A Leader in Managed IT, Multi-Cloud and Cybersecurity Services for the Global Financial Services Industry

[redacted] 2024Q4
External and Internal Network Penetration Testing & Social Engineering Report

2024Q4 / v1.0

Project Objective

Abacus Group was contracted by [redacted] to perform a full network penetration test with social engineering between the dates of November 11, 2024, and December 13, 2024, on [redacted] external and internal infrastructure. The integration of both social engineering and network penetration testing allowed Abacus Group to more fully emulate a real-world advanced persistent threat (APT) of moderate sophistication whose intent is to compromise [redacted] information systems.

Objectives of this Exercise:

- Stealthily manipulate [redacted] employees into unknowingly allowing unauthorized access to confidential information or privileged access to information systems in order to evaluate the following:
  - The level of employee security awareness
  - Maturity and implementation level of technical security controls
  - Company information security management policies and employee adherence to those policies

- Bring attention to the weakest areas of [redacted] security posture by exploiting the highest risk security gaps and attack vectors present across [redacted] external and internal networks.

- Provide full due diligence information to [redacted] such as vulnerability details, risk mitigation recommendations, reconnaissance processes, exploitation methods, information system statistics, any compromised credentials, any acquired system configuration files, kill-chain diagrams, network diagrams, and more.

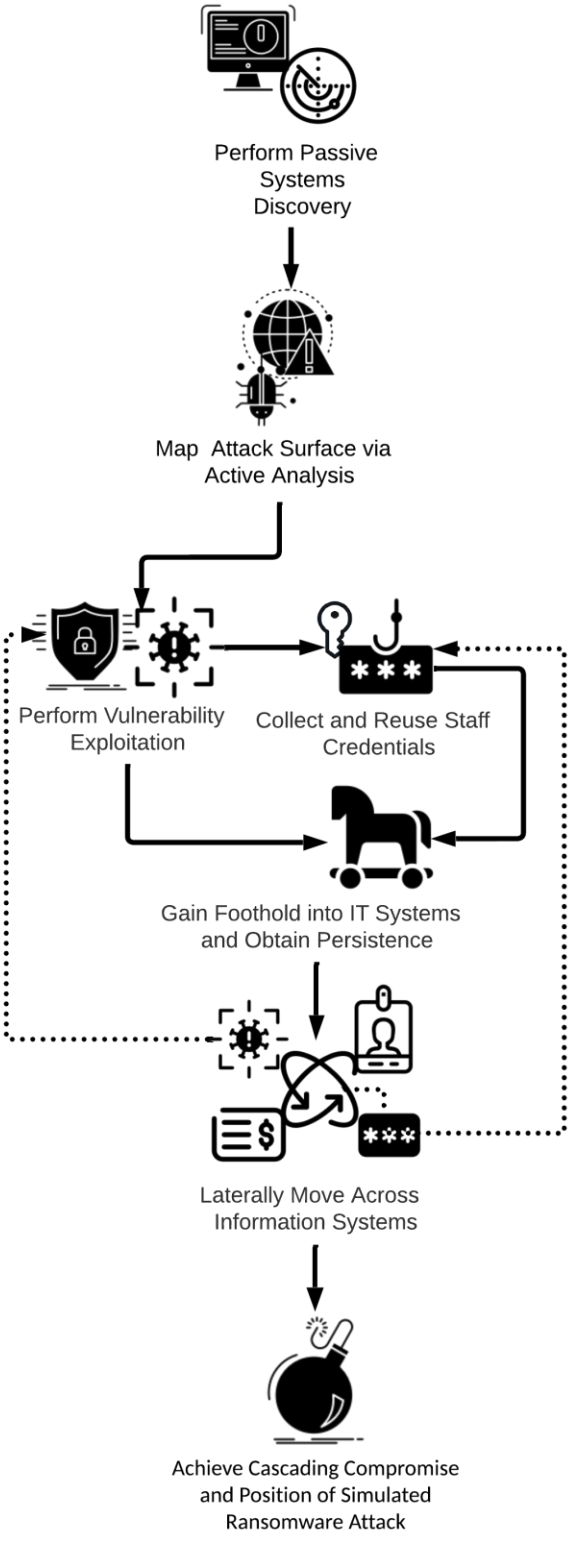
Abacus Group performed testing in accordance with NIST SP800-115 (Technical Guide to Information Security Testing and Assessment), PTES (Penetration Testing Execution Standard), and the MITRE ATT&CK framework. The findings in this report are not necessarily exhaustive; they are limited to IT system targets within the signed Rules of Engagement (RoE) scope or directly approved by [redacted] point of contact during the engagement. Furthermore, resource restrictions and the need to avoid disrupting business operations limit the testing that may be performed.

This report reflects [redacted] security posture, as seen during the dates in which the penetration testing was conducted. Future changes to any applications or infrastructure will alter the security position of the environment from its current state. Additionally, as time passes, new types of attacks may arise which were previously unknown to the security industry. Considering this, Abacus Group always recommends that all information systems undergo recurring security testing within a reasonable timeframe.

Table of Contents

Project Objective 1
Penetration Testing Methodology 3
Risk Scoring 4
Risk Results Key 5
Penetration Testing Summary 7
External Network Penetration Testing Narrative 8
Internal Network Penetration Testing Narrative 15
Social Engineering Reconnaissance 31
Social Engineering Campaign 1: O365 Password Spray + Credential Stuffing with MFA Bypass 36
Social Engineering Campaign 2: SMS Phishing (Smishing) 38
Social Engineering Campaign 3: Spearphishing via Impersonation of the Academy Group 45
Social Engineering Campaign 4: General Phishing - LifeLock 47
Risk Details 50
Conclusion 66
Appendix A – MITRE ATT&CK Tactic Definitions 67

Penetration Testing Methodology

Pentesting Phases	MITRE ATT&CK Tactics	Abacus Group's Standard Kill Chain
Conduct Organizational Reconnaissance	Reconnaissance TA0043	
Conduct Intelligence Gathering	Resource Development TA0042	
Analyze the Attack Surface		
Conduct Initial Exploitation	Initial Access TA0001	
Establish a Foothold	Execution TA0002	
	Persistence TA0003	
	Defense Evasion TA005	
Conduct Lateral Movement	Lateral Movement TA0008	
Privilege Escalation	Privilege Escalation TA0004	
	Discovery TA0007	
	Collection TA0009	
Establish Command and Control	Command and Control TA0011	
Demonstrate the Practical Impact	Impact TA0040	

Risk Scoring

To present the findings in a manner easily digested and prioritized, Abacus Group uses the traditional aspects of Magnitude of Impact and Ease of Exploitation to determine the Level of Risk associated with individual findings identified in this security assessment.

Magnitude of Impact

The Magnitude of Impact rating is a measure of the damage each weakness could inflict on the organization and is based on access, data, etc., obtained through exploitation (i.e., level of access gained, types of information accessed, the strength of security measures bypassed).

Rating	Definition
HIGH	Exploitation could seriously affect system confidentiality, availability, integrity, or authentication. Resources to mitigate high risks should receive priority.
MODERATE	Exploitation could moderately affect system confidentiality, availability, integrity, or authentication.
LOW	Exploitation could minimally affect system confidentiality, availability, integrity, or authentication. The presence of multiple low impact findings could result in a finding with a higher impact rating.

Ease of Exploitation

The Ease of Exploitation rating measures the degree of difficulty for exploiting each finding. The higher the rating, the easier it is to exploit the finding and, therefore, the more likely it is to be exploited.

Rating	Definition
HIGH	Exploitation is easily accomplished using freely and readily available tools, techniques, and exploits.
MODERATE	Exploitation is moderately accomplished using a combination of freely available and custom tools, techniques, and exploits.
LOW	Exploitation is difficult to accomplish and requires a significant investment of time to develop custom tools, techniques, and exploits.

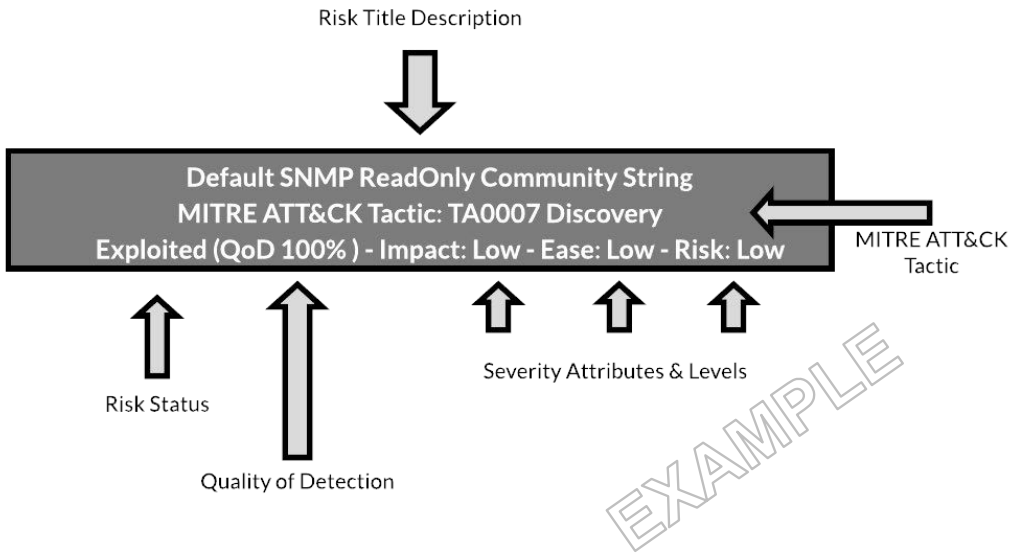
Level of Risk

		MAGNITUDE OF IMPACT		
		HIGH	MODERATE	LOW
EASE OF EXPLOITATION	HIGH	HIGH	MODERATE	MODERATE
	MODERATE	MODERATE	MODERATE	LOW
	LOW	MODERATE	LOW	LOW

Security Findings that are noteworthy but do not have an associated risk are labeled as Informational. Informational Security Findings are not inherently usable as attack vectors but may have associated operational excellence recommendations for implementing additional technical safeguards and controls.

