



# Breaching a Bank: Mission Impossible Style

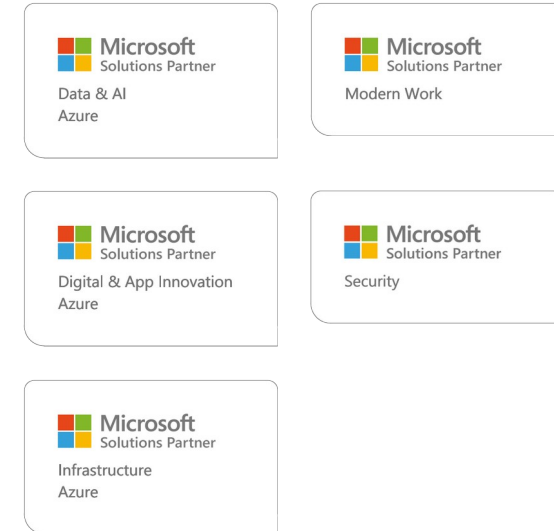
Certified  
  
Corporation

 zenzero

# Agenda

- ❑ Introduction
- ❑ The Red Team Infrastructure
- ❑ Initial Access
- ❑ Privilege escalation & Domain Compromise
- ❑ Key Takeaways for blue teams
- ❑ Q&A

# Introduction Zenzero



# Introduction – Red Team

-># whoami

Ridhwan Roshan (Rid) – Senior Red Team Consultant

- 4 Years of experience in Offensive Security
- Adversary Simulation, Malware Dev, Pentesting
- OSCP, CRT0, CREST CRT

