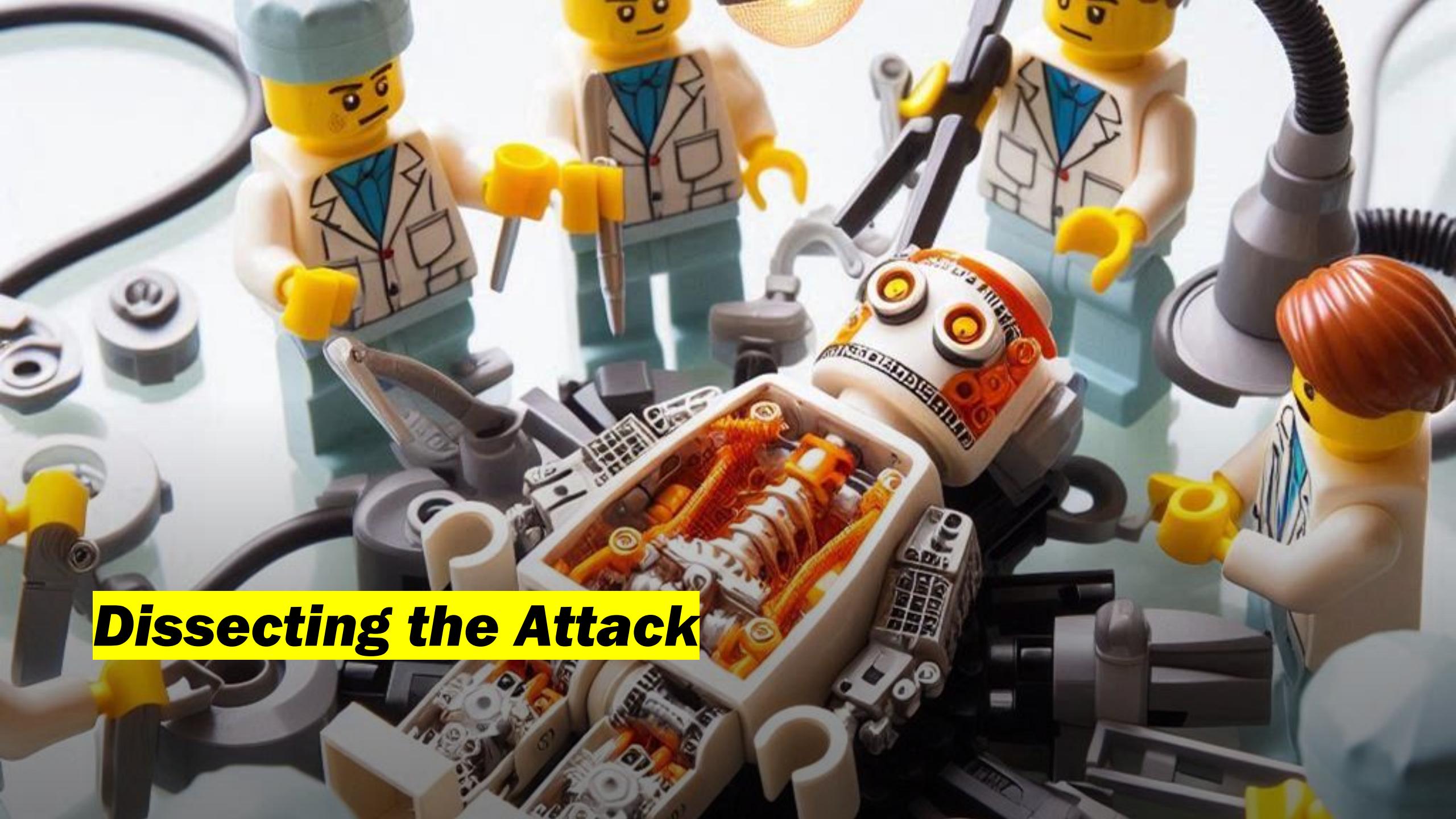
- Cybersecurity Dude, City of Littleton
- Director of Cybersecurity, @Fortune500
- CISSP, Linux+, OSCP+ (Candidate)
- 3 Real Babies, 3 Fur Babies
- Paratrooper in a previous life

<https://securitypimp.net/>

https://x.com/security_pimp

<https://github.com/varthdader>

<https://www.linkedin.com/in/jmedina303/>

A photograph of several LEGO minifigures dressed as scientists or technicians in a laboratory setting. They are gathered around a complex mechanical device, possibly a printer or a machine used for creating documents. One figure in the foreground is holding a small electronic component, while others look on. The scene is filled with various scientific and technical equipment, including a microscope, test tubes, and control panels. The overall theme is one of technical analysis and investigation.

Dissecting the Attack

Dissecting the Attack

Phishing

91% of cyberattacks start with a phishing email

MiTM

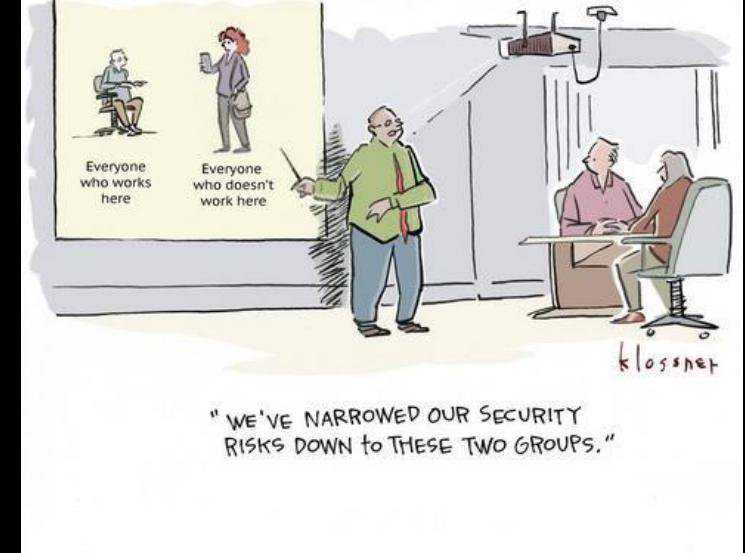
In 2021 was responsible for 19% of all cyber attacks

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]

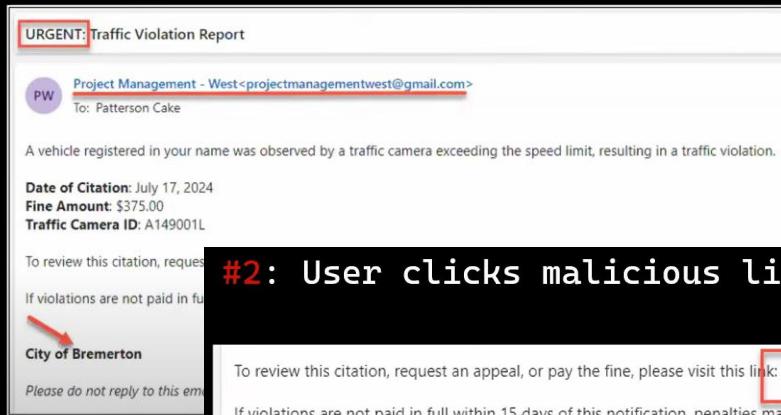
WHEN AN EMPLOYEE OPENS AN UNKNOWN EMAIL ATTACHMENT



Dissecting the Attack

[Phishing]

#1: Trigger an emotional response with call to action

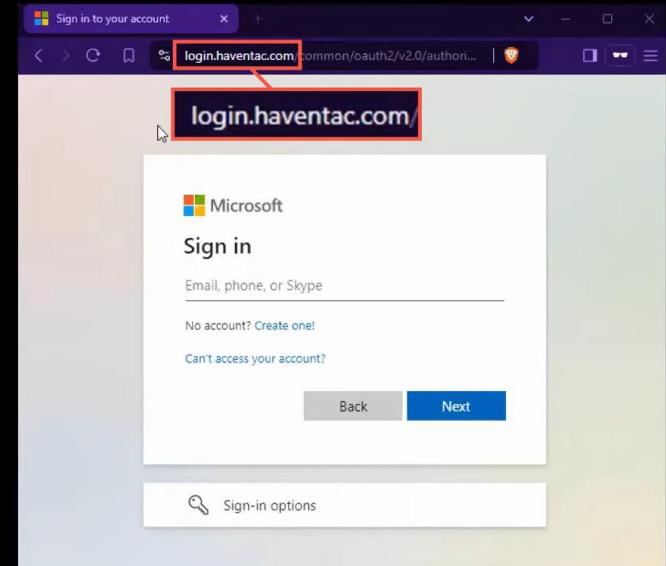


#2: User clicks malicious link to “Evil Proxy”

To review this citation, request an appeal, or pay the fine, please visit this link: [Traffic Violations](https://dropbox.com/css-java-optimization/d)
If violations are not paid in full within 15 days of this notification, penalties may apply

```
kali@kali: ~
:lures
+---+-----+-----+-----+-----+
| id | phishlet | hostname | path | redirector | redirect_url |
+---+-----+-----+-----+-----+
| 0  | new-a365 |          | /ppcIwpKL |           | https://outlo...
+---+-----+-----+-----+-----+
:lures get-url 0
https://login.haventac.com/ppcIwpKL
:|
```

#3: User visits malicious M365 login

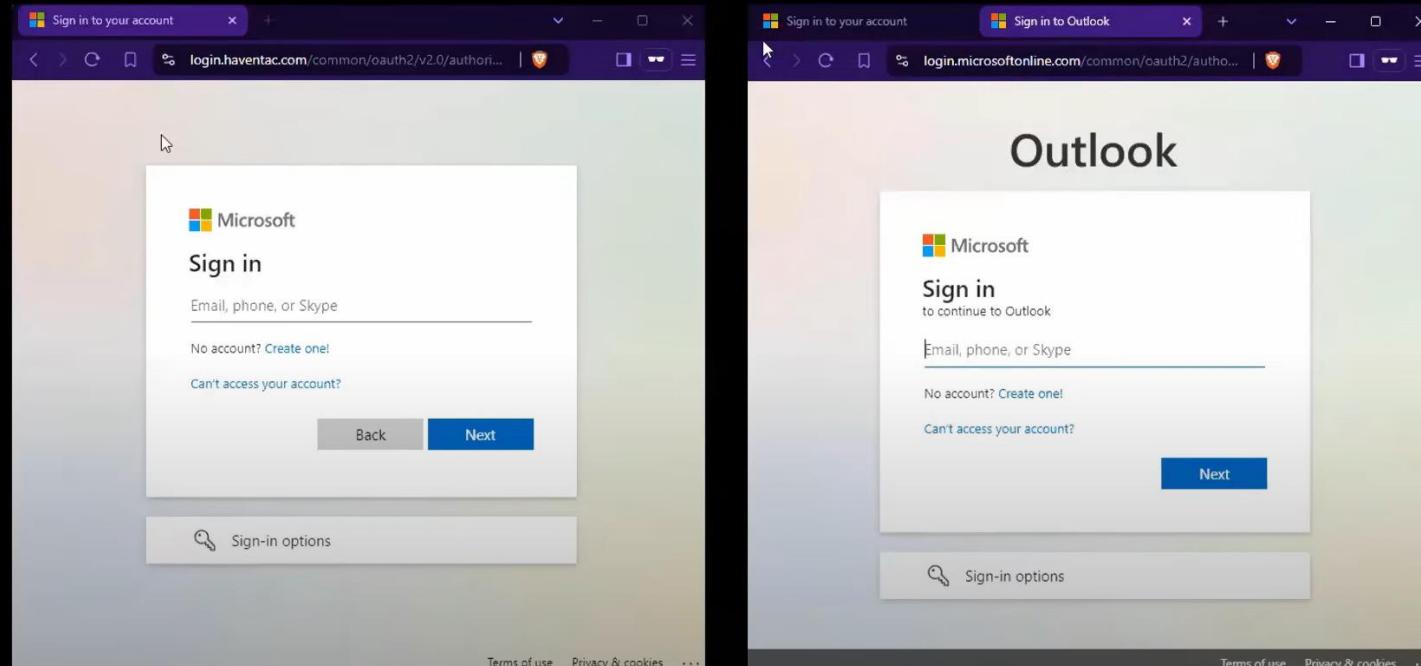


- Phishing Past MFA w/AiTM

Dissecting the Attack

[Phishing]

“Will the real M365 login please stand up!?!?”