Risk Results Key

Pertinent, insightful metrics accompany the title bar of each noteworthy risk.

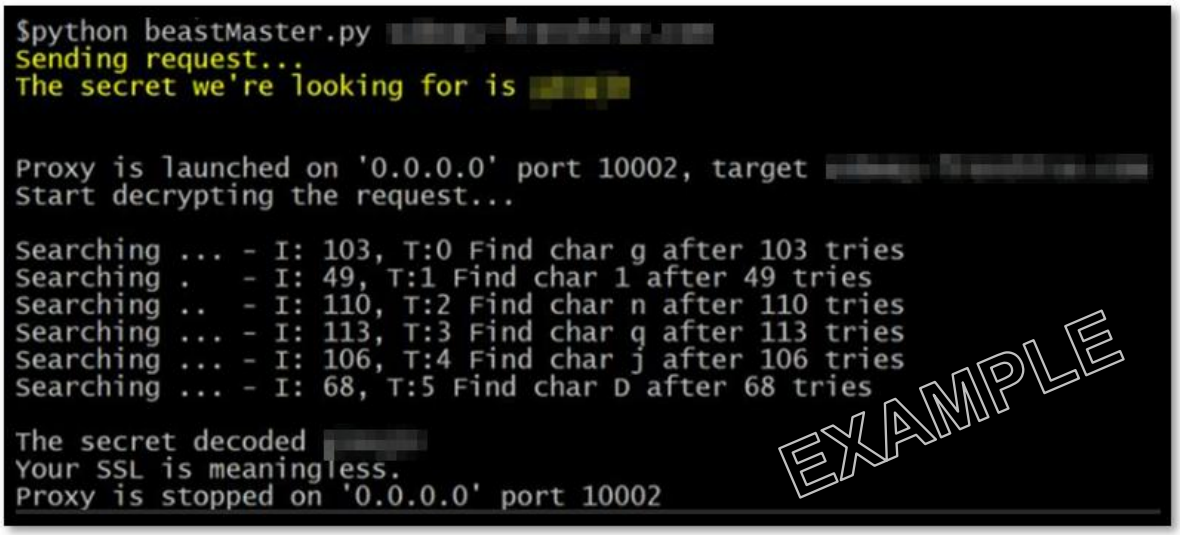


- **Risk Title Bar**
  - ***Risk Title Description***
    - Contains a brief description of the pertinent risk.
  - ***MITRE ATT&CK Tactic***
    - Defines the MITRE ATT&CK Tactic category to which the risk is most closely associated to.
  - ***Risk Status***
    - Specifies if the risk was detected or exploited. In many situations, a high-severity risk is detected but not exploited due to the potential service impact to a production system and subsequent violation of the project Rules of Engagement (RoE).
    - In some cases of a service-impactful risk, a proof-of-concept exploit can be safely performed.
  - ***QoD (Quality of Detection)***
    - For "*Detected*" but not exploited risks, QoD is a value between 0% and 100% (i.e., confidence) that ranks the reliability of the executed network vulnerability test or fingerprinted information system.
  - ***Impact***
    - The Impact rating is a measure of the damage each weakness could inflict on the organization and is based on access, data, etc., obtained through exploitation.
  - ***Ease***
    - The Ease rating measures the degree of difficulty for exploiting each finding. The higher the rating, the easier it is to exploit the finding and, therefore, the more likely it is to be exploited.
  - ***Risk***
    - The Risk rating is based largely upon the potential negative impact to the pertinent environment combined with the ease of exploitation as illustrated in the matrix on the previous page.

Insecure TLS Protocols and Cipher Suites Susceptible to BEAST Attack
MITRE ATT&CK Tactic: TA0001-Initial Access
Exploited – **Impact:** Moderate – **Ease:** Moderate – **Risk:** Moderate

Summary:
The affected endpoints supported outdated TLS versions 1.0 and 1.1, along with weak cipher suites with known attacks. This may allow a malicious actor to sniff webserver traffic and decrypt the content of an encrypted session, gaining access to potentially sensitive information. TLSv1.0 is considered obsolete, and TLSv1.1 is rapidly being retired from production. It was possible to leverage the Browser Exploit Against SSL/TLS (BEAST) attack to defeat TLS on the affected endpoints.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Update TLS configurations for modern or intermediate compatibility. Intermediate is the recommended configuration for the vast majority of services that do not need compatibility with legacy clients, such as Windows XP or old versions of OpenSSL, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

- **Risk Body**
  - ***Summary***
    - Contains a high-level overview of the risk description.
  - ***Risk Detection Result(s)***
    - Demonstrates evidence that the risk exists, showcases exploitation if exploitation was performed.
  - ***Risk Mitigation Recommendation(s)***
    - Gives recommendations on how to best mitigate this risk.
  - ***Reference(s)***
    - Lists useful outside references that elaborate on the risk and/or provide additional mitigation recommendations.
  - ***Affected Endpoint(s)***
    - Lists every endpoint detected as being affected by this risk.

Penetration Testing Summary

[redacted]

Organization	[redacted]		
Point of Contact Name	[redacted]	Security Testing Timeframe	[redacted]
Point of Contact Phone	[redacted]	Point of Contact Email	[redacted]

Total Count of Security Findings:

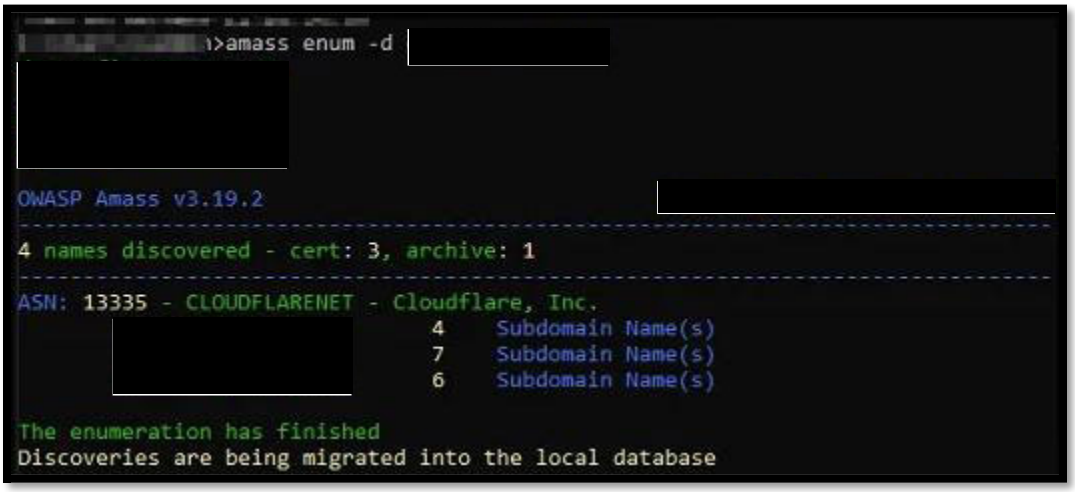
3	6	5	1
High	Moderate	Low	Informational

Summary of Risk Results	
Risk Title Description	**Affected Endpoint(s)**
NBNS, LLMNR, and/or mDNS Service Poisoning	[redacted]
OpenSSH Susceptible to CVE-2024-6387	[redacted]
Cisco Smart Install (SMI) Remote Code Execution	[redacted]
Insufficient Conditional Access Policies	Organization-Wide
IPv4/IPv6 Dual Stack Environment Without First Hop Security	[redacted]
Lack of Dynamic ARP Inspection	[redacted]
Lack of DHCP Snooping	[redacted]
Weak User & Admin Password Complexity Requirements	[redacted]
Lateral Movement via Windows Remote Management (WinRM)	[redacted]
Content-Security-Policy (CSP) Not Implemented	[redacted]
Out of Date jQuery Potentially Susceptible to Multiple Vulnerabilities	[redacted]
SMB/MSRPC Null Session	[redacted]
Printers With Jetdirect Are Accessible and Exploitable	[redacted]
DHCP Guard Not Enabled	[redacted]

External Network Penetration Testing Narrative

Abacus Group's role was to replicate the vantage point of a malicious actor with no access or prior information about [redacted] information systems. This engagement was a full-scope external network penetration test designed to assess how well [redacted] networks could withstand an attack from a sophisticated, real-world adversary. All penetration testing activities performed by Abacus Group came from the source subnets of [redacted], [redacted], and [redacted] as defined in the RoE.