-># nslookup RedTeam.zenzero.org.uk

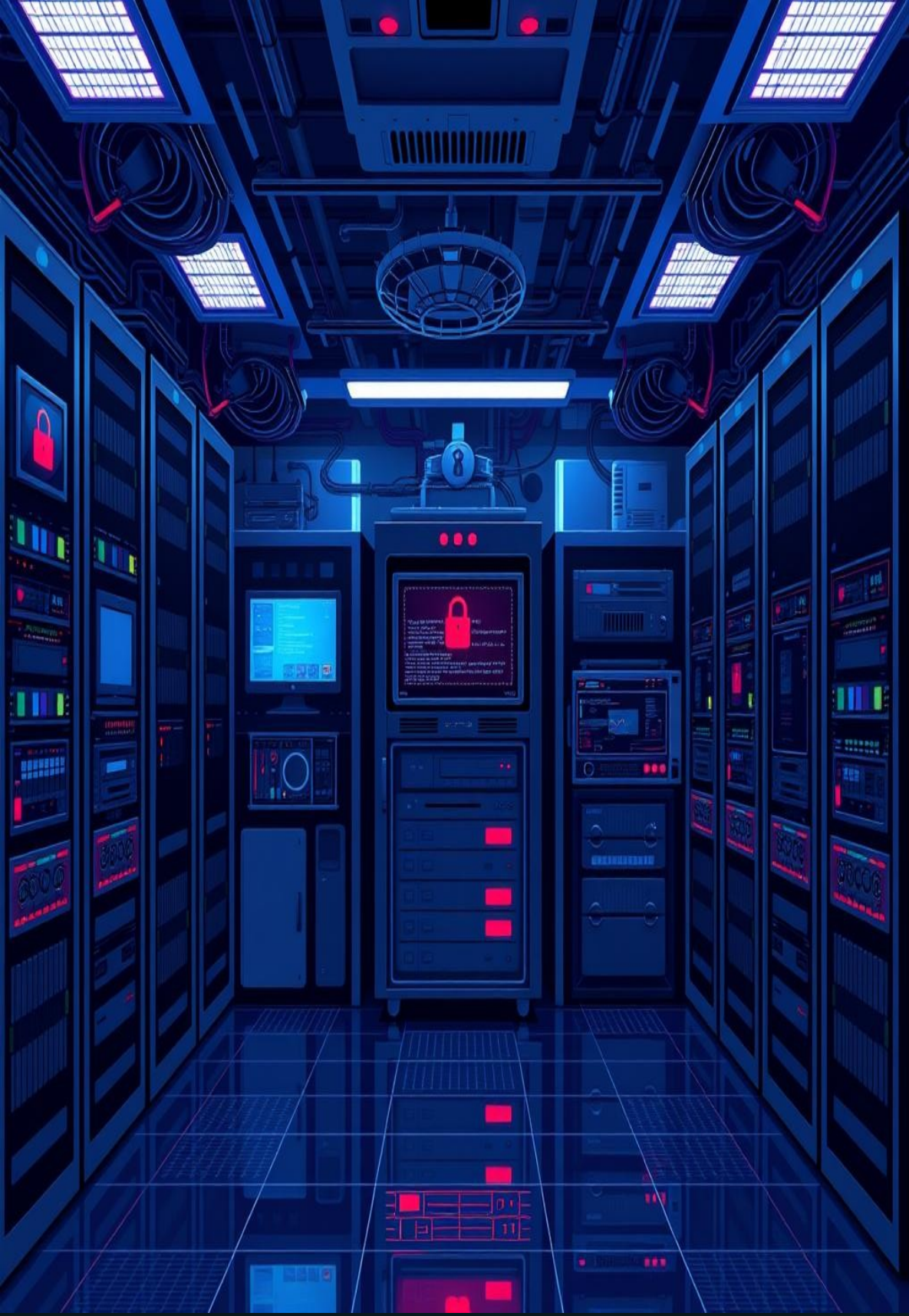
Zia Rehaman (Z) – Head of Red Team

- 20 year of experience in offensive security Operations
- Maintained various CHECK & CREST certifications
- CREST Assessor & CREST Fellowship

Abdul Ikbal (Abs) – Head of Cyber

- 13 years of Experience in pentesting
- Physical & Social Engineering Specialist
- Lead MAS, Held CREST Certifications





# Red Team Infrastructure

- ❑ Command & Control
  - ❑ 2 x C2's with one redirector each
  - ❑ Hosted in AWS and GCP
  - ❑ Legitimate Domains and SSL Certs installed
  
- ❑ The Phishing Servers
  - ❑ 1 x GoPhish server with modifications Made to avoid signatures
  - ❑ IP Rotation Via Mailgun
  - ❑ 15 + Domains purchased
  - ❑ acmehub.com, acmesign.com, acmeconnect.com,

# Phase 1 : Mission Briefing

Target Bank: Acme Bank

Assets: \$20 Billion USD

Operations: Global

Employees: 4,000 +

Headquarters: United Kingdom

Assessment Duration: 80 days

## Objective

Breach the External Perimeter and Gain access to the Internal Systems



# Reconnaissance

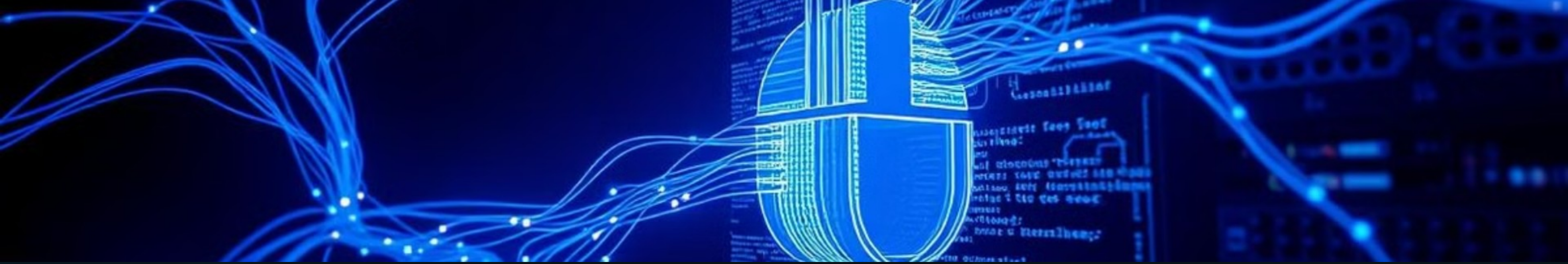
## OSINT:

- Shodan, Censys to identify exposed systems.
- LinkedIn, hunter.io, Intelx.io – to identify usernames, email etc