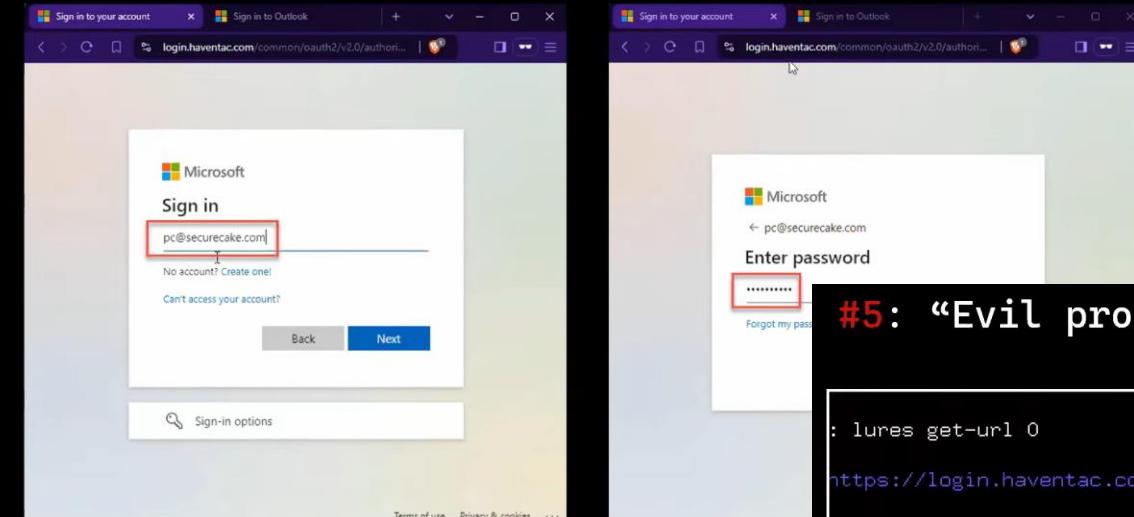


- Phishing Past MFA w/AiTM

Dissecting the Attack

[Phishing]

#4: User enters username and password



#5: “Evil proxy” captures username and password

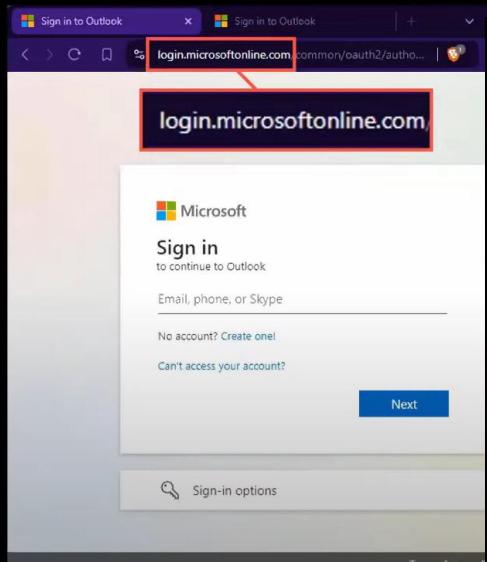
```
: lures get-url 0
https://login.haventac.com/ppcIwpKL
[19:12:58] [war] session cookie not found: https://login.haventac.com/ppcIwpKL (172.221.112.235) [new-o365]
[19:12:58] [imp] [0] [new-o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 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] [+] dynamic redirect to URL: https://outlook.office.com
[19:17:30] [+++] [0] detected authorization URL - tokens intercepted: /common/SAS/ProcessAuth
```