Abacus Group approached this attack surface analysis from a fully black-box perspective. DNS subdomain enumeration was performed using techniques such as wordlist-based DNS resolution, reverse IP address lookups, MX and SOA record inspection, and Autonomous System (AS) number lookups. This helped provide a baseline of IP addresses and subdomains associated with [redacted] including server infrastructure and external web applications. These techniques allowed Abacus Group to establish an understanding of the full attack surface of the organization. This information was then corroborated by leveraging a powerful open-source intelligence (OSINT) tool called OWASP Amass.



Demonstrating domain and subdomain enumeration

DNS Zone Transfer (AXFR) DNS requests were sent to all DNS servers. DNS servers should not permit zone transfers towards any IP address from the internet. Since zone files contain complete information about domain names, subdomains, and IP addresses configured on the target name server, this information is useful for the reconnaissance of external and internal company information systems. However, no relevant DNS entries were found to be vulnerable to DNS Zone Transfer attempts.

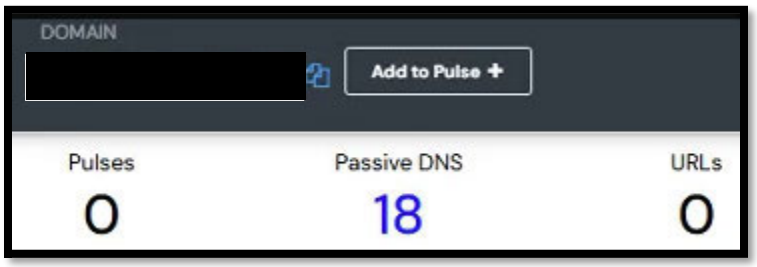
Scanning for subdomain takeover vulnerabilities was also performed on [redacted] root domains. Subdomain takeover is a type of vulnerability that appears when an organization has configured a DNS CNAME entry for one of its subdomains pointing to an external service (ex. Heroku, GitHub, Bitbucket, Desk, Squarespace, Shopify, etc.) but that organization no longer utilizes the service. An attacker could register to the external service and claim the affected subdomain. As a result, the attacker could host malicious code (ex., for stealing HTTP cookies) on the organization's subdomain and use it to attack legitimate users.

Subdomain	IP Address	CNAME	Response Code	Vulnerable
		Not found	200	✓ No
		Not found	200	✓ No
		Not found	521	✓ No
		Not found	200	✓ No
		cfipartners.com.	200	✓ No

Subdomain takeover scanning resulting in no vulnerable subdomains

Virus Total Analysis, AlienVault Open Threat Exchange (OTX), and Criminalip.io were also used to collect information about any potential Indicators of Compromise (IoCs) or relevant OSINT data potentially affecting [redacted] information systems.

IoC analysis via VirusTotal

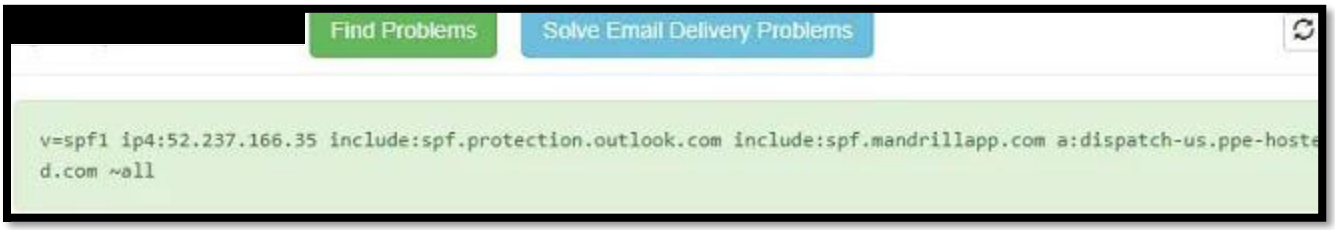


IoC analysis via AlienVault OTX

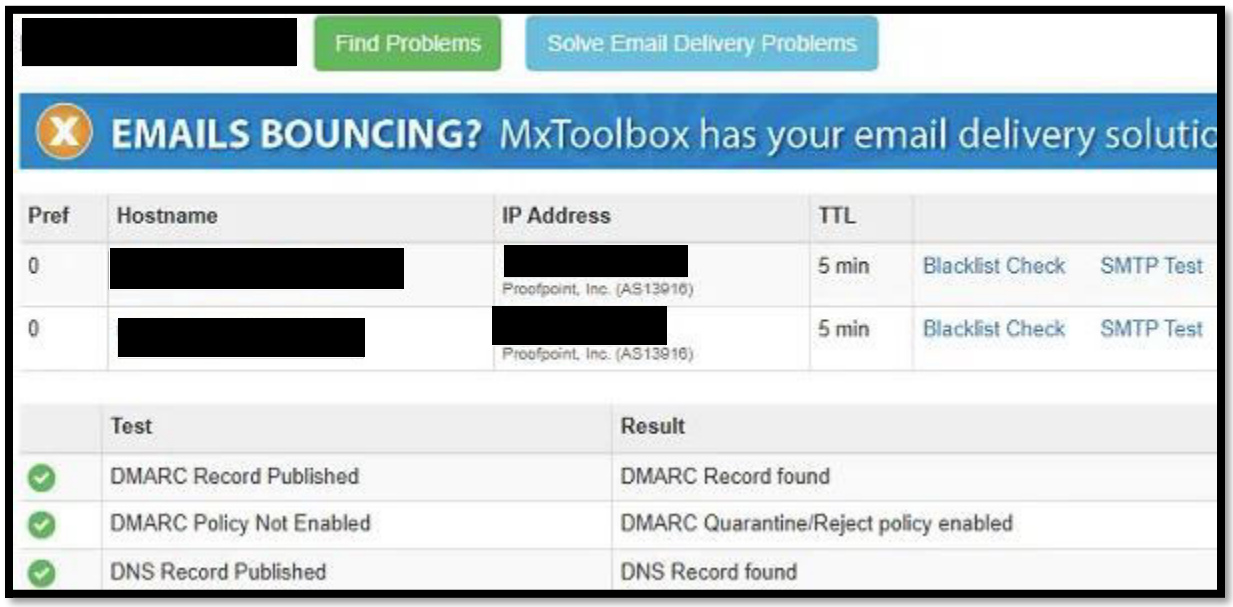
Abacus Group also utilized a publicly available domain impersonation, bitsquatting, and typosquatting monitoring tool called Dnstwist to assess if potentially malicious actors had purchased domains for use in social engineering campaigns against [redacted] employees. Dnstwist is a free tool leveraged by numerous commercial products such as Splunk ESCU, RecordedFuture, SpiderFoot, DigitalShadows, SecurityRisk, SmartFense, ThreatPipes, Palo Alto Cortex XSOAR, Rapid7, Mimecast, Watcher, Intel Owl, PatrOwl, VDA Labs and Appsecco.

Demonstrating domain impersonation analysis via DNStwist

Abacus Group assessed the mail records of [redacted] which revealed that the DomainKeys Identification Mail (DKIM) record was well configured as well as an enabled Domain-based Message Authentication Reporting and Compliance (DMARC) policy. However, the Sender Policy Framework (SPF) was overly permissive, including an IP address from a non-publicly accessible gateway. Though this is warranted as a security concern, Abacus Group has reduced the severity to informational.



Observed SPF record for [redacted]