## Attack Surface Enumeration:

- Key External assets identified
- Network perimeter enumerated

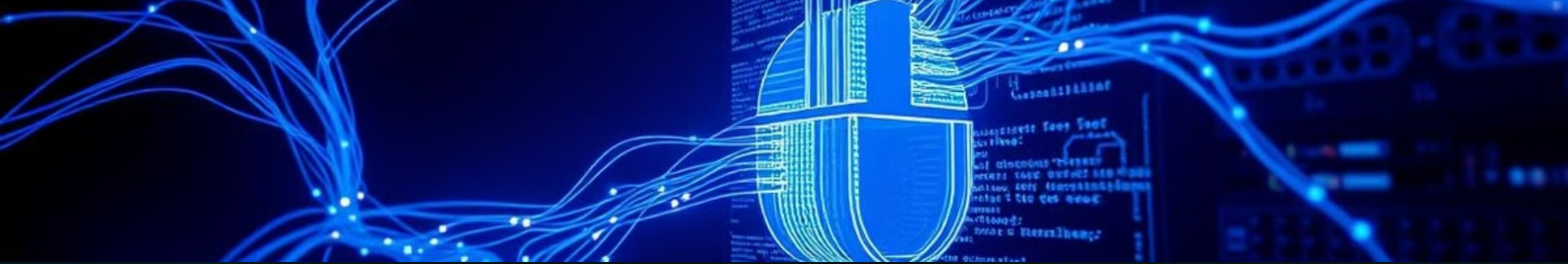




# Failed Tactics, Techniques and Procedures

The Following phishing IOCs failed:

Activity	IOCs	Results
Link based campaign – 50 recipient's	<a href="http://www.acmehub.com">www.acmehub.com</a> <a href="mailto:updates@acmehub.com">updates@acmehub.com</a>	5 clicks, no credential submissions Blocked by Defender for Cloud URL Detonation
Link based campaign – 24 recipient's	<a href="http://sso.acmehub.com">sso.acmehub.com</a> <a href="mailto:info@acmehub.com">info@acmehub.com</a>	0 opens - Blocked by Defender for Cloud URL Detonation