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
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
1WltEZUfGMrBjg-Ydk3ZsdoBAAA.AgABFwQAAAApTwJmzXqdR4BN2mihe0MYAgDs_wUA9P9VmI0YaT-BnmGhUsMA8dPnzLGN6YRGw1bH0sbsrP
JE_u19sRJRL01PqaJ911MwzOpLixFxmZQHznCwaYHiEi3Fa9F9-r70166pb8z5ZBBelHJmrERpLjfBKulmSM16p2_yONCdbffeMbCC2tsr6Ai"}]
```

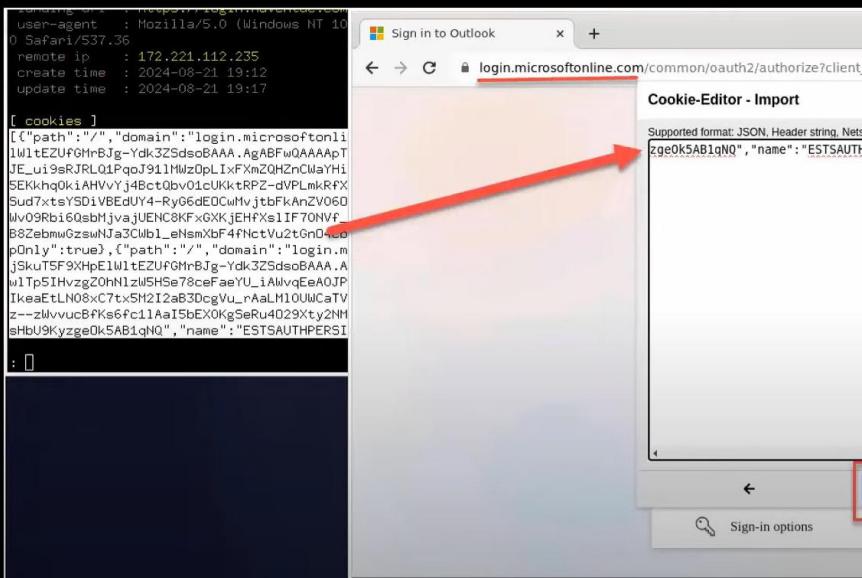


- Phishing Past MFA w/AiTM

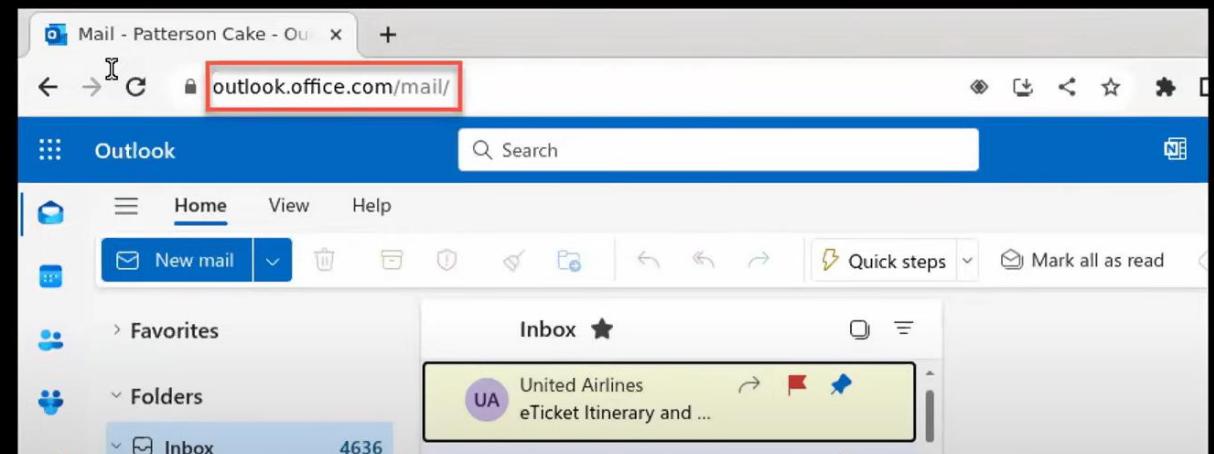
Dissecting the Attack

[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!

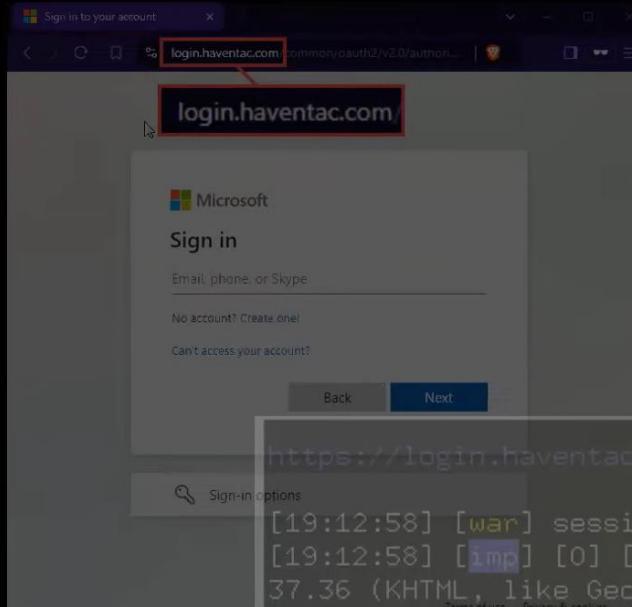


- Phishing Past MFA w/AiTm

Dissecting the Attack

[Phishing]

#1-7: Becoming the “User”



M365 IAM:

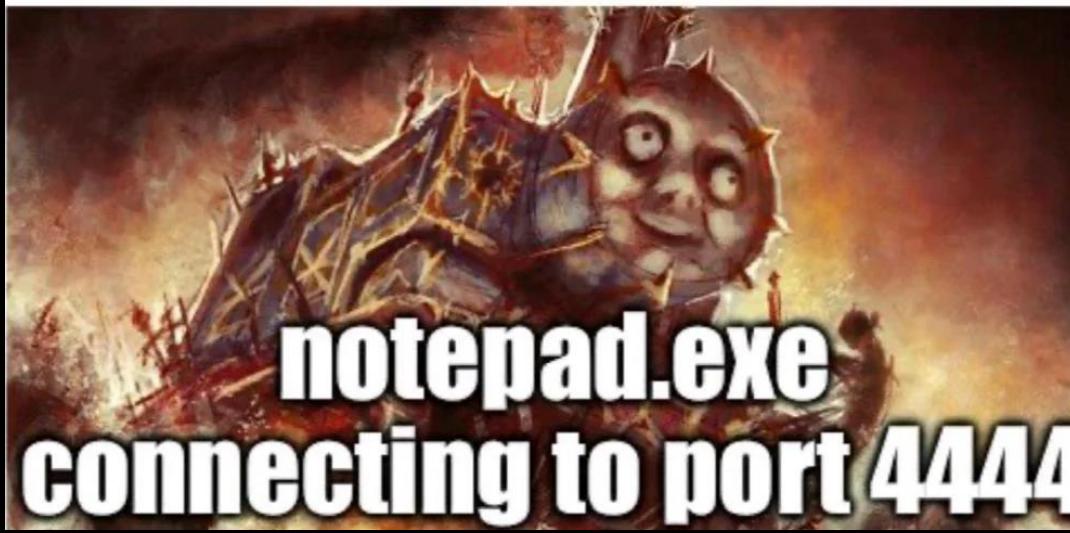
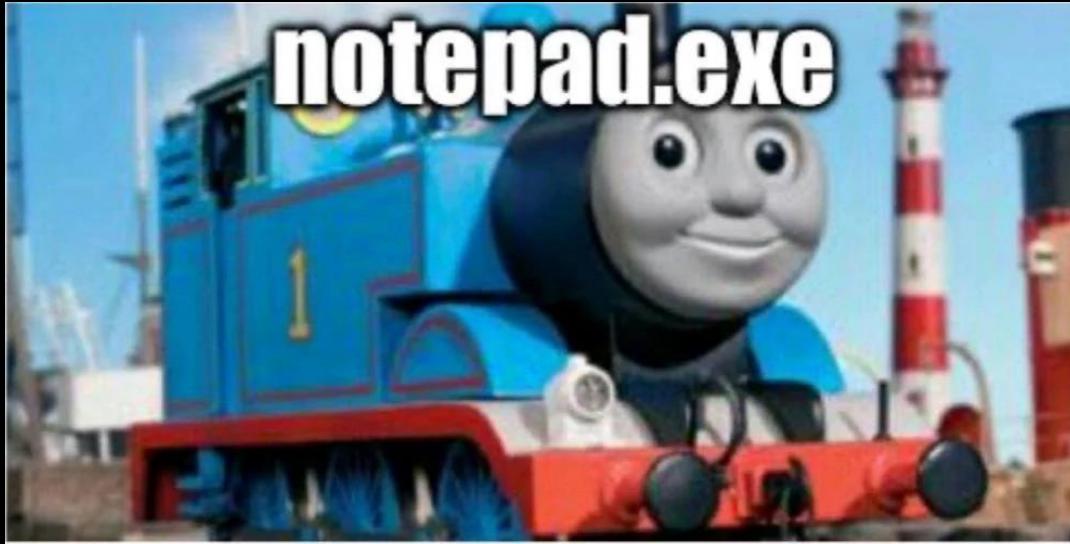
- a. Username/PW ✓
- b. Device/Browser (User-Agent) ✓
- c. MFA/Device ✓
- d. Session Cookie ✓
- e. Source IP

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] [imp] [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]

OVERALL PROCESS REVISTED



redsiege.com

11

AS-REQ – User encrypts timestamp using NTLM Hash

AS-REP – KDC/DC decrypts payload, sends TGT

TGS-REQ – User sends TGT, requests ticket for service

TGS-REP – KDC/DC builds ticket for service

ST – Sent ticket to server



Member Server

***Dissecting the Attack
[Lateral Movement]***



SERVICE TICKET

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 NTLM Hash



Your portion

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

redsiege.com

12

Dissecting the Attack
[Lateral Movement]

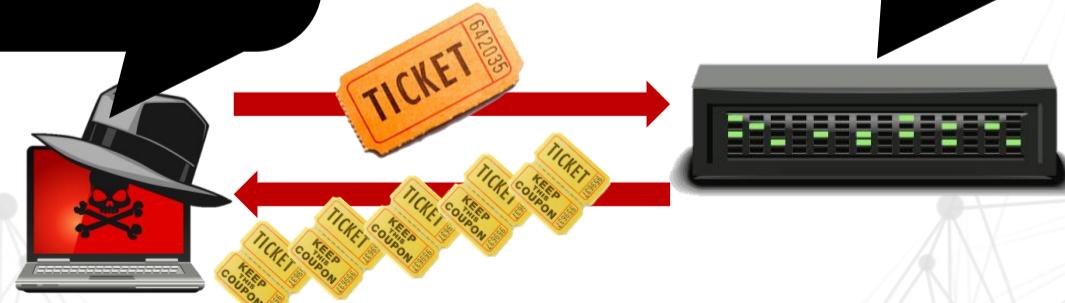
REQUESTING TICKETS

The system doesn't have to be...

- Accessible
- Available
- Exist*

Here is my TGT,
Can I get a ST for
Sql01
Web01
Mail01
...

Sure thing! Your TGT looks good.
The services will authorize you,
not me. I can't keep track of all
that



Dissecting the Attack
[Lateral Movement]



KERBEROASTING

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]

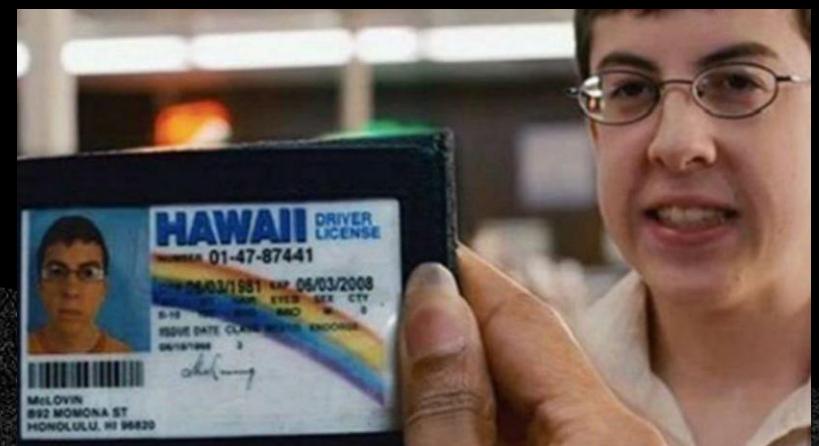
- Golden Ticket – Requires full domain compromise. Use for **persistence and pivoting**
- Kerberoasting – Requires access as any user. Use to **escalate** and **pivot**
- Silver Ticket – Requires service hash. Use for **persistence and escalation**
- Pass-the-Ticket – Requires access as user. Use to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

Kerberos Attacks (Tim Medin)

<https://www.youtube.com/watch?v=9l0FpUA25Nk>

<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

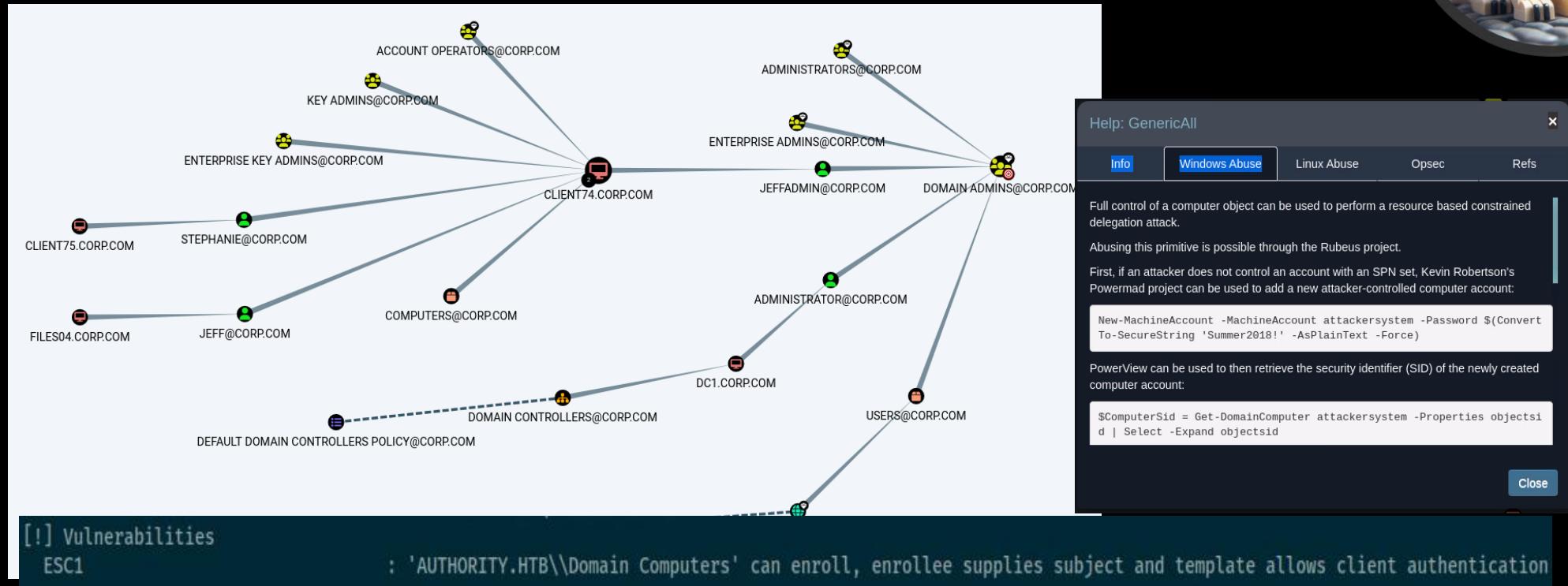
SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED

`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

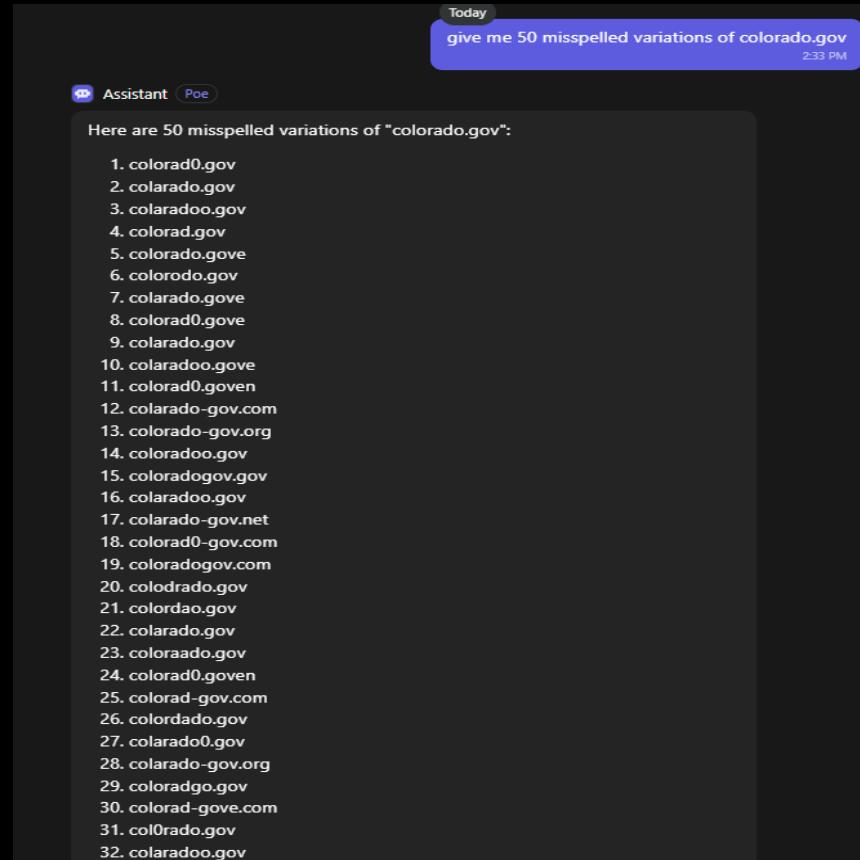
[Domain Hardening]



- 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>



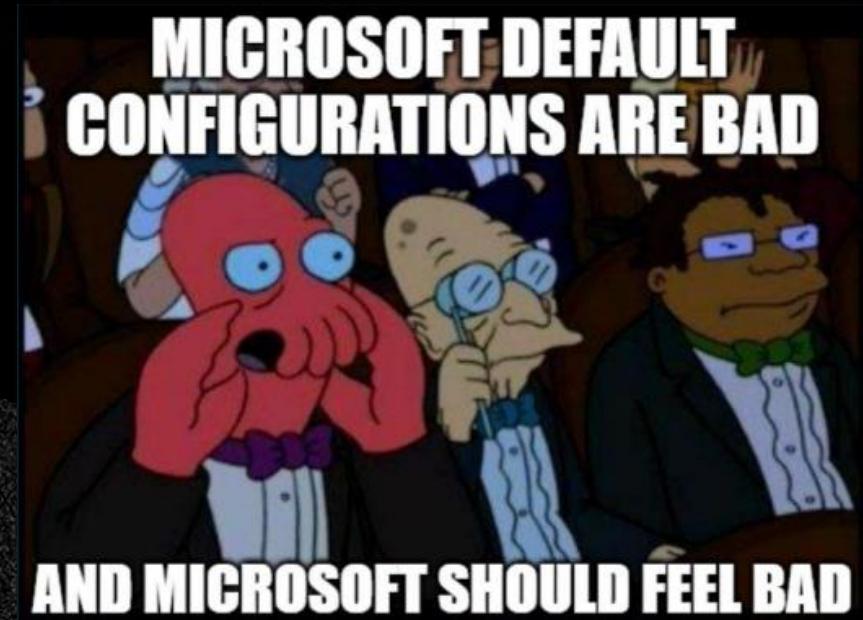
<script> ..... </script>

</body>
</html>
```