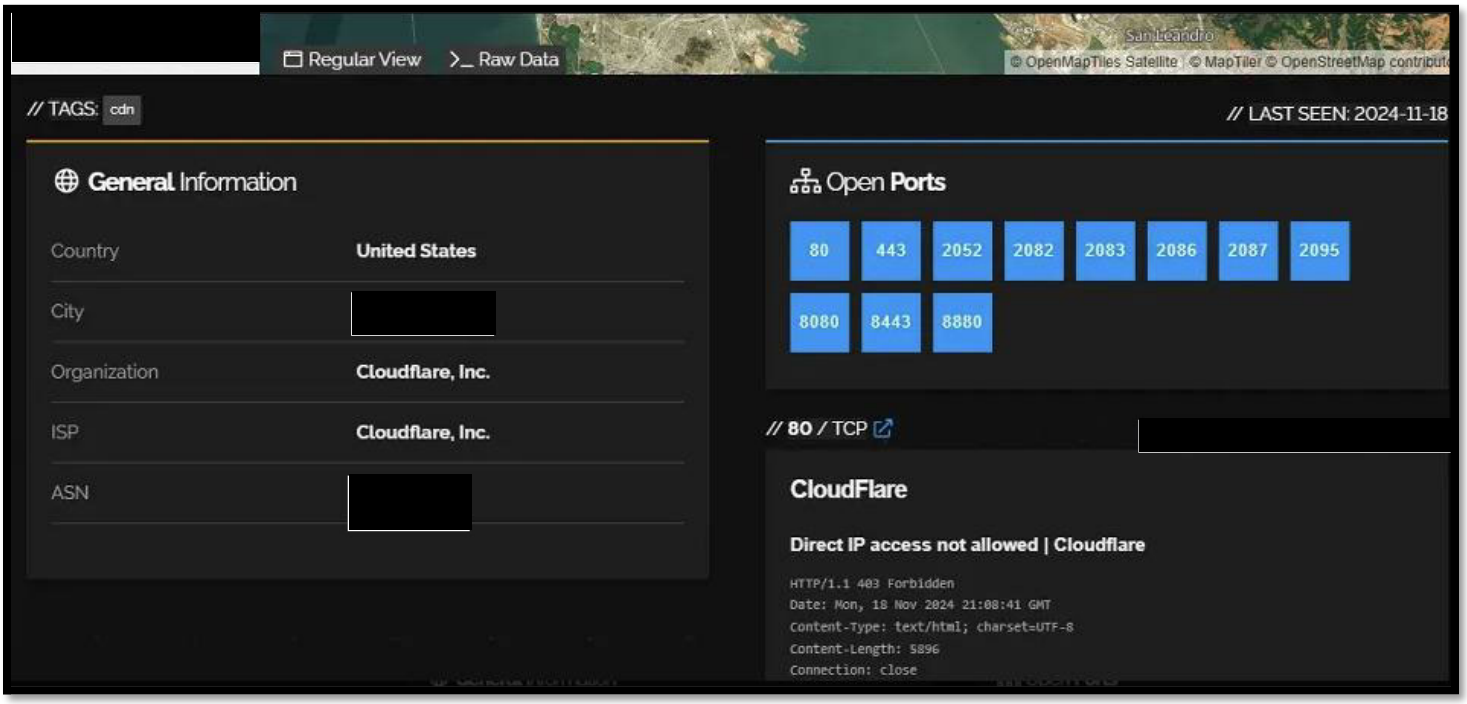


Mail record assessment demonstrating a DMARC record enabled

To further supplement passive analysis and OSINT data collection, Abacus Group used Google Dorking to search for any exposed log files, company documents, login pages, databases, or paste site dumps that could appear online within search indexes. During reconnaissance exercises, Google Dorking is often used to reveal sensitive metadata about the target company that would assist during active attacks.

Demonstrating Google Dorking via dorker.py

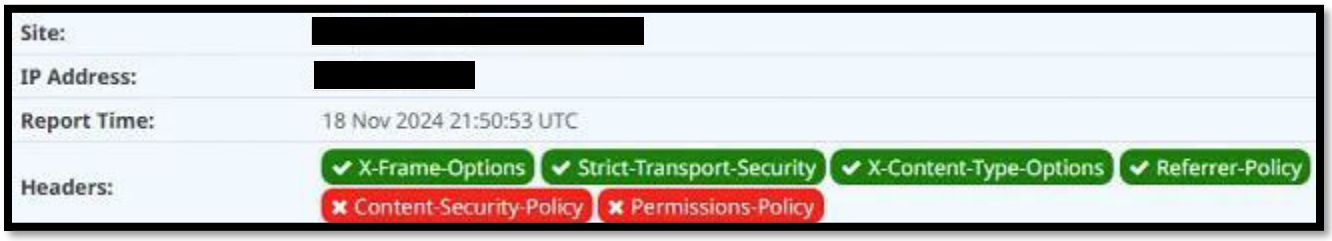
Abacus Group continued the engagement by employing both active and passive analysis techniques to collect as much identifying information as possible about [redacted] attack surface. This fingerprinting process involved collecting details of open TCP/UDP ports, listening services, specific software versions, operating system identifiers, and more. Validation was performed using both automated tools and manual inspection.



Demonstrating attack surface and web component analysis with Shodan

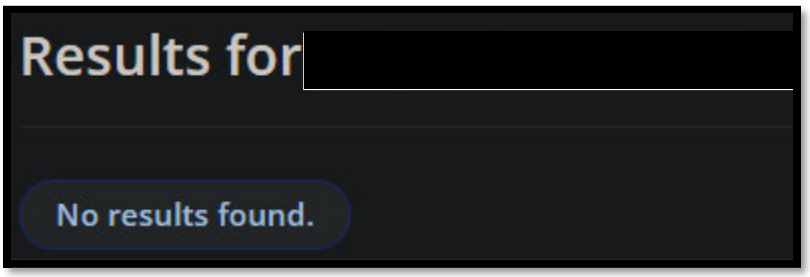
Demonstrating attack surface and web component analysis with Wappalyzer

Abacus Group then confirmed whether the web application implemented the recommended security headers, such as the "Content-Security-Policy" (CSP) and HTTP "Strict-Transport-Security" (HSTS) headers. The CSP was identified to be missing, which is warranted as a low-severity vulnerability.

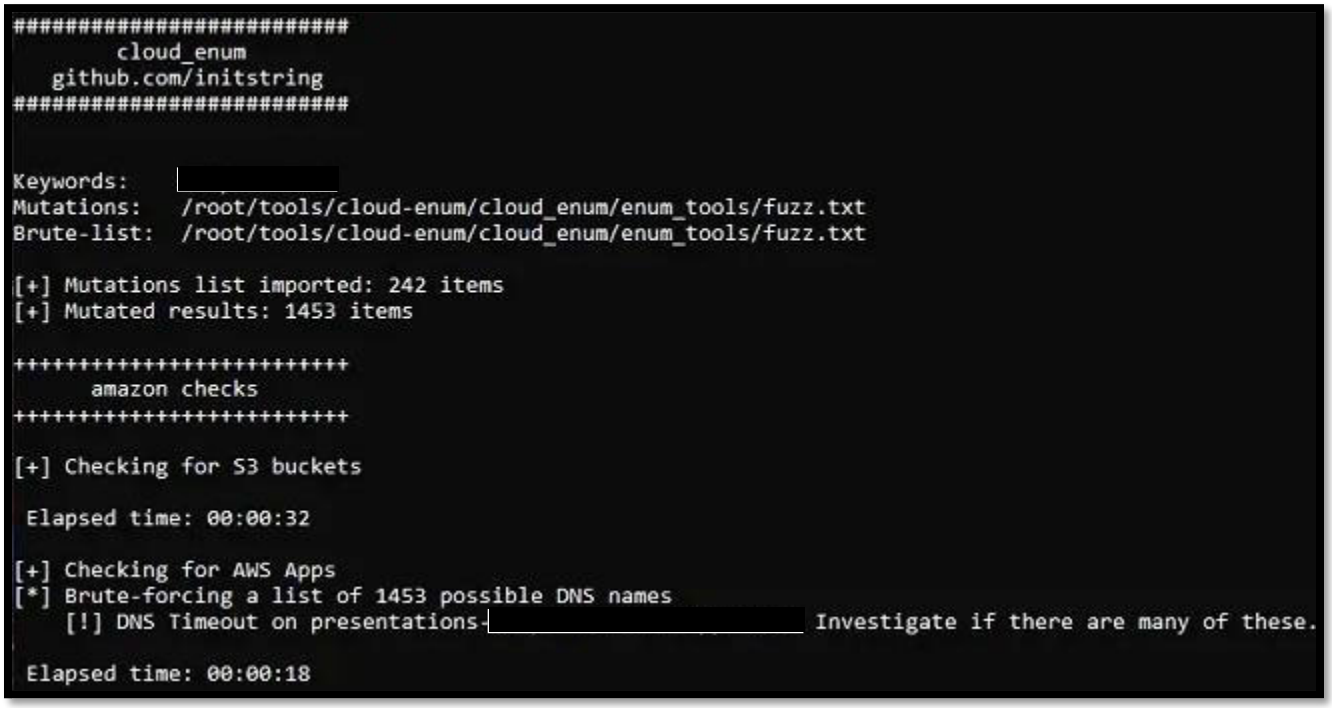


Demonstrating security header analysis

Abacus Group leveraged public search engines, and custom OSINT tooling to determine if [redacted] had any unintentionally exposed cloud resources. This process involved systematically enumerating common Azure Website DNS, storage accounts such as Amazon S3 buckets and Azure Blob, databases, virtual machines, and more.



Exposed cloud asset analysis via Grayhatwarfare

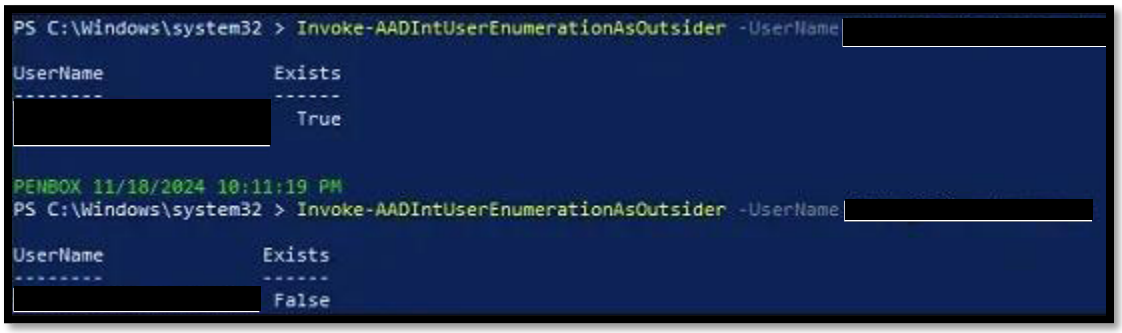


Demonstrating external cloud resource reconnaissance via CloudEnum

Having confirmed the domain being utilized, Abacus Group leveraged an open-source tool called AADInternals to enumerate details related to the Azure tenant, including associated domains, tenant id and region, and the use of DesktopSSO. Desktop SSO, also called Seamless SSO enables users to be automatically signed into the corporate network when using their corporate devices. However, the use of DesktopSSO also enabled Abacus Group to verify if specified users exist in the organization and output some login details for that user.