Link based campaign – 91 recipient's	<a href="http://acmedocusign.com">acmedocusign.com</a> <a href="mailto:notifications@acmedocusign.com">notifications@acmedocusign.com</a>	0 opens - Blocked by Defender for Cloud URL Detonation
Link based campaign – 12 recipient's	<a href="http://acmesign.com">acmesign.com</a> <a href="mailto:dse_na3@acmesign.com">dse_na3@acmesign.com</a>	Blocked by Defender for Cloud URL Detonation

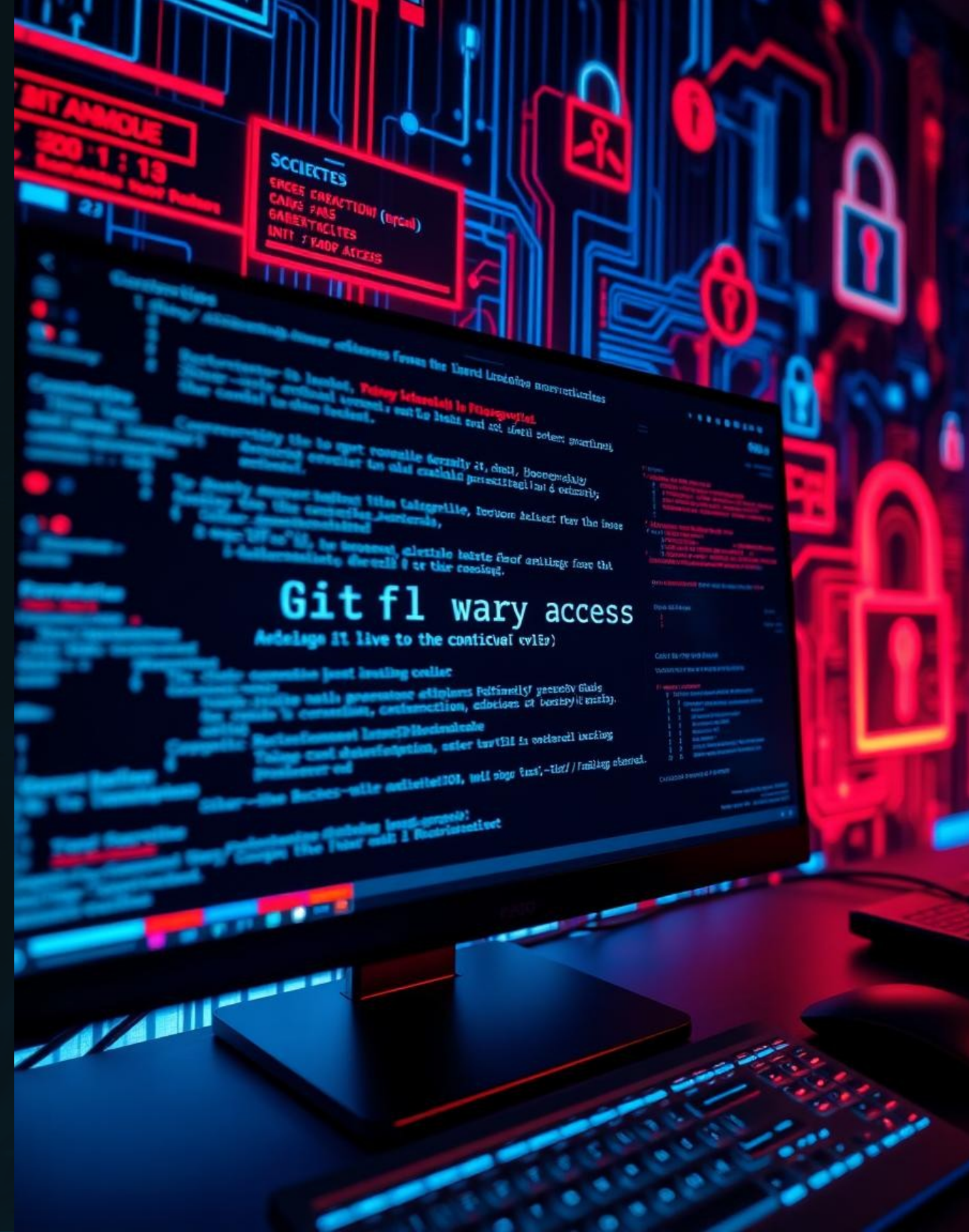
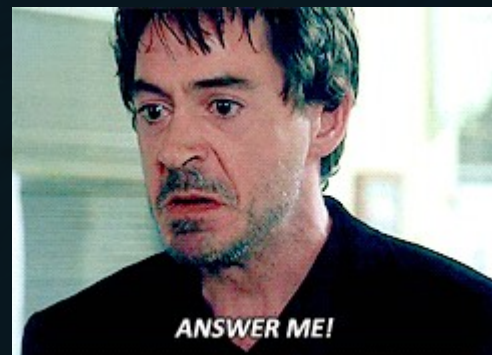