- 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]**



Home > Users

Users | Sign-in logs

City of Littleton

Search

Date : Last 1 month Show dates as : Local Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date Application Status IP address Location

Columns

Search columns

Date Request ID User Username Application Status IP address Location Resource Resource ID Client app Operating system Device browser Correlation ID Conditional Access User type Cross tenant access type Home tenant ID Home tenant name Unique token identifier Resource tenant ID App owner tenant ID Resource owner tenant ID Sign-in identifier Session ID Autonomous system number IP address (seen by resource) Global Secure Access IP address Through Global Secure Access Microsoft Entra app authentication library Is CAE Token Flagged for review Token issuer name Token issuer type Incoming token type Authentication Protocol Client credential type

Save

Pre-Attack

[Hardening o365]

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

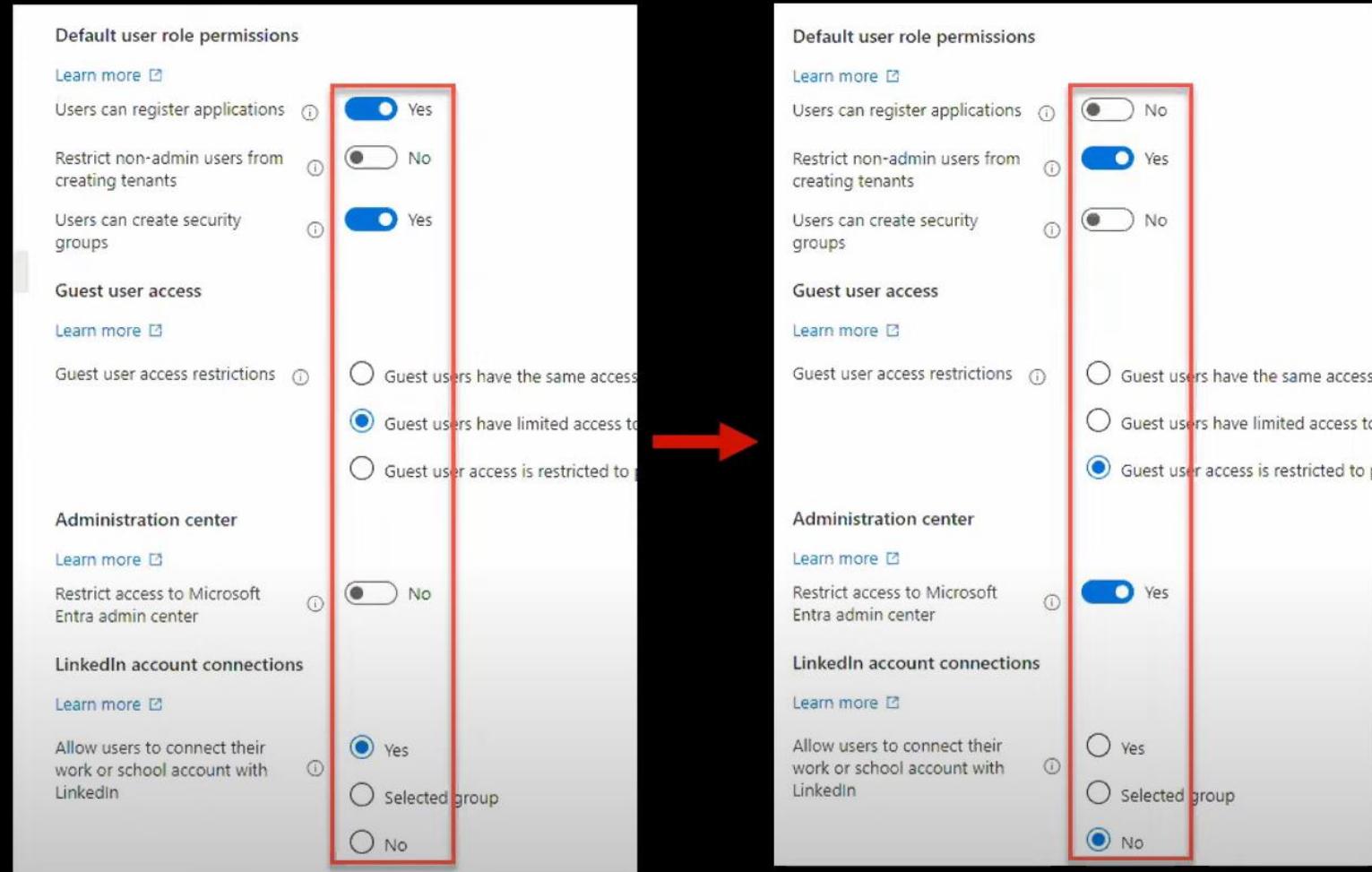
The screenshot shows the Microsoft Entra admin center interface. The left sidebar is titled "Microsoft Entra admin center" and includes sections for Home, What's new, Diagnose & solve problems, Favorites, Identity (Overview, Users, All users, Deleted users, User settings), Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection (Security Center, Identity Secure Score, Multifactor authentication), Troubleshooting + Support (New support request), and Authentication methods.

The main content area is titled "Security | Risky sign-ins" and shows a search bar, download, learn more, export data, configure trusted IPs, troubleshoot, and filter buttons. It also displays a message about a 30-day trial and a summary table with two selected items.

A modal window titled "Risk state" is open, listing five options: At risk, Confirmed compromised, Confirmed safe, Dismissed, and Remediated. The "At risk" option is checked. An "Apply" button at the bottom of the modal is highlighted with a green arrow.

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 😷
<i>Passwordless</i> with Push Notification + Code	NO 😷
FIDO2 Passkey – YubiKey hardware token	YES 😊
FIDO2 Passkey – Smartphone	YES 😊
<i>Passwordless</i> with FIDO2 Passkey – YubiKey	YES 😊
<i>Passwordless</i> 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]

✉ colorado.gov DMARC:

```
"v=DMARC1; p=none; fo=1;
rua=mailto:dmarc_rua@emaildefense.proof
point.com;
ruf=mailto:dmarc_ruf@emaildefense.proofp
oint.com"
```

ⓘ Neither p=quarantine or p=reject were found. Email Spoofing is Possible.

Send-MailMessage -SmtpServer <Recipient>

Extension: (MailFail) - MailFail — Mozilla Firefox

Mail Fail Sponsored by Black Hills Information Security

✉ colorado.gov MX:

No MX Record Found. This Domain can't Receive Emails.

✉ colorado.gov SPF:

```
"v=spf1 a ip4:165.127.10.50
ip4:165.127.240.12 ip4:165.127.240.13
ip4:216.128.251.155 ip4:64.78.237.245
ip4:52.175.224.30 ip4:206.16.212.235 "
"ip4:206.16.212.244 ip4:63.241.232.119
ip4:129.82.111.40 ip4:129.82.111.41
ip4:129.82.111.141 include:sendgrid.net
include:_spf.firebaseio.com ~all"
```

ⓘ Check if Any IPs Within the CIDR Ranges are SMTP Open Relays.

```
nmap -p 25,587,465 -v --open --script smtp
```

ⓘ The SPF Record Contains Multiple Pairs of Double Quotes, the Record MUST be Treated as if These Strings are Concatenated Together Without Adding Spaces. This Sometimes has Unintended Consequences.

No SPF Domains Available to Purchase. [sendgrid.net, firebaseemail.com]

MailFail: Who's Spoofing You?