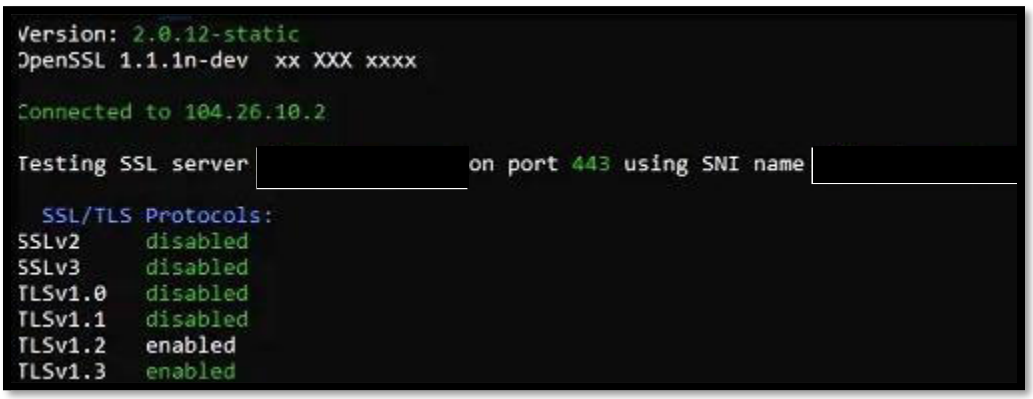
While neither Abacus Group nor Microsoft considers this to be an inherent security vulnerability, it is worth noting that a malicious actor may leverage a technique similar to the following proof of concept to enumerate users prior to a password spraying or social engineering attack.

Enumerating Azure tenant information via AAD Internals



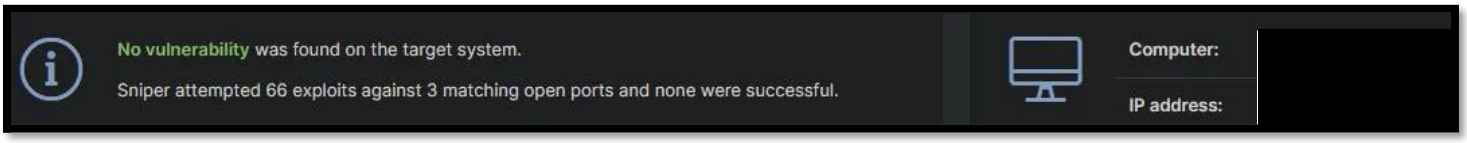
Demonstrating a user enumeration proof of concept

Abacus Group assessed the SSL/TLS configuration of the in-scope endpoints to determine if any would be susceptible to cryptographic-based attacks, such as the BEAST (browser exploitation against SSL/TLS) attack.



Demonstrating SSL/TLS cipher analysis

Abacus Group also leveraged a variety of automated vulnerability scanners across the scope of endpoints. Such vulnerability scanners included, but were not limited to, Nessus, OWASP Zap, Sn1per, and OpenVAS. During this stage of the engagement, Abacus Group leveraged these vulnerability scanners to corroborate evidence from the manual analysis and to identify any additional vulnerabilities for review and analysis.



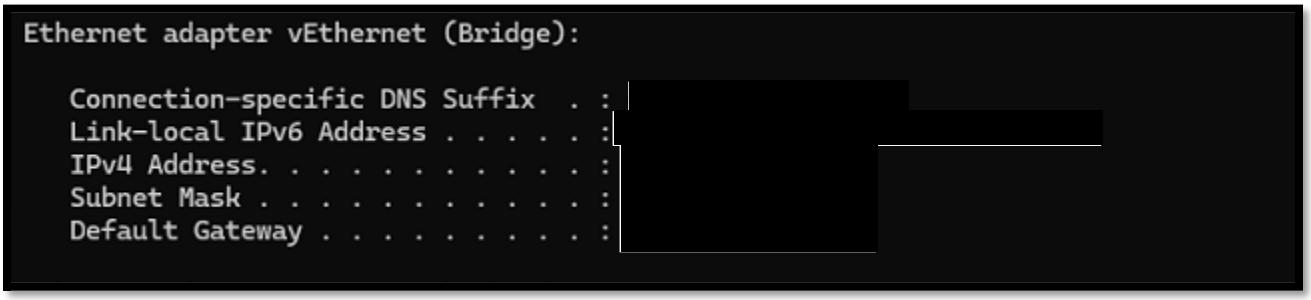
Demonstrating attack surface analysis

Having exhausted all viable in-scope attack vectors, Abacus Group completed the external network penetration testing activities. Only two low-risks findings were identified. There are few methods for ingress, and the use of social engineering would most likely be needed to obtain access to internal systems. Given the size and complexity of [redacted] attack surface, the relatively low quantity of findings indicates that a well-established security program.

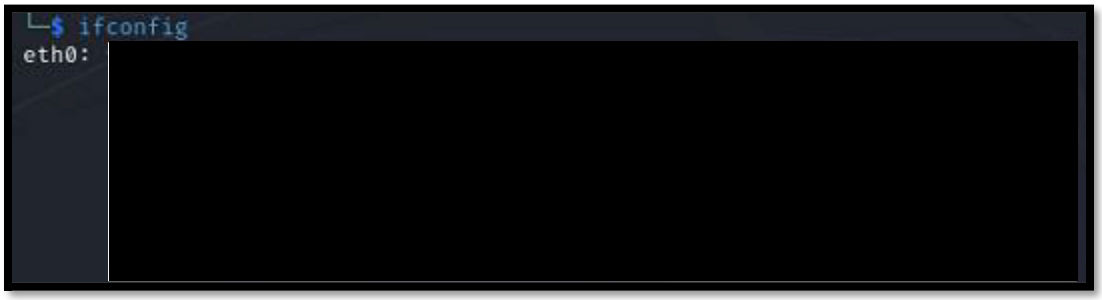
Internal Network Penetration Testing Narrative

Abacus Group's role was to replicate the vantage point of a malicious actor who had breached [redacted] external perimeter and gained access to their internal network as a user on the [redacted] network. To achieve this, a physical penetration testing device was remotely deployed on the standard user workstation virtual local area network (VLAN) within [redacted] office. This device, [redacted], and an associated Kali Linux virtual machine, [redacted], allowed Abacus Group engineers to replicate the scenario that a malicious actor had compromised a standard user workstation. [redacted] provided the following scope and context prior to the engagement.

Initial reconnaissance was performed to determine network settings and route details on the internal network penetration testing appliance.

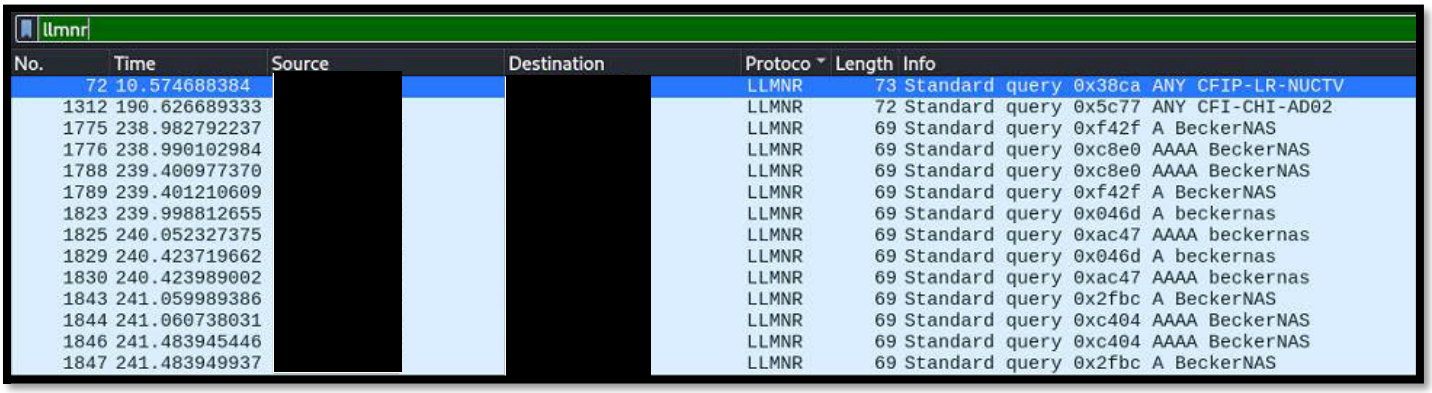


Confirming the IP address of the Windows 10 penetration testing appliance

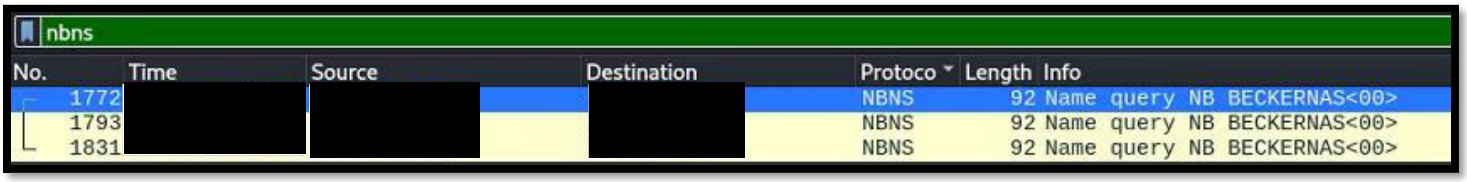


Confirming the IP address of a Kali Linux virtual machine also used for penetration testing