# Improvising the Approach

- Shifting from link based to phone number-based phishing
- A skype numbers was procured matching as much numbers and sequence as possible to original helpdesk
- An email with a fake helpdesk number was sent to 88 recipients

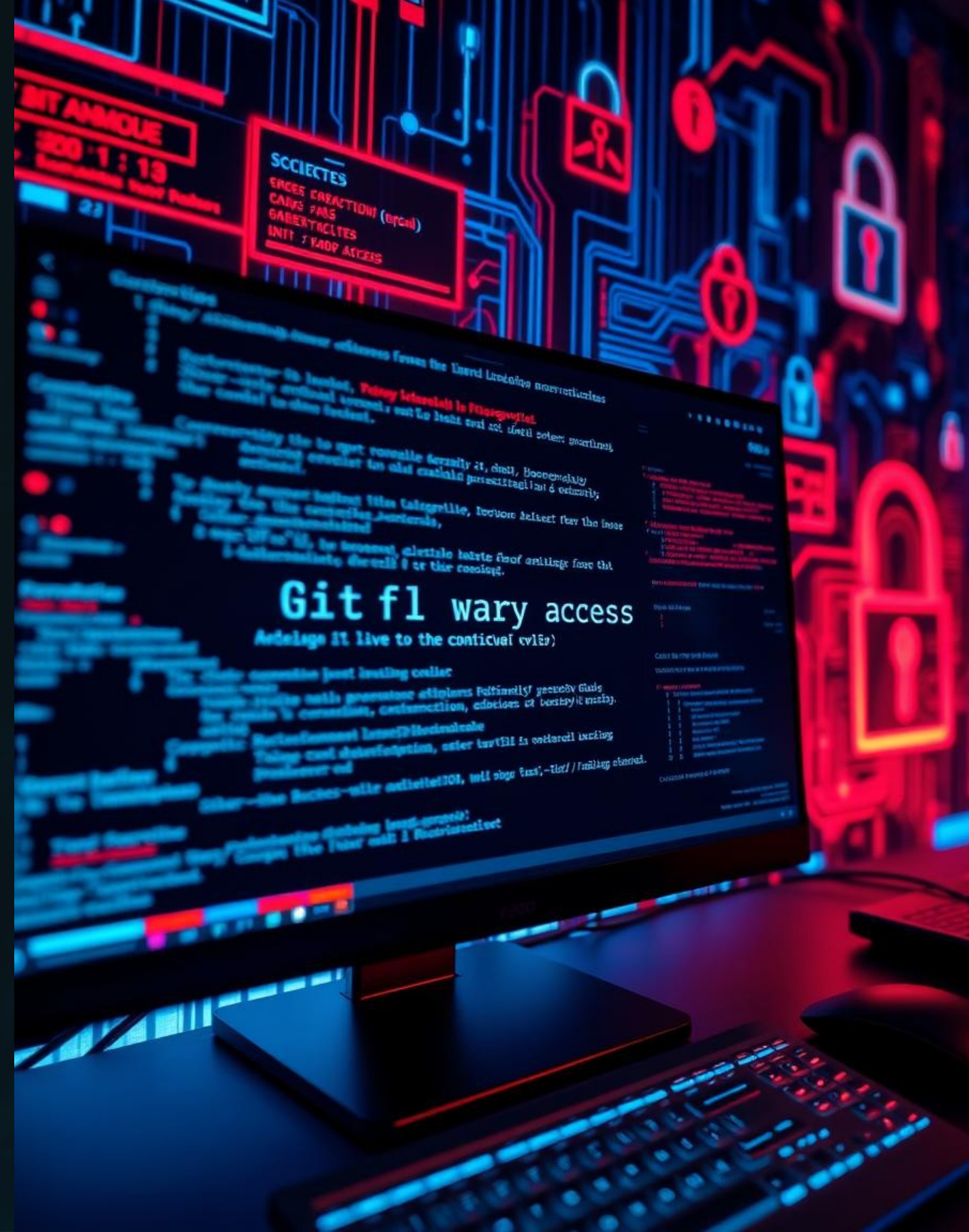
# Gaining Initial access – Failed

- A user called John, called the fake helpdesk numbers
- Incoming Call #1 from John:
  - Malicious URL delivered verbally
  - M365 Credentials failed to capture
- Outgoing Call #2 to John:
  - Malicious URL delivered verbally again
  - URL blocked when browsed from Acme
- Outgoing Call #3 to John:
  - No Response
  - Thinking this is the END!



# M365 Access & Bypassing MFA

- John called back, probably was making himself a sandwich
- Incoming Call #4 from john:
  - Requested to access the link via Mobile Device
  - M365 Credentials were captured
  - M365 Authenticator code requested verbally and provided
  - RSA Pin code requested verbally and provided
  - Zenzero's Authenticator app added to 365
- Finally, Access to M365.



# M365 Enumeration



- Access to departmental SharePoint slides, Technical Documents
- Software and Hardware data
- Excel files containing Credentials
- VPN User guides
- 14,000 usernames from azure
- John's personal & travel Detail's



# Problems! Problems! Problems!

- John was a workaholic! Never logouts!
- Needed RSA Token code
- Email IT Helpdesk for a new RSA
- Recon Call #1 to the Bank's Helpdesk
  - Helpdesk probed on the process for resetting RSA token
  - Revealed resetting RSA token would invalidate the current installation

# Gaining Initial Access

- John was about leave the country for vacation after a week
- 3 Hour - Window

## #Hour 3

- Outgoing Call #2 to Helpdesk posing as John:
  - Request RSA Token Reset - Successful
  - Received the QR Code on John's email from Helpdesk
  - Follow up email from Helpdesk deleted
- Fake helpdesk email sent to John :
  - RSA token access extended
  - John did not contact the IT support.



# Gaining Initial Access

## #Hour 2

- Login attempt on Production VPN:
  - Created a new azure windows VM
  - Authentication Successful
  - Compliance checks failed on device

## #Final Hour

- Login attempt on Test VPN:
  - Authentication Successful
  - Device Compliance not enforced in test VPN
  - Gained Foothold on the internal network



# After Breach

## Goals:

- XDR Bypass – CrowdStrike Falcon and Trellix
- Privilege Escalation from standard user
- Domain Compromise
- Monitor Bank Communications
- Gain Access to Cloud Applications