(<https://www.youtube.com/watch?v=UbdMAsWus8>)



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]

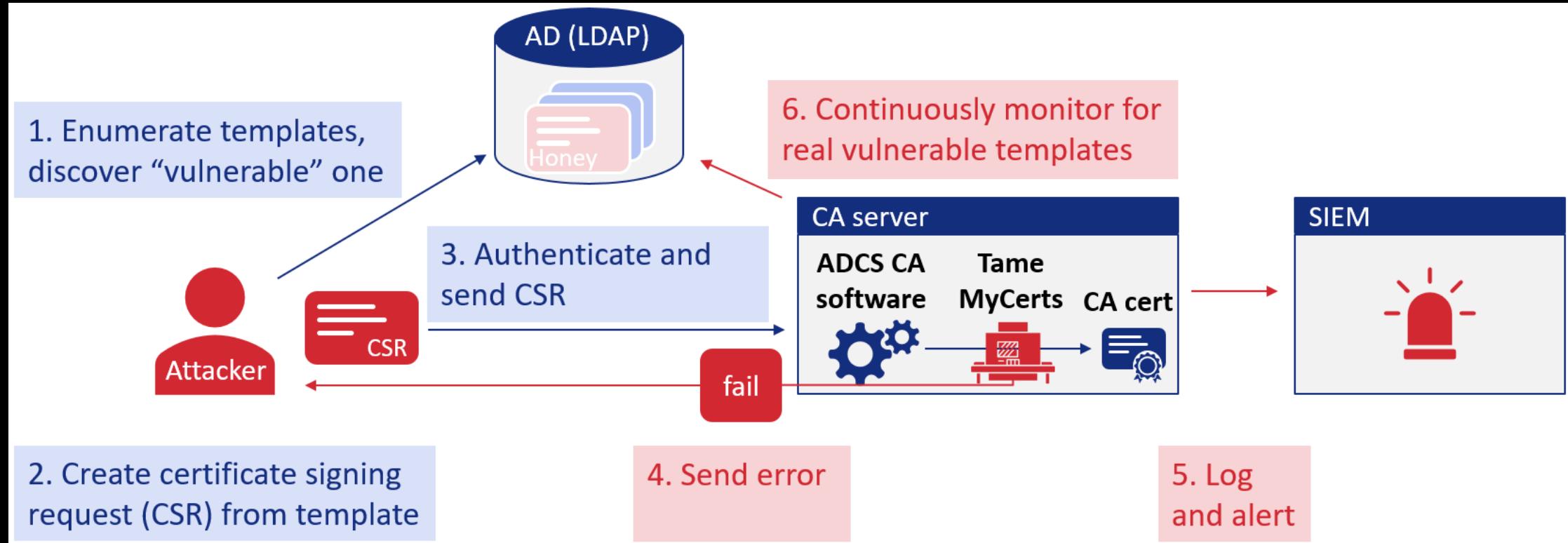
The screenshot shows the DejaVu web interface. At the top, there's a header with 'DejaVu | Engine' and a 'Health Monitor' status indicator. On the left, a sidebar includes a user icon ('Admin Online'), main navigation links ('Decoy Management', 'Manage Decoys', 'Add Server Decoy', 'Add Client Decoy', 'N/W and File Management', 'Breadcrumbs', 'Settings'), and a 'Decoy Name' search bar. The main content area is titled 'Decoy Management' and 'Manage Decoys'. It displays a table of decoy configurations:

Decoy Name	Network Location	Interface	Services	IP Address	Web Server Files
BEE-Services1	IT	eth1	FTP; TFTP; APACHE;	1.1.1.102	DEFAULTW0A.zip
BEE-Services2	IT	eth1	SMB; RDP - Noninteractive; SNMP;	1.1.1.103	
BEE-Services3	IT	eth1	MODBUS; S7COMM;	1.1.1.104	
BEE-Services4	IT	eth1	SSH - Interactive; VNC; TELNET;	1.1.1.105	
BEE-Services5	IT	eth1	MSSQL; MYSQL;	1.1.1.106	
BEE-Services6	IT	eth1	HONEYCOMB;	1.1.1.107	
BEE-WrkStn1	IT	eth2	NBNSCLIENT;	1.1.1.108	
BEE-WrkStn2	IT	eth2	ARPMITM;	1.1.1.109	

- 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=ICwmK00vHNC>

The screenshot shows the Canary Tokens website interface. At the top, there's a navigation bar with links for 'DOCUMENTATION' and 'THINKST CANARY'. The main heading is 'Create a Canarytoken. Deploy it somewhere.' with the tagline 'Know. When it matters.' Below this, there are several categories of tokens:

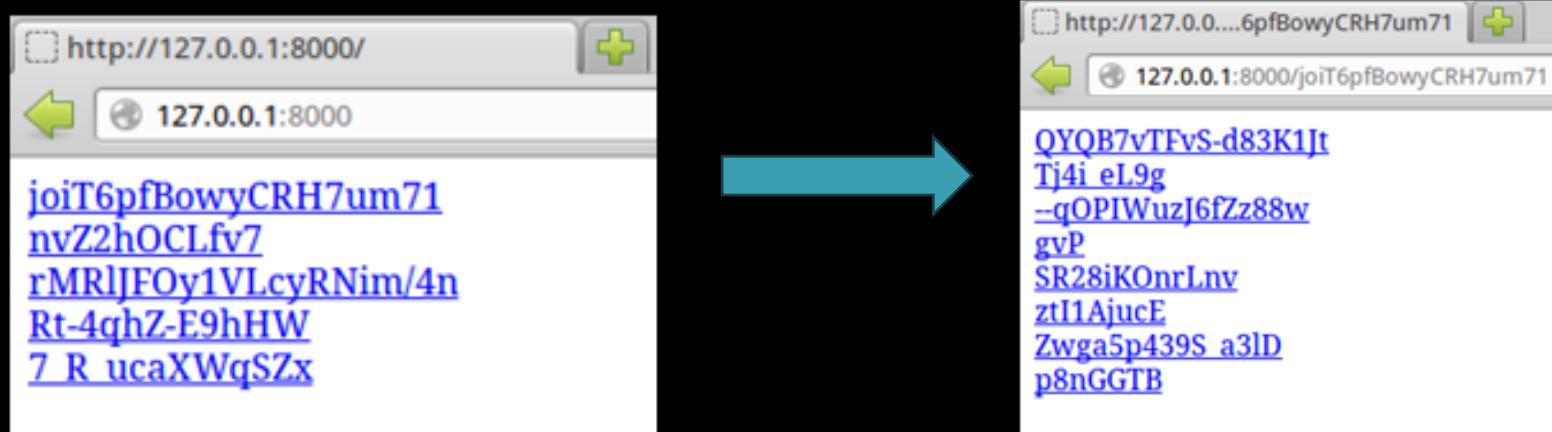
- All**: Web bug, DNS, Credit Card, QR code, MySQL, Create Canarytoken.
- Microsoft**: Fake App, Log4shell, Fast redirect.
- Phishing**: Get an alert when an attacker uses your Azure Service.
- Cloud**: Get an alert when an attacker attempts to use your credit card.
- Database**: Get an alert when an attacker follows your QR Code.
- Other**: Get an alert when an attacker loads your MySQL dump.

A search bar is located at the top right. On the right side, there's a large form titled 'Create Windows Fake File System Token' with fields for 'Canarytoken Settings' (directory: C:\Secrets), 'Create (fake) files for the following Industry/Sector' (choose industry), 'Mail me here when the alert fires' (email: your-email@email.com), and 'Remind me of this when the alert fires' (note: E.g: Fake file system token on off-site backup server). A 'Create Canarytoken' button is at the bottom right of the form.

Pre-Attack

[Spider Trap]

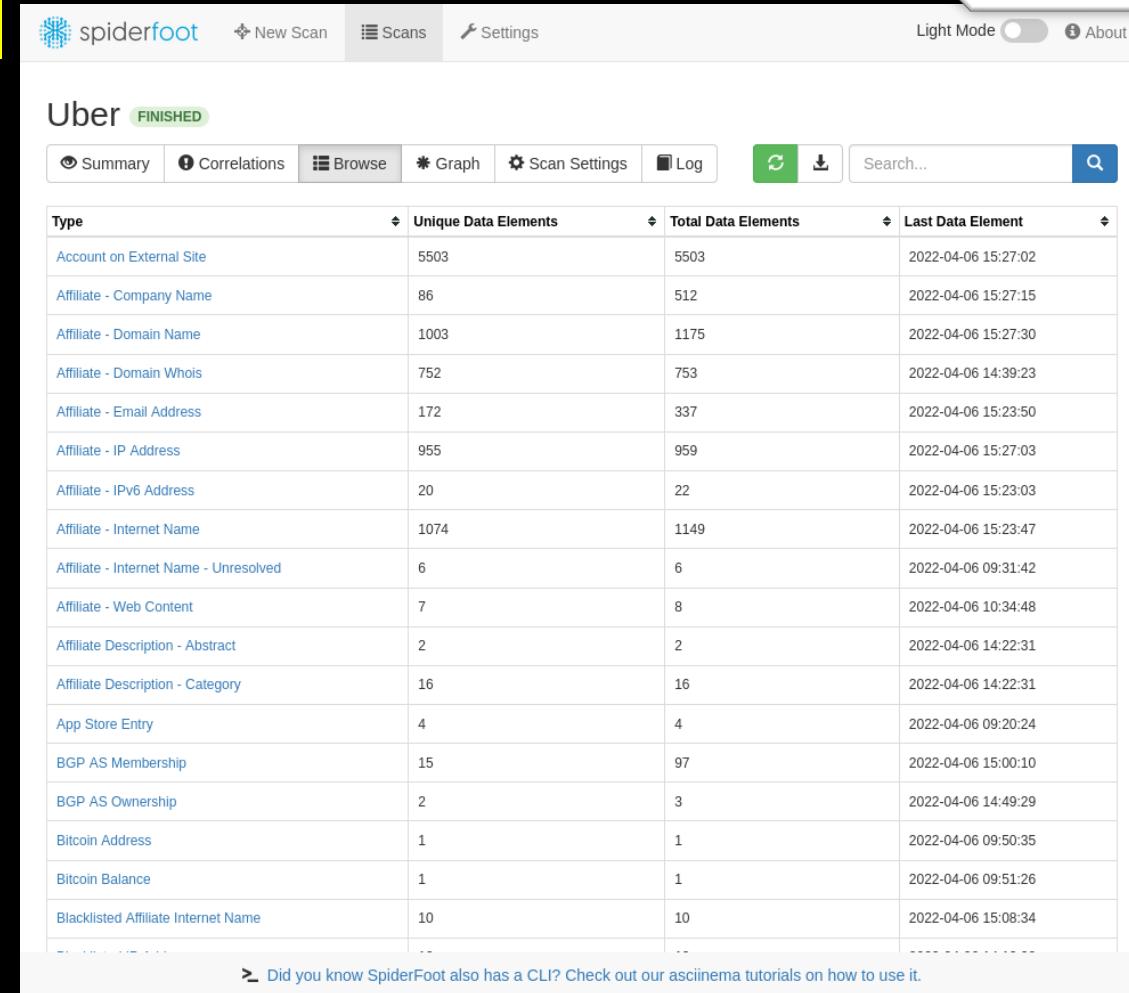
```
/opt/spidertrap$ python3 spidertrap.py directory-list-2.3-big.txt
```



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

Pre-Attack

[OSINT]



The screenshot shows the Spiderfoot OSINT tool interface. At the top, there's a navigation bar with 'New Scan', 'Scans', 'Settings', 'Light Mode' (switched off), and 'About'. Below the navigation is a search bar with placeholder 'Search...'. The main area displays a table titled 'Uber FINISHED'. The table has columns for 'Type', 'Unique Data Elements', 'Total Data Elements', and 'Last Data Element'. The data includes various types of information such as 'Account on External Site', 'Affiliate - Company Name', 'Affiliate - Domain Name', etc., with their respective counts and last update times.