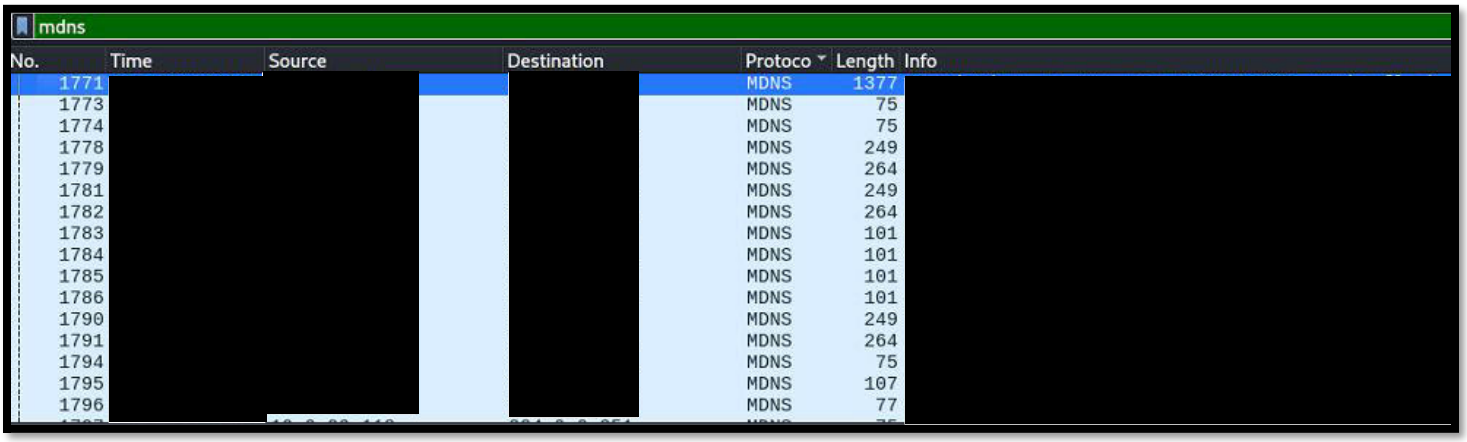
Passive reconnaissance was initiated by analyzing network traffic using tools such as Wireshark and Responder to understand the environment better. Captured traffic was filtered for services that could provide additional insight into the environment, such as CDP (Cisco Discovery Protocol), LLDP (Link-Layer Discovery Protocol), NBNS (NetBIOS), LLMNR (Link-Local Multicast Name Resolution), as well as assessing if the environment is dual-stack with the presence of IPv6 traffic.



Passive network analysis via Wireshark identified LLMNR traffic



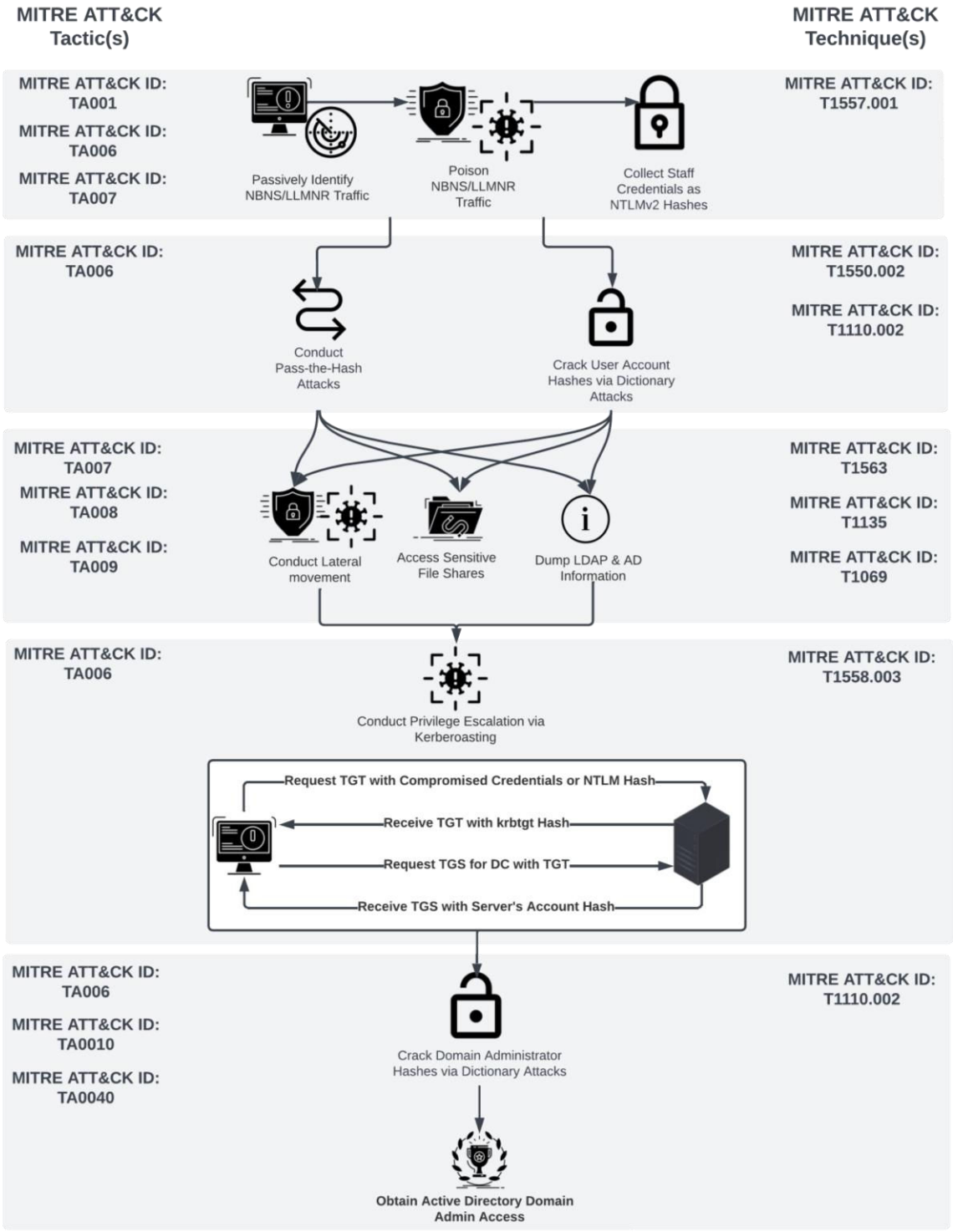
Passive network analysis via Wireshark identified NBNS traffic



Passive network analysis via Wireshark identified mDNS traffic

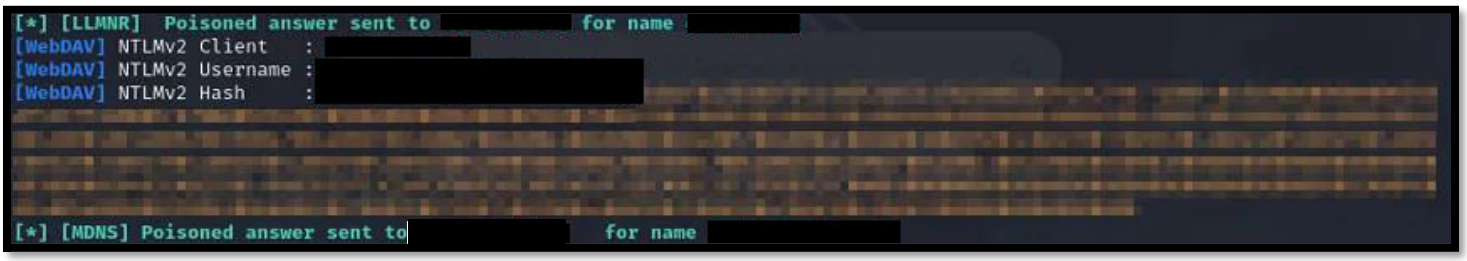
In response to discovering either NBNS or LLMNR traffic, a malicious actor would often utilize a tool such as Responder to perform NetBIOS/LLMNR poisoning. First, Responder would listen to multicast NetBIOS/LLMNR queries, spoof a response under the right conditions, and direct the victim to the machine that Responder is running on. Should the victim machine then attempt to connect to the attacking machine, Responder exploits the connection and would steal NTLM hashes, which could then be cracked using other tools. This attack vector generally provides two potential paths for further system compromise. First, malicious actors can attempt to crack the captured hashes using large-scale dictionary attacks offline. Alternatively, malicious actors can choose to conduct a pass-the-hash attack, enabling the possibility of authentication on behalf of the victim without cracking the hashed password.