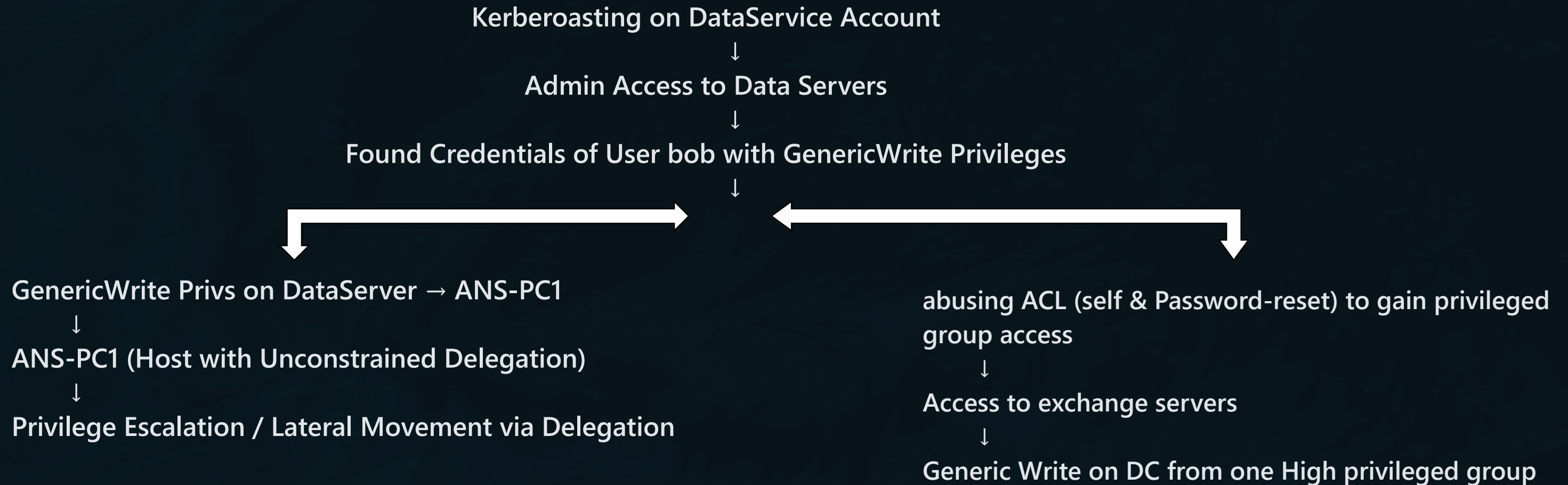
# Phase 2: Enumeration

- Pivoted from VPN -> Ctrix
- Enumeration:
  - Powershell Enabled
  - 40+ Domain Controllers
  - Critical Servers, ESXi logins, File Shares etc
  - Crowdstrike Falcon and Trellix EDR agents
  - Misconfigurations Identified
- Keys to the kingdom:
  - Shares had access to 18TB of storage files
  - Sensitive information like bank documents, Vulnerability reports, Passwords etc

# Enumeration

- Misconfigurations Identified:
  - 50+ Service accounts had SPN set (Can be kerbroastable)
  - 2 Service accounts were part of admin groups of few data Integration servers
    - DataService
    - TransferService
  - 1 x Unconstrained Delegation set – ANS-PC1
  - 1 x account had generic write privileges over ANS-PC1: "*Bob*"
- Conclusion:
  - 2 Service accounts
  - Needed a valid attack path to reach the *Bob*

# Attack Path



# Attack Path

Deep dive into shares for credentials



Root password for ESXI



Domain Controller compromise



Data Exfiltration

# Test Environment Setup & Research

- Replication of the environment provided
- Procurement of CrowdStrike Falcon and Trellix
- Every commands and possible enumeration techniques were tested
- 1 live of the Land technique didn't raise any alerts
- Bespoke malware created to evade both the EDRs