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



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



Pre-Attack

[Red Teaming]

“Win” Red Team Exercises

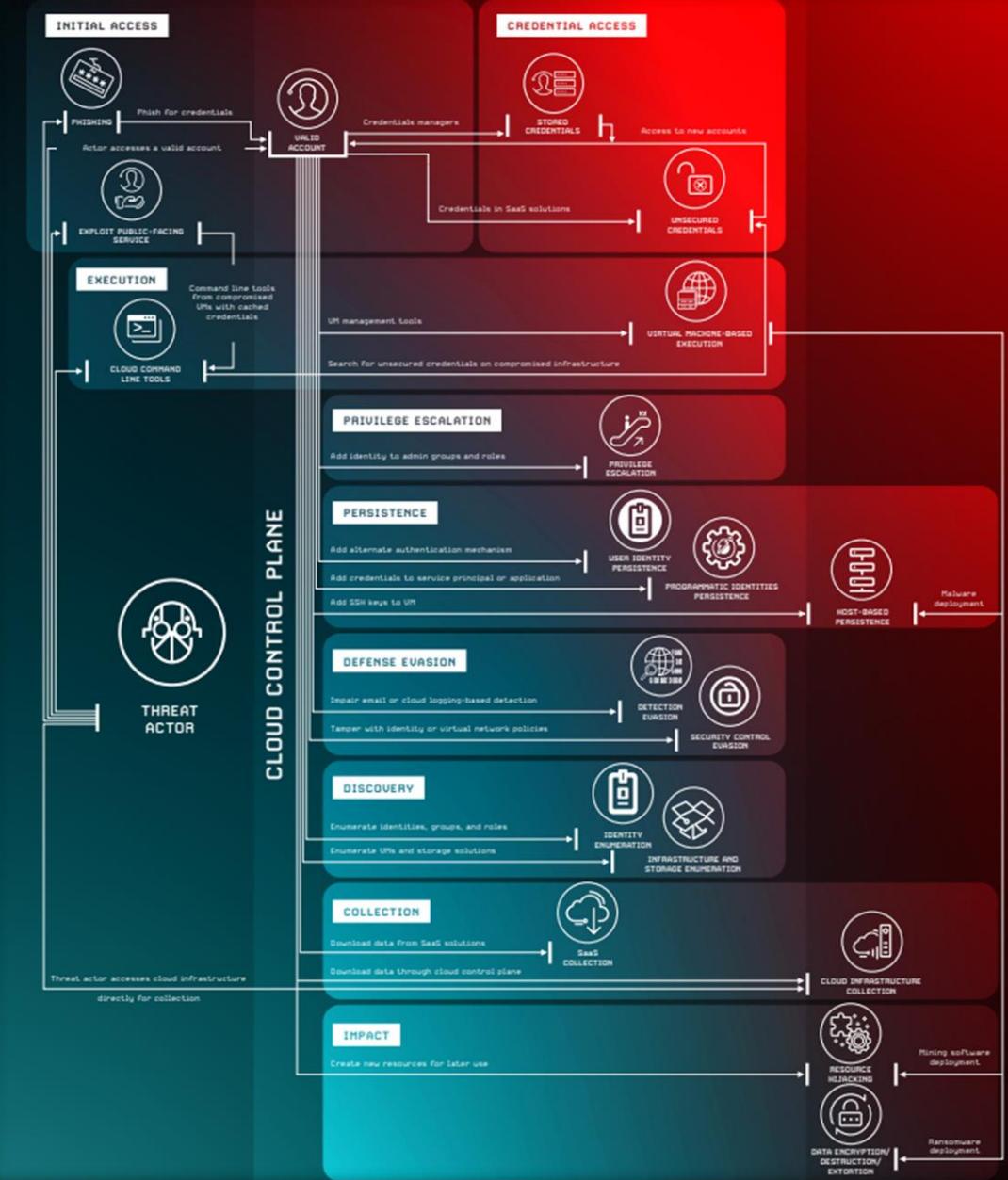
Even when defenses fail, the real winners of red team exercises are the companies that use them to boost their security posture.

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>)



Order	Technique	TestName	auto_generated_guid	supported_platforms	ieoutSeco
1	T1105	Download a file using wscript	16a3f-efac-4b26-8336-b9cb18c45	windows	120
2	T1033	System Owner/User Discovery	59bf-addf-4b4a-be86-8d09cc18	windows	120
3	T1033	System Discovery - SocGholish whoami	7a03-eb80-41c5-b744-bb37ac7f	windows	120
4	T1482	Windows - Discover domain trusts with nltest	641d-0498-48d2-b9ff-c71e496cc	windows	120
5	T1218.011	Rundll32 with Ordinal Value	a74b-ba89-482a-8a3e-a5fea36	windows	120
6	T1055.012	Process Hollowing using PowerShell	b27b4-39ef-4e8c-af88-463a78e7l	windows	120
7	T1069.002	Basic Permission Groups Discovery Windows (Domain)	id77d-8998-48c0-8024-df263dc2	windows	120
8	T1087.002	Wvtutil - Discover NTLM Users Remote	63d4-a836-4993-a74e-0a19b848	windows	120
9					
10					
<hr/>					
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 PowerShell C:\WINDOWS\system32\cmd.exe /c start notepad					
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 Git "powershell.exe" & {[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12} powershell -ep bypass					
stateful-rules Multiple Net Reconnaissance C:\Windows\cmd\user /domain					
stateful-rules Multiple Reconnaissance 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					

TECHNIQUES

Enterprise

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access

ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may use elevation control mechanisms to gain elevated privileges. These mechanisms are intended to be used by an adversary to gain elevated privileges in order to escalate their access.

Enterprise Techniques

Techniques represent 'how' an adversary achieves a tactical objective. For example, an adversary may dump credentials to achieve credential access.