A malicious actor would utilize these aforementioned user credentials to conduct lateral movement to additional systems, enumerate additional information, explore network-attached file shares, and ultimately attempt to escalate privileges. One of the most common and reliable methods of active directory exploitation is known as Kerberoasting. During this type of attack, a compromised active directory account is used to query the domain controller to enumerate service principal names (SPNs), then use a valid Kerberos ticket-granting-ticket (TGT) to obtain a ticket-granting-service (TGS) associated with those SPNs. These recovered hashes would then be targeted in a dictionary-based attack or brute-forced to reveal the plain-text passwords and ultimately compromise the domain administrator, resulting in complete network compromise.



Demonstrating the potential attack vector leveraging NBNS/LLMNR poisoning

NBNS, LLMNR, and mDNS service poisoning resulted in multiple password hashes being captured. Abacus Group engineers took these offline to crack them. Abacus Group successfully cracked the credentials for the user **Administrator**. In order to crack the credentials for the user Administrator, engineers took the hashes offline and utilized a hash cracking machine that uses "rainbow tables," which are immense lists of pre-computed hashes for every possible password. Utilizing the rainbow tables, a password hash is able to be matched to a pre-determined plaintext string.



*Responder - Capturing and poisoning LLMNR/mDNS/WebDAV to attain NTLMv2 hashes for user **Administrator***

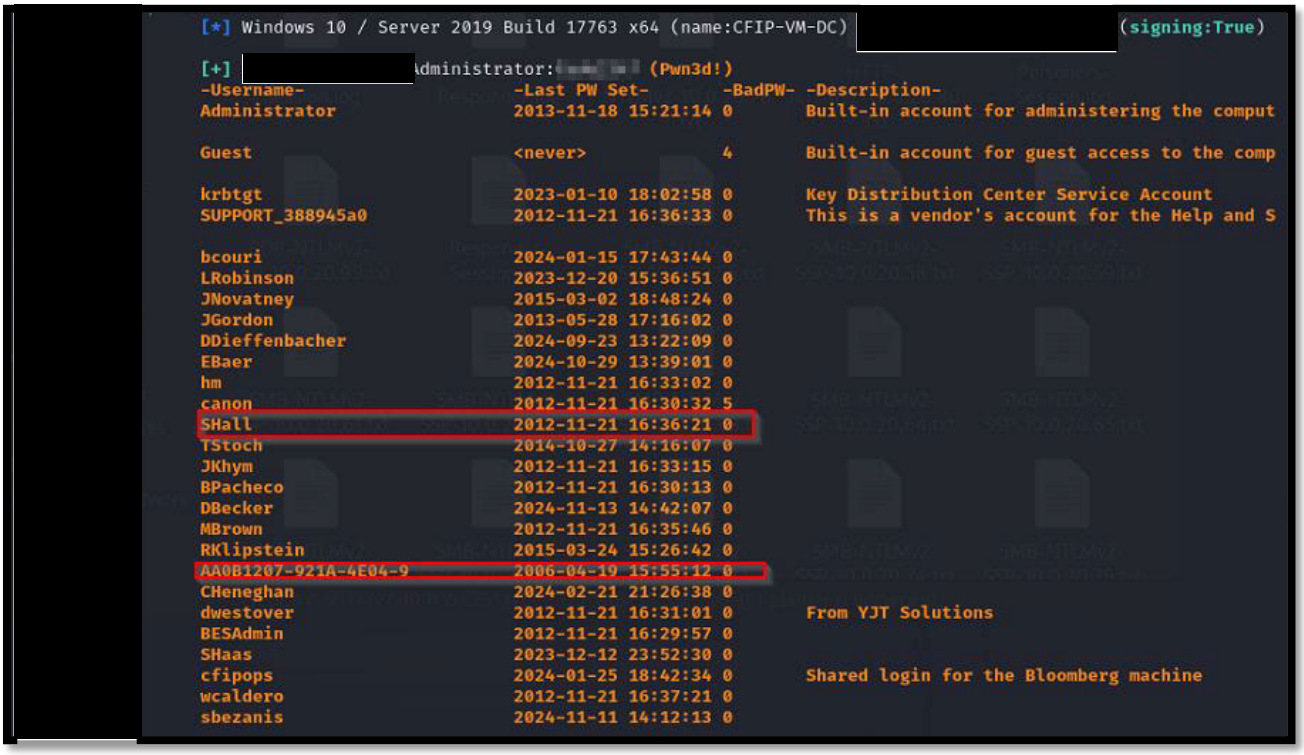
The credentials for the user Administrator were utilized against multiple endpoints throughout the testing environment to further enumerate domain users, user policies, password policies, and antivirus.

NetExec - Verifying Administrator access on [redacted] DWS-71, which originally produced NTLMv2 hashes

NetExec – Enumerating local users on [redacted] DWS-71

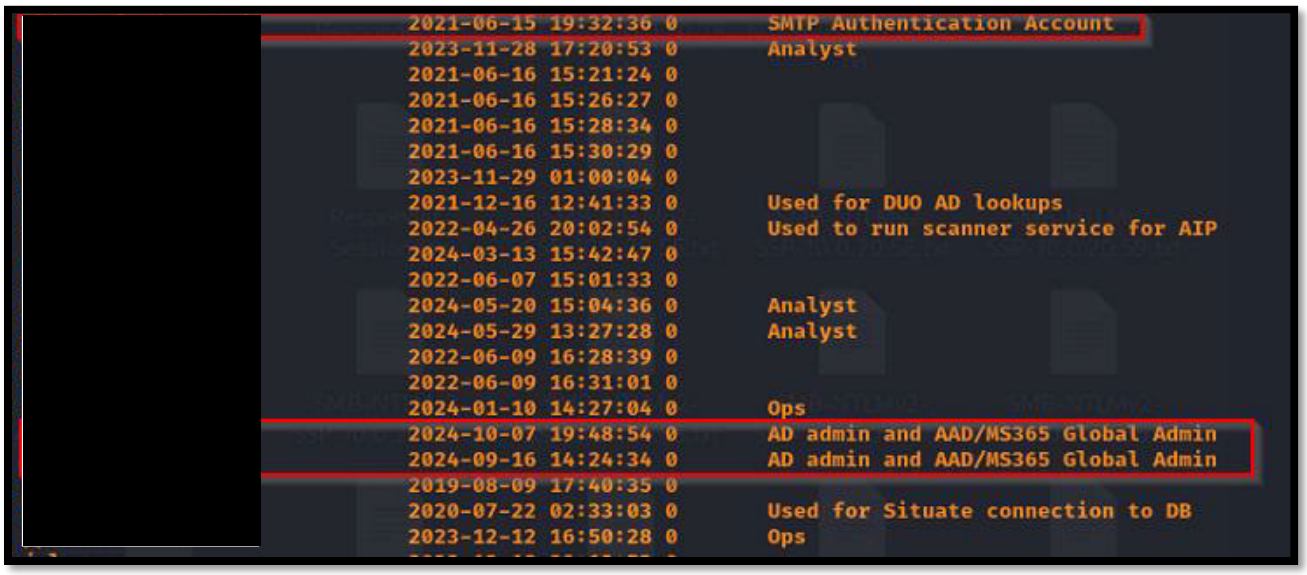
NetExec - Verifying Administrator access on [redacted] VM-DC