# XDR Bypass – Malware

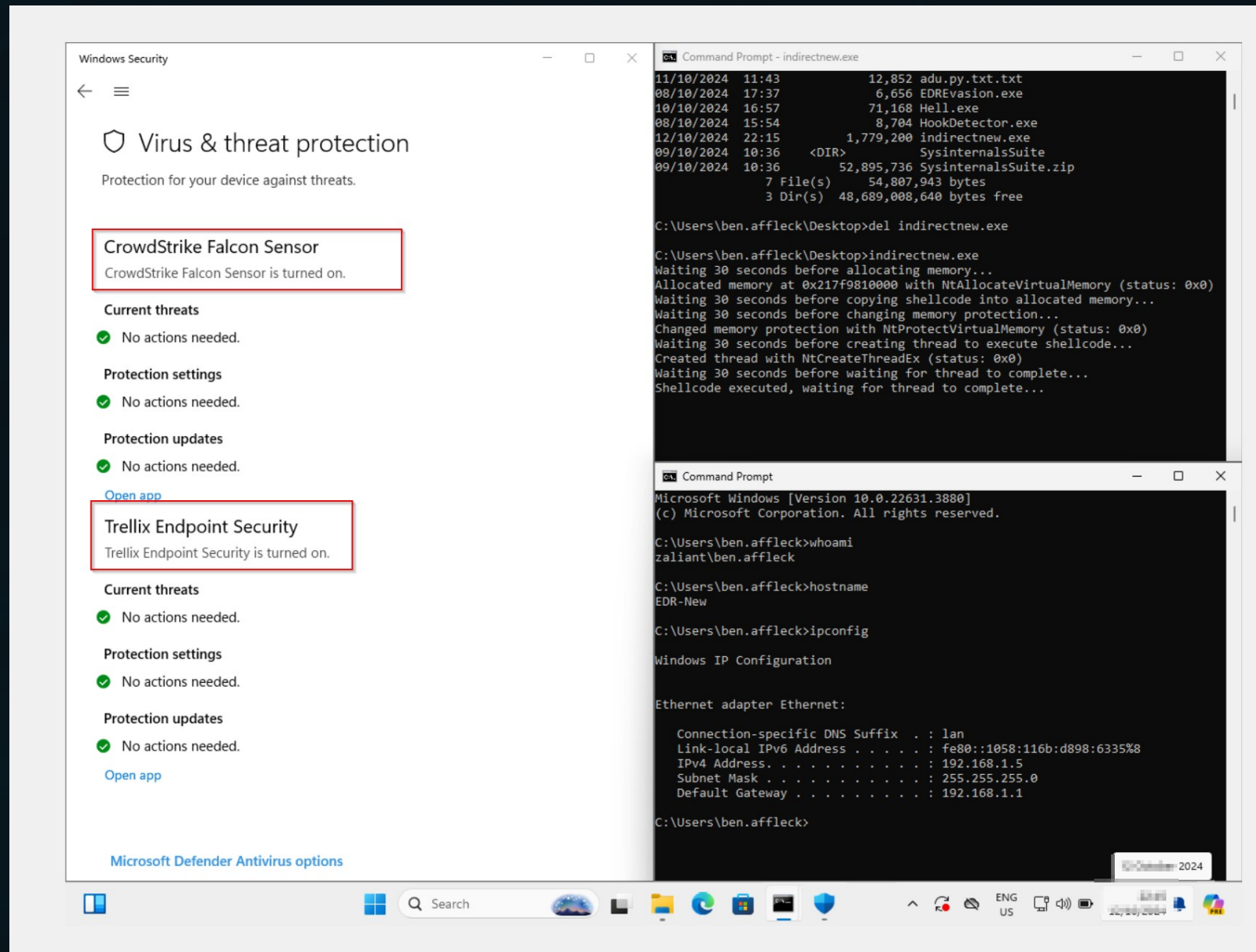
Configurations: Aggressive mode – CS Falcon, Trellix – All security policies included in the trial version

EDR Checks	Evasion Technique	Implementation
Static Analysis	Obfuscation	Stripping debug symbols/information using golang
Runtime Analysis	Shellcode Encryption	Shellcode encrypted with AES + GCM
Behavioral Analysis	Sleep	30 seconds sleep before any API call
Userland Hooks	Indirect Syscalls	Implemented in Go
Process Integrity	Process Injection	QueueUserApc Process Injection
Network Connections (Process wide)	Inject into Legitimate Porcess	Injected Into MSEdge/ Chrome to connect over 443

Note: This was a configurational bypass. A bypass to touch/dump LSASS process was not feasible within the given time frame.

# Testing before Exploitation

- Malware was tested in our replicated environment before deploying



# Testing before Exploitation

The screenshot shows a terminal window with a table of network connections and an Event Viewer window showing logs. The terminal window has a menu bar with 'avoc', 'View', 'Attack', 'Scripts', and 'Help'. The table below lists connection details:

ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
10ed6db4	192.168.1.5	192.168.1.5	ben.affleck	EDR-NEW	Windows 10	indirectnew.exe	10268	0s	healthy

The Event Viewer window shows the following logs:

- 17:27:28 Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
- 17:26:48 [\*] Started "New-HTTPS" listener
- 17:26:56 [+] Spider connected to teamserver
- 17:26:56 [-] Spider disconnected from teamserver
- 17:27:28 [+] Neo connected to teamserver
- 17:28:07 [\*] Started "New-Https" listener
- 17:30:02 [\*] Initialized 2a200c4c :: Ghost@192.168.1.6 (TEST-C2)
- 17:34:19 [\*] Initialized 7999b022 :: Ghost@192.168.1.6 (TEST-C2)
- 17:37:13 [\*] Initialized 2ea655a8 :: Ghost@192.168.1.6 (TEST-C2)
- 17:40:11 [\*] Initialized 10ed6db4 :: ben.affleck@192.168.1.5 (EDR-NEW)