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

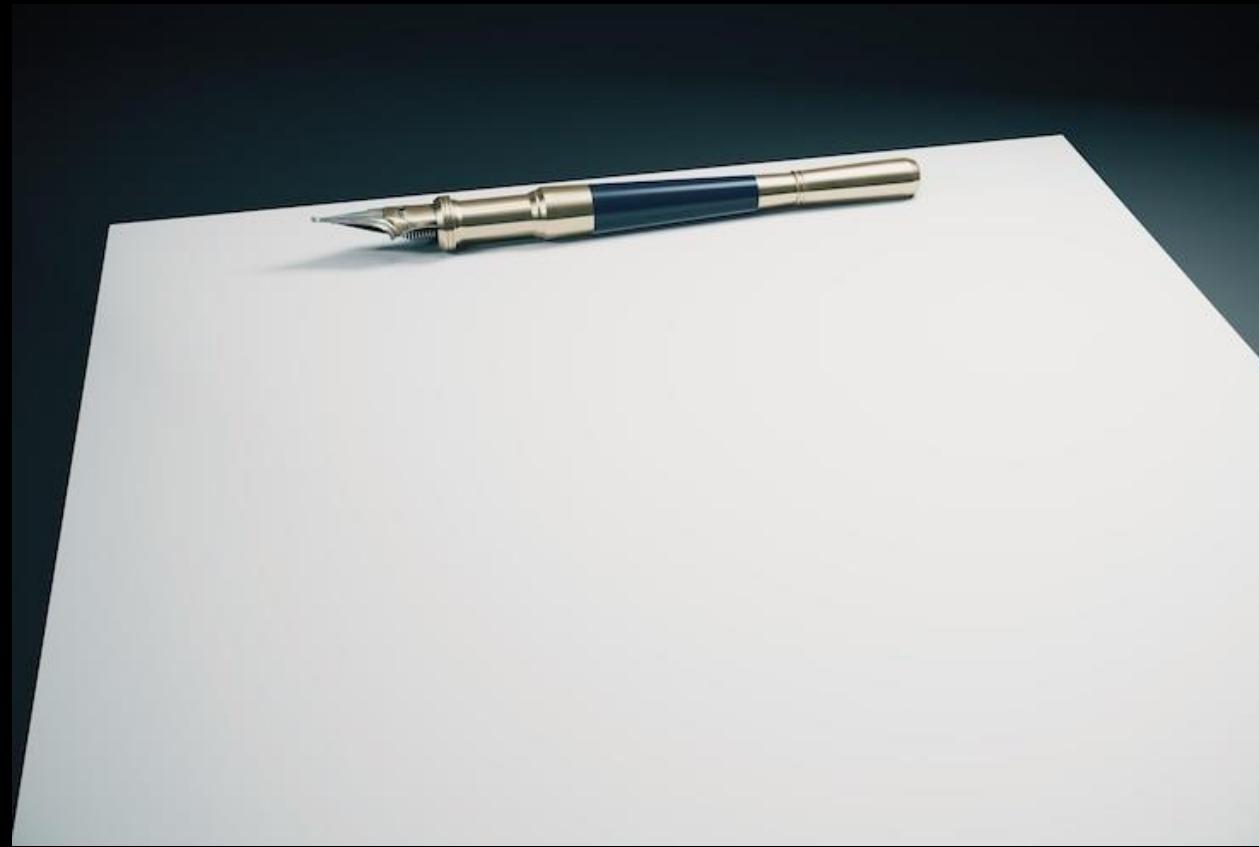
Browser Analysis

Real Time Domain
Reconnaissance

Real Time Host
Reconnaissance

Real Time
Network
Reconnaissance

During the Battle



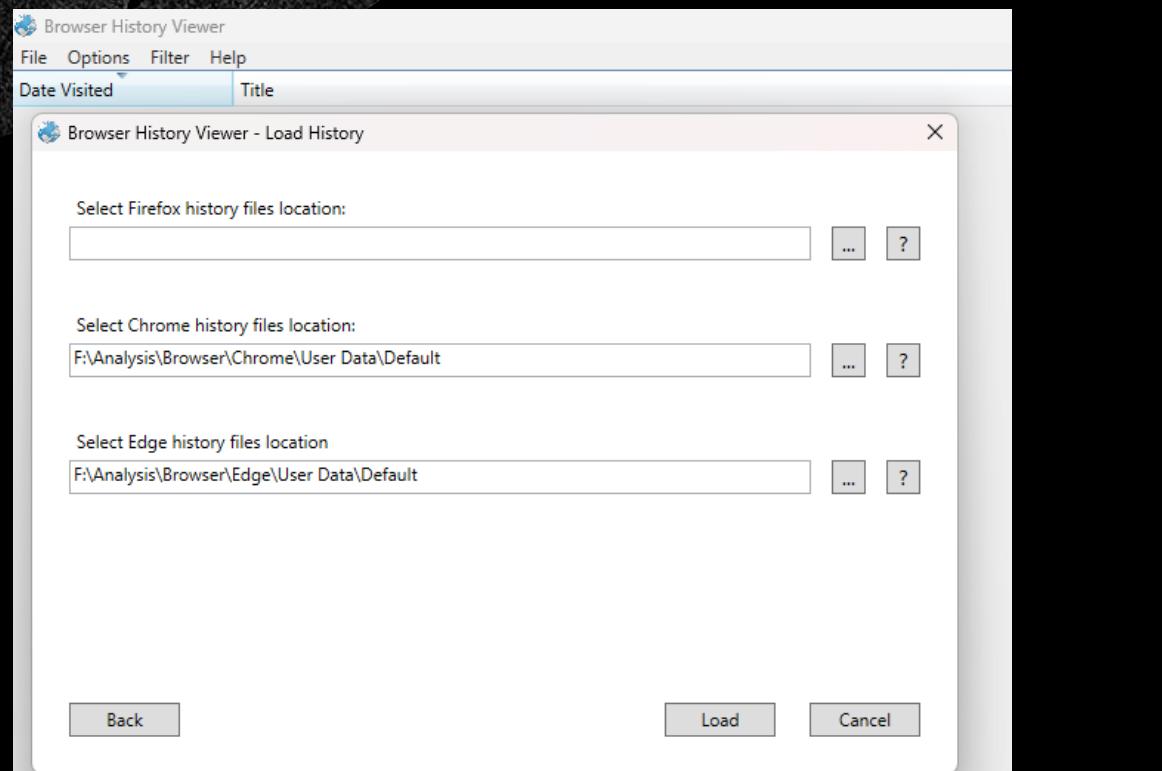
During the Battle

[Browser Analysis]

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



Date Visited	Title	URL	V	C	W
02/05/2025 07:50:39			31	55	Ch
02/05/2025 07:44:49			11	15	Ed
02/05/2025 07:44:30			1	2	Ed
02/05/2025 07:40:23	Support_Helpdesk	https://qcecerd.z10.web.core.windows.net/wwwbinf01USAHTML/?bcd=1-877-671-6313#	1	2	Ed
02/05/2025 07:29:11	Support_Helpdesk	https://qcecerd.z10.web.core.windows.net/wwwbinf01USAHTML/?bcd=1-877-671-6313	1	2	Ed
02/05/2025 07:29:04	Support_Helpdesk	https://qcecerd.z10.web.core.windows.net/wwwbinf01USAHTML/?bcd=1-877-671-6313	1	1	Ed
02/05/2025 07:29:03	Support_Helpdesk	https://qcecerd.z10.web.core.windows.net/?bcd=1-877-671-6313	1	1	Ed
02/05/2025 07:28:59	An Unusual Discovery In Antarctica's	https://yolonevs.net/an-unusual-discovery-in-antarctica-deep-ice-changes-everything-we-knew-about-history/?utm_source=taboola&utm_term=msn-msn&utm_medium=cpc&utm_campaign=yLUS.D_TOF+-Antarctica&cost=0.18&tbcli=GJDIDmAVyRizh695yq7MADl6kHG0C1o	1	1	Ed
02/05/2025 07:28:59	An Unusual Discovery In Antarctica's	https://api.taboola.com/2.0/json/msn-msn/recommendations_notify-click/app_type:bidder&app.apkey:6962914382/c91b118c/cddc97a4e50059face98/response_id:ba59ba8df5954727141650d18c4b...db9c27badff469d97a8123ba1ed011&response_session=v2_3dc5c50n1	1	1	Ed
02/05/2025 07:27:12	www.msn.com	https://www.msn.com/en-us/news/world/russia-ukraine-war-frontline-update-as-of-april-27/ar-AA1DIMKFcoid=ennewsntp&pc=DCTS&cvid=d7dad911a74a738a1eb6c152a51860&ei=20	11	12	Ed
02/05/2025 07:27:06			41	42	Ed
02/05/2025 07:27:05			41	42	Ed
02/05/2025 07:27:05			16	16	Ed
02/05/2025 07:27:05			16	16	Ed
02/05/2025 07:27:05			16	16	Ed
02/05/2025 07:27:05			15	18	Ed
02/05/2025 07:27:01			42	42	Ed
02/05/2025 07:27:01			1	1	Ed
02/05/2025 07:26:37			1	1	Ed
02/05/2025 07:26:36			15	18	Ed
02/05/2025 07:12:53			1	2	Ed
02/05/2025 07:08:49			2	2	Ed
02/05/2025 07:08:49			11	15	Ed
02/05/2025 07:08:48			2	2	Ed
02/05/2025 07:08:42			11	15	Ed
02/05/2025 07:08:04			1	1	Ch
02/05/2025 07:06:48			32	34	Ch
02/05/2025 07:06:48			86	86	Ch



During the Battle

[Meerkat]

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
2_20250403-070858Z_ARP.csv	Microsoft Excel Comma S...	1 KB	No	3 KB	81%	4/3/2025 1:08 PM
2_20250403-070858Z_AuditPolicy.csv	Microsoft Excel Comma S...	1 KB	No	7 KB	86%	4/3/2025 1:09 PM
2_20250403-070858Z_Autoruns.csv	Microsoft Excel Comma S...	1 KB	No	4 KB	74%	4/3/2025 1:08 PM
2_20250403-070858Z_BitLocker.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	38%	4/3/2025 1:09 PM
2_20250403-070858Z_ComputerDetails.csv	Microsoft Excel Comma S...	1 KB	No	3 KB	55%	4/3/2025 1:09 PM
2_20250403-070858Z_Connections.csv	Microsoft Excel Comma S...	3 KB	No	27 KB	92%	4/3/2025 1:10 PM
2_20250403-070858Z_Disks.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	18%	4/3/2025 1:09 PM
2_20250403-070858Z_DLLs.csv	Microsoft Excel Comma S...	3 KB	No	41 KB	94%	4/3/2025 1:10 PM
2_20250403-070858Z_DNS.csv	Microsoft Excel Comma S...	4 KB	No	35 KB	90%	4/3/2025 1:09 PM
2_20250403-070858Z_Drivers.csv	Microsoft Excel Comma S...	8 KB	No	55 KB	87%	4/3/2025 1:09 PM
2_20250403-070858Z_EnvVars.csv	Microsoft Excel Comma S...	1 KB	No	7 KB	87%	4/3/2025 1:09 PM
2_20250403-070858Z_EventsLoginFailures.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
2_20250403-070858Z_Hosts.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
2_20250403-070858Z_Hotfixes.csv	Microsoft Excel Comma S...	4 KB	No	100 KB	97%	4/3/2025 1:09 PM
2_20250403-070858Z_LocalGroups.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
2_20250403-070858Z_LocalUsers.csv	Microsoft Excel Comma S...	1 KB	No	4 KB	80%	4/3/2025 1:09 PM
2_20250403-070858Z_NetAdapters.csv	Microsoft Excel Comma S...	1 KB	No	2 KB	53%	4/3/2025 1:10 PM
2_20250403-070858Z_NetRoutes.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	74%	4/3/2025 1:10 PM
2_20250403-070858Z_Proceses.csv	Microsoft Excel Comma S...	27 KB	No	226 KB	89%	4/3/2025 1:10 PM
2_20250403-070858Z_RecycleBin.csv	Microsoft Excel Comma S...	2 KB	No	15 KB	90%	4/3/2025 1:10 PM
2_20250403-070858Z_Registry.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:10 PM
2_20250403-070858Z_RegistryMRU.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
2_20250403-070858Z_RegistryPersistence.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:09 PM
2_20250403-070858Z_ScheduledTasks.csv	Microsoft Excel Comma S...	15 KB	No	90 KB	84%	4/3/2025 1:10 PM
2_20250403-070858Z_Services.csv	Microsoft Excel Comma S...	26 KB	No	139 KB	82%	4/3/2025 1:10 PM
2_20250403-070858Z_Sessions.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	31%	4/3/2025 1:10 PM
2_20250403-070858Z_Shares.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	44%	4/3/2025 1:10 PM
2_20250403-070858Z_Software.csv	Microsoft Excel Comma S...	4 KB	No	12 KB	71%	4/3/2025 1:10 PM
2_20250403-070858Z TPM.csv	Microsoft Excel Comma S...	1 KB	No	1 KB	56%	4/3/2025 1:10 PM
2_20250403-070858Z_USBHistory.csv	Microsoft Excel Comma S...	0 KB	No	0 KB	0%	4/3/2025 1:10 PM
J2_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>)



```
Administrator: Command Prompt

C:\Users\Admin\Desktop>.\BLUESPAWN-client-x64.exe --mitigate --action=audit

| [B] | [L] | [U] | [E] | [S] | [P] | [A] | [W] | [N] |
| / \ | / \ | / \ | / \ | / \ | / \ | / \ | / \ | / \ | / \ |

[*][LOW] Auditing Mitigations
[INFO] Checking for presence of M1025 - Privileged Process Integrity
[WARNING] M1025 - Privileged Process Integrity is NOT configured.
[*][LOW] M1025 - Privileged Process Integrity is NOT configured.
[INFO] Checking for presence of M1028-WFW - Windows Firewall must be enabled with no exceptions
[WARNING] M1028-WFW - Windows Firewall must be enabled with no exceptions is NOT configured.
[*][LOW] M1028-WFW - Windows Firewall must be enabled with no exceptions is NOT configured.
[INFO] Checking for presence of M1035-RDP - Limit Access to Resource over Network
[INFO] M1035-RDP - Limit Access to Resource over Network is enabled.
[*][LOW] M1035-RDP - Limit Access to Resource over Network is enabled.
[INFO] Checking for presence of M1042-LLMNR - Link-Local Multicast Name Resolution (LLMNR) should be disabled
[WARNING] M1042-LLMNR - Link-Local Multicast Name Resolution (LLMNR) should be disabled is NOT configured.
[*][LOW] M1042-LLMNR - Link-Local Multicast Name Resolution (LLMNR) should be disabled is NOT configured.
[INFO] Checking for presence of M1042-NBT - NetBIOS Name Service (NBT-NS) should be disabled
[WARNING] M1042-NBT - NetBIOS Name Service (NBT-NS) should be disabled is NOT configured.
[*][LOW] M1042-NBT - NetBIOS Name Service (NBT-NS) should be disabled is NOT configured.
[INFO] Checking for presence of M1042-WSH - Windows Script Host (WSH) should be disabled
[WARNING] M1042-WSH - Windows Script Host (WSH) should be disabled is NOT configured.
[*][LOW] M1042-WSH - Windows Script Host (WSH) should be disabled is NOT configured.

[FINISHED] Mitigation Audit is NOT configured
```