The terminal window shows a chat window with the following content:

```
2/10/2024 17:42:33 [Neo] Demon » whoami
[*] [687DE502] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [31 bytes]
[+] Received Output [2800 bytes]:

serName          SID
=====
ALIANt\ben.affleck  S-1-5-21-1165996711-597505425-1296197758-1104

ROUP INFORMATION          Type          SID          Attributes
=====
veryone                   Well-known group  S-1-1-0      Mandatory group, Enabled by default, Enabled group,
UILTIIN\Users             Alias           S-1-5-32-545 Mandatory group, Enabled by default, Enabled group,
T AUTHORITY\INTERACTIVE  Well-known group  S-1-5-4      Mandatory group, Enabled by default, Enabled group,
ONSOLE LOGON              Well-known group  S-1-2-1      Mandatory group, Enabled by default, Enabled group,
T AUTHORITY\Authenticated Users Well-known group  S-1-5-11     Mandatory group, Enabled by default, Enabled group,
T AUTHORITY\This Organization Well-known group  S-1-5-15     Mandatory group, Enabled by default, Enabled group,
OCAL                      Well-known group  S-1-2-0      Mandatory group, Enabled by default, Enabled group,
uthentication authority asserted identity Well-known group  S-1-18-1     Mandatory group, Enabled by default, Enabled group,
andatory Label\Medium Mandatory Level Label           S-1-16-8192  Mandatory group, Enabled by default, Enabled group,

rivilege Name            Description          State
=====
eShutdownPrivilege      Shut down the system Disabled
eChangeNotifyPrivilege  Bypass traverse checking Enabled
eUndockPrivilege         Remove computer from docking station Disabled
eIncreaseWorkingSetPrivilege Increase a process working set Disabled
eTimeZonePrivilege      Change the time zone Disabled

[*] BOF execution completed

2/10/2024 17:45:50 [Neo] Demon » shell whoami
[*] [F1C398A6] Tasked demon to execute a shell command
[+] Send Task to Agent [112 bytes]
[+] Received Output [21 bytes]:
aliant\ben.affleck

en.affleck/EDR-NEW indirectnew.exe/10268 x64 (zaliant.local)
>>
```

# Exploitation

- Successful Reverse connection back to our C2 after 5 minutes of malware execution
- Socks Proxy initiated successfully

The screenshot displays the Havoc interface. At the top, a menu bar includes 'Havoc', 'View', 'Attack', 'Scripts', and 'Help'. Below this is a table with the following columns: ID, External, Internal, User, Computer, OS, Process, PID, Last, and Health. A single row is visible, representing an active agent with ID '76e417fe', running 'msedge.exe' on a 'Windows 2019 Server' at computer 'VA12'. The 'Last' column shows '40s' and the 'Health' column shows 'healthy'. Below the table, there are several tabs: 'Teamserver Chat', 'Listeners', '[6a2902be] ben.affleck/EDR-NEW', and '[76e417fe] VA12'. The active chat window shows the following log entries:

```
09/12/2024 20:43:10 Agent 76E417FE authenticated as [redacted] :: [Internal: 10.61.32.112] [Process: msedge.exe\10860] [Arch: x64] [Pivot: Direct]
09/12/2024 20:45:57 [ghost] Demon » whoami
[*] [1DC7B358] Tasked demon to get the info from whoami /all without starting cmd.exe
[+] Send Task to Agent [31 bytes]
[+] Received Output [8192 bytes]:
UserName      SID
-----
[redacted] S-1-5-21-1483617462-2015505939-1458450816-206956
```





# Lateral Movement & Priv Esc

- The service account \$DataService had admin privileges over multiple data integration servers
- Enter-PSSession was used to laterally move since the account was part of \$DenyLogonLocally and \$DenyRemoteLogon
- Few Data integrations servers were enumerated thoroughly
- A script in the C:\ps1-scripts folder on \$DS1 system had credentials of *Bob*
- No Alerts so far!



# Domain Compromise

- Debating on which attack path to take? Delegation or Abusing groups
- Naah, We'll go for the third.
- Logged into vSphere as root user
- Powered off one of the DC, retrieved VMDK file, copied to a share folder

# Data Exfiltration

- Web filters were in place restricting access to uncategorized website - 24 hours time from before being blocked permanently
- Hosted a website called acme.finance with OwnCloud
- Exfiltrated the VMDK file

# Key Takeaways

- Configuring EDRs and XDRs with better detection settings
- Implementing Advanced IOC with event-based rules
- Configuring Alerts on critical endpoints
- Impossible logon, Geo-restrictions
- Security awareness and Red team exercises

Q&A

Thank you!