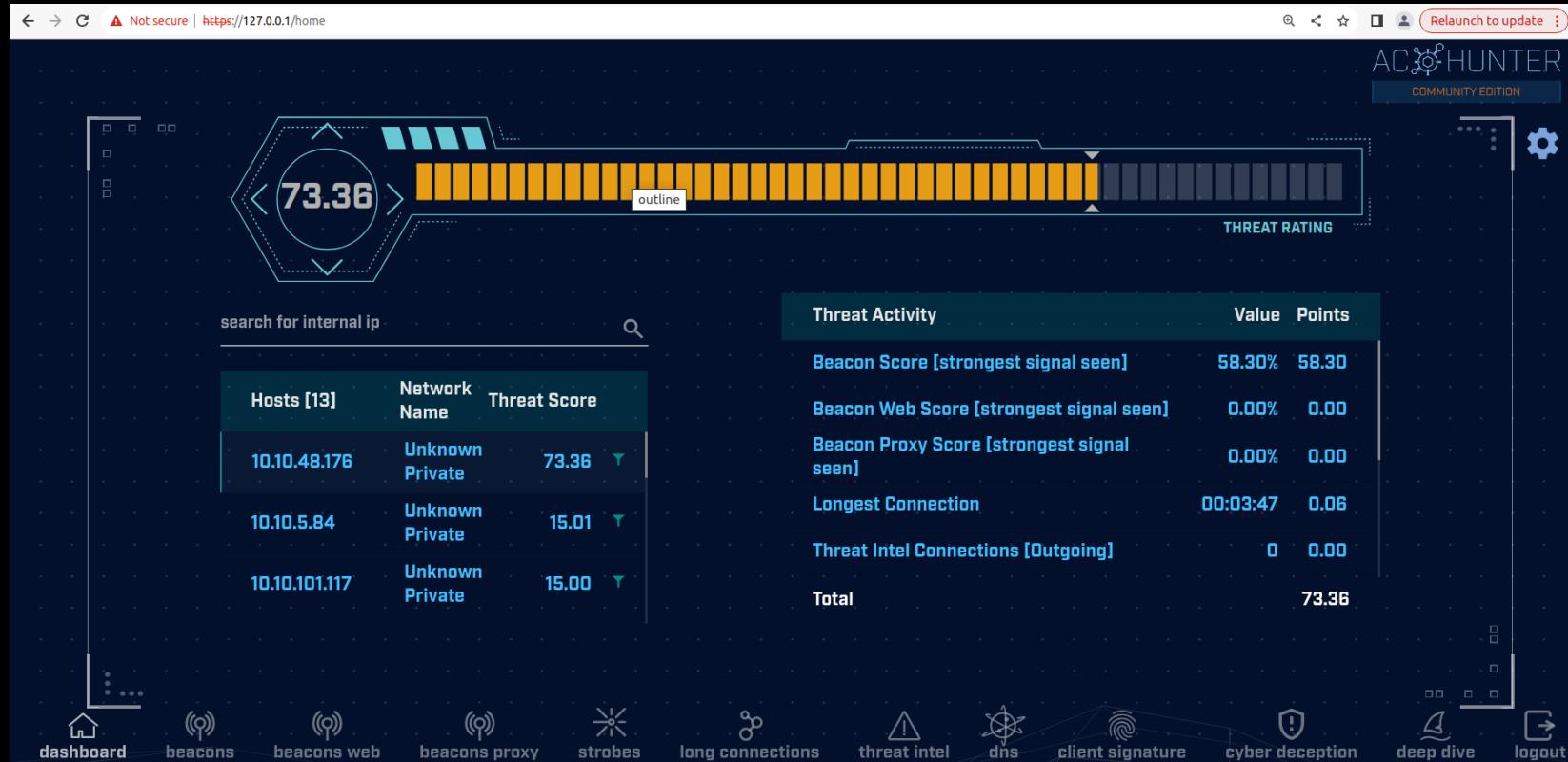
```
.\BLUESPAWN-client-x64.exe --mitigate --action=audit  
.\BLUESPAWN-client-x64.exe --hunt -a Cursory --log=console,xml
```

During the Battle

[Host Reconnaissance]

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

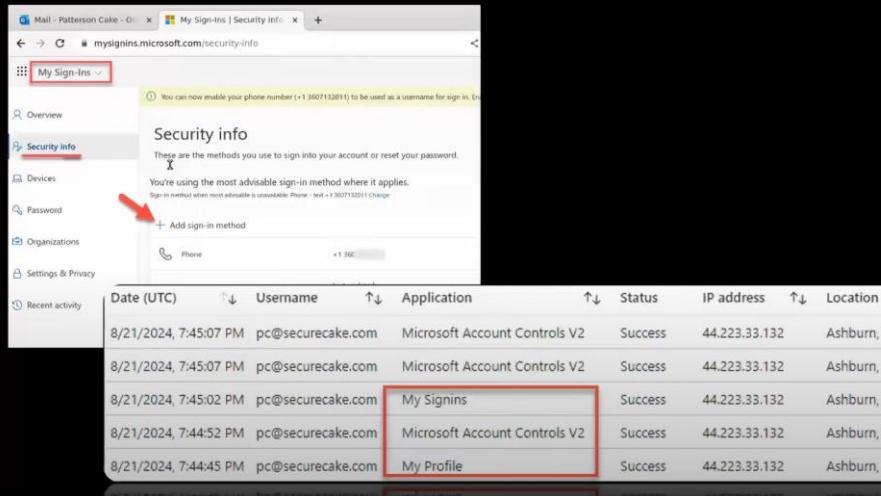
Post-Attack
[Phishing Cleanup]

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



The screenshot shows the Microsoft 365 Security Info page under the 'My Sign-ins' tab. It displays a table of sign-in logs. A red arrow points to the '+ Add sign-in method' button. The table rows are highlighted with red boxes:

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

M365 BEC Investigation

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

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

- Phishing Past MFA

Post-Attack

[Roast Hunting]

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

INVADING THE REALM:

THREE VITAL KERBEROS ATTACK TYPES



Roasting Attacks

AS-REQ Roasting & Kerberoasting crack and steal user passwords.



Delegation Attacks

Impersonate a user to access another resource.



Ticket Abuse

Steal Ticket Granting Tickets (TGTs) or Ticket Granting Services (TGS') from a particular user.

How to defend:

Don't set users with Kerberos pre-authentication disabled, and protect accounts with strong passwords.

How to defend:

Disable unconstrained delegation and place users into the Protected Users Group where possible.

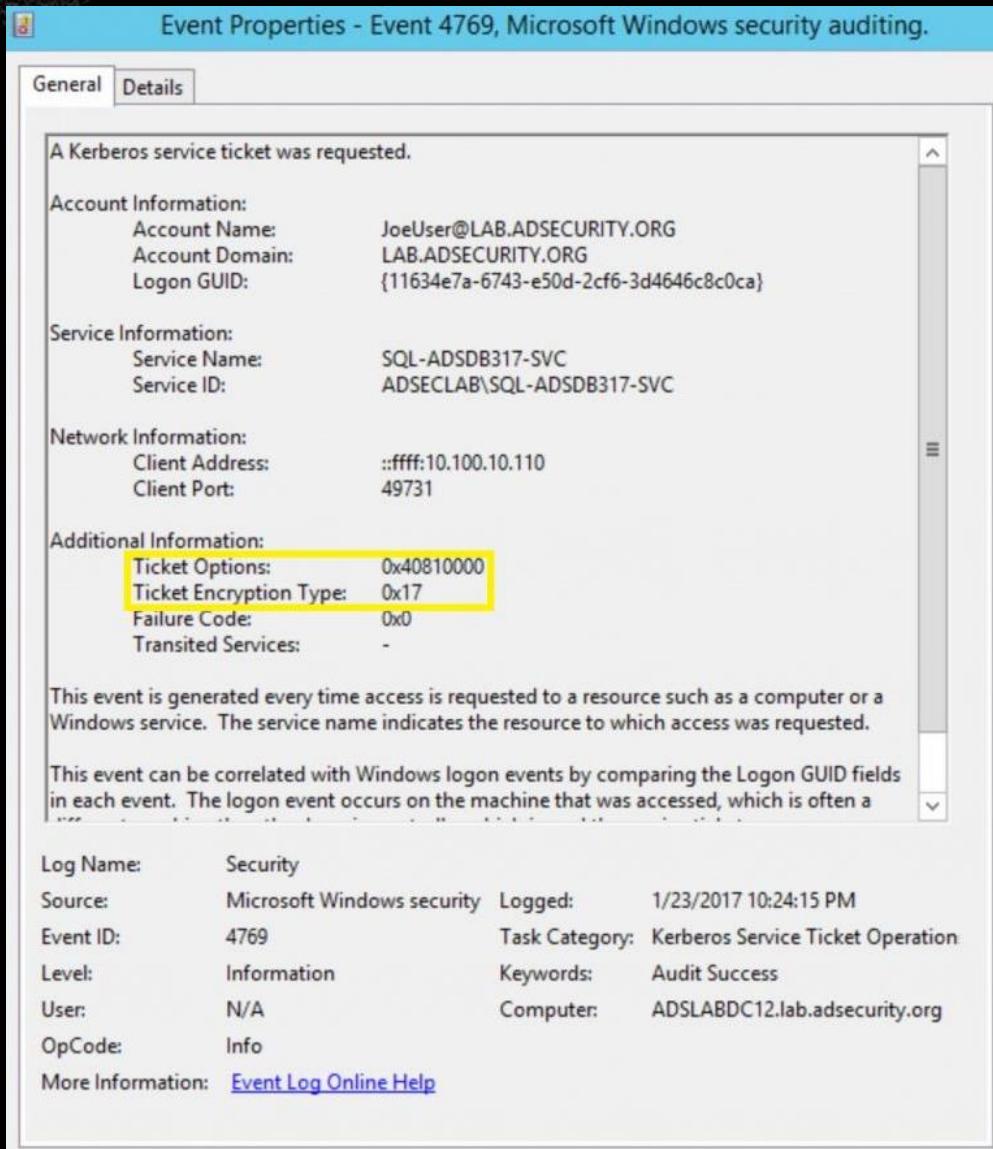
How to defend:

Limit the number of admin accounts and utilize Multi-factor authentication.

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?