NetExec - Verifying Administrator access across 10.0.20.0/24

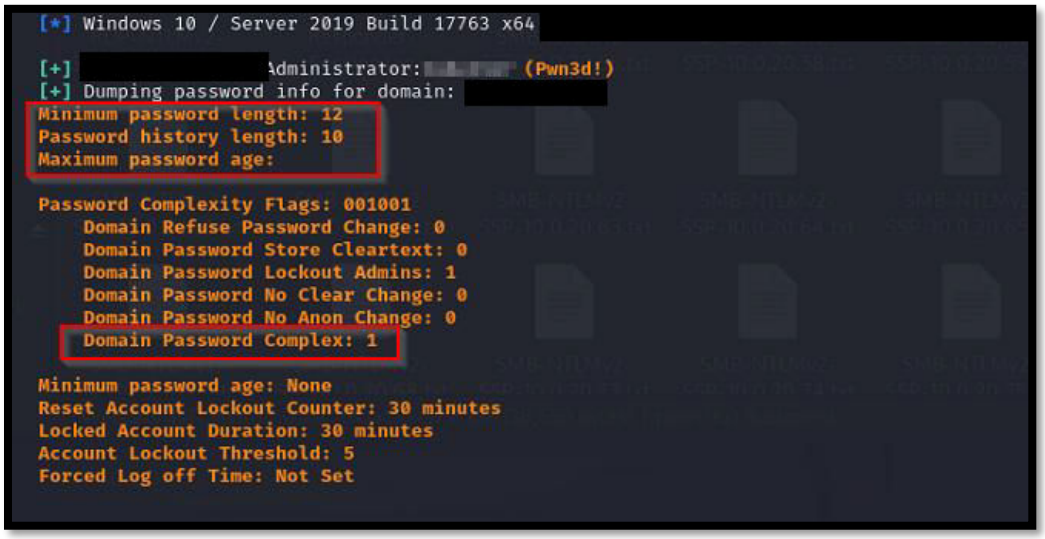


NetExec – Enumerating domain users utilizing [redacted] VM-DC

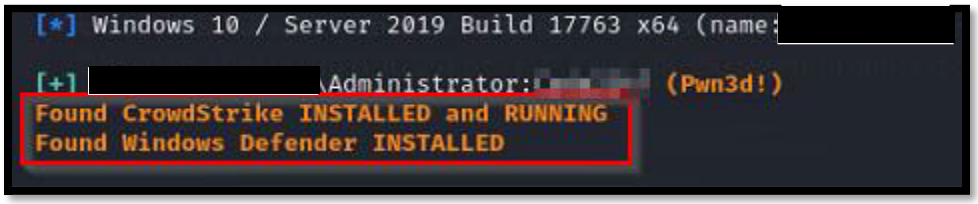
NetExec – Enumerating admin users via [redacted] SV-AD



NetExec – Identifying domain user permission/accesses via descriptions utilizing [redacted] VM-DC

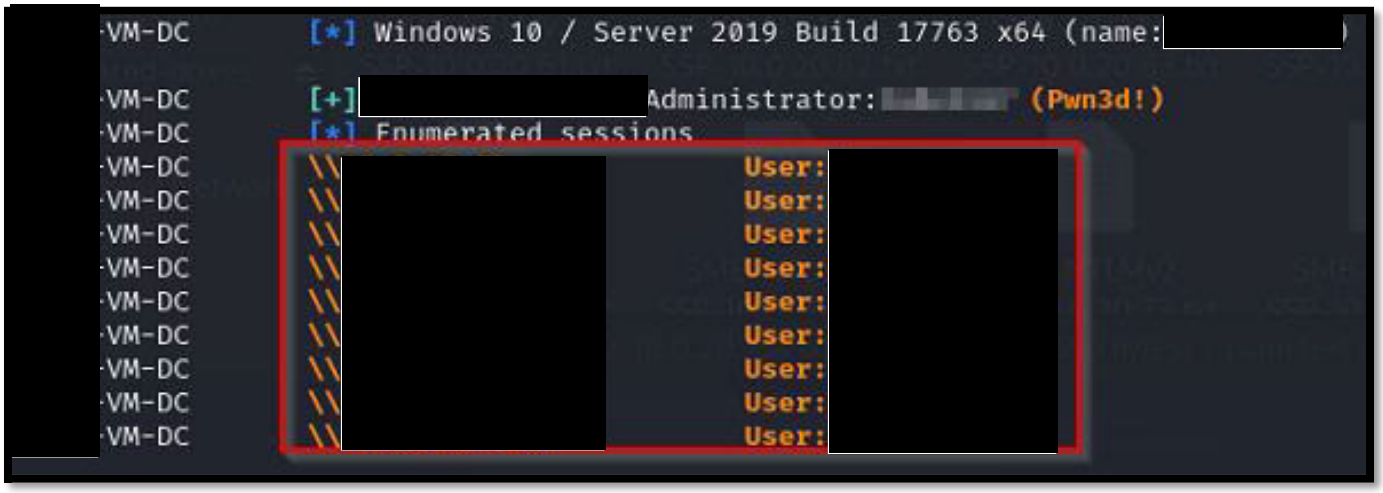


NetExec – Enumerating domain password policy utilizing [redacted] VM-DC

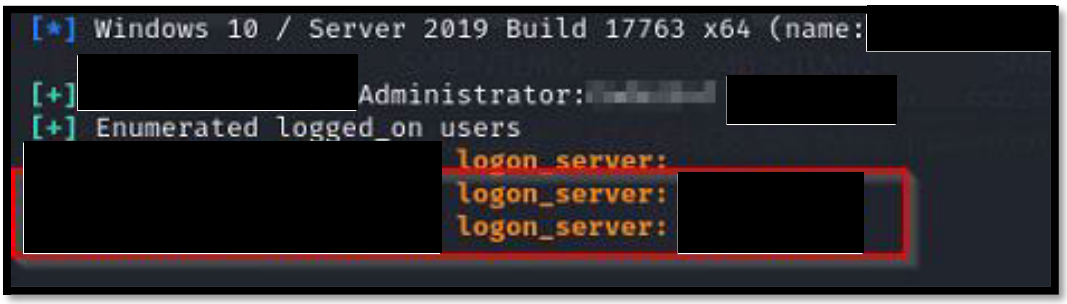


NetExec – Enumerating Antivirus/EDR products being utilized on [redacted] VM-DC

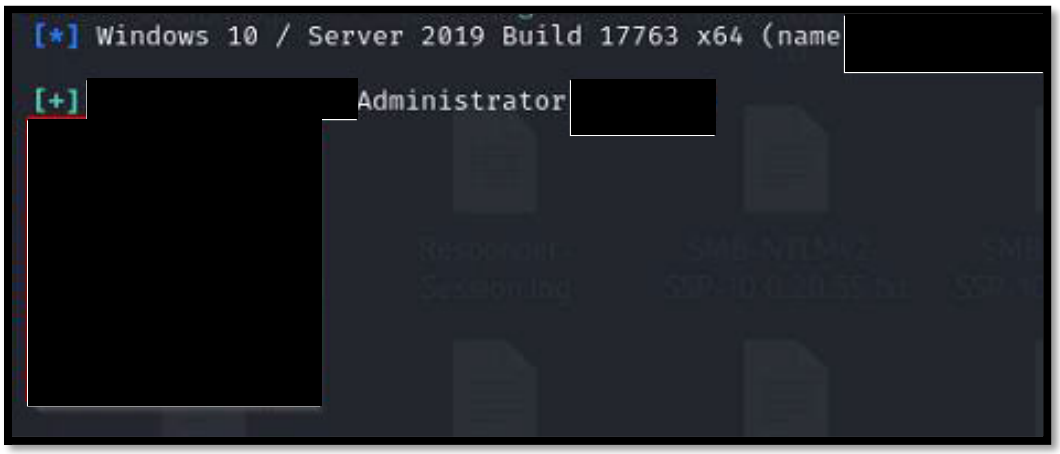
Following the identification that the credentials for the user Administrator were that of the domain administrator, Abacus Group engineers finished credentialed reconnaissance and began to move into credentialed exploitation throughout the environment. Abacus Group concentrated efforts on the domain controllers and associated servers to achieve maximum impact. The credentialed exploitation included the enumeration of active sessions, logged-on users, trusted and unconstrained delegations, ASREProasting, Kerberoasting, and SMB share access.



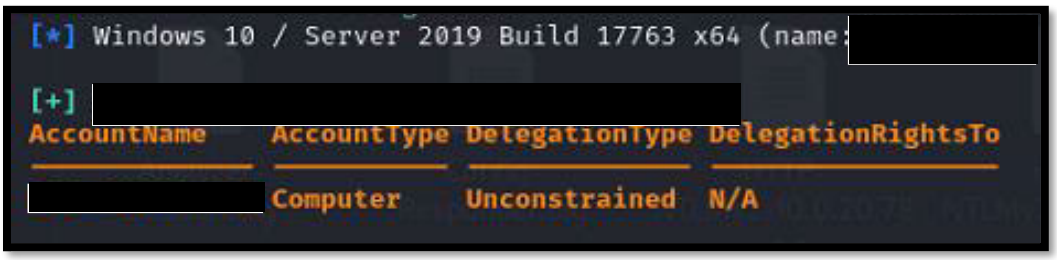
NetExec – Enumerating active sessions across the domain



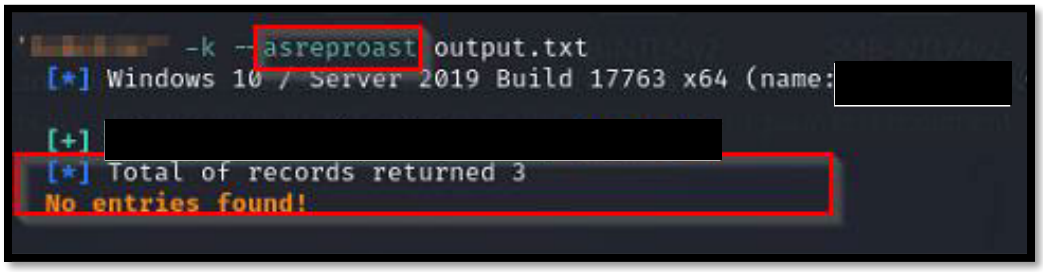
NetExec – Enumerating the logged-on users for [redacted] VM-DC



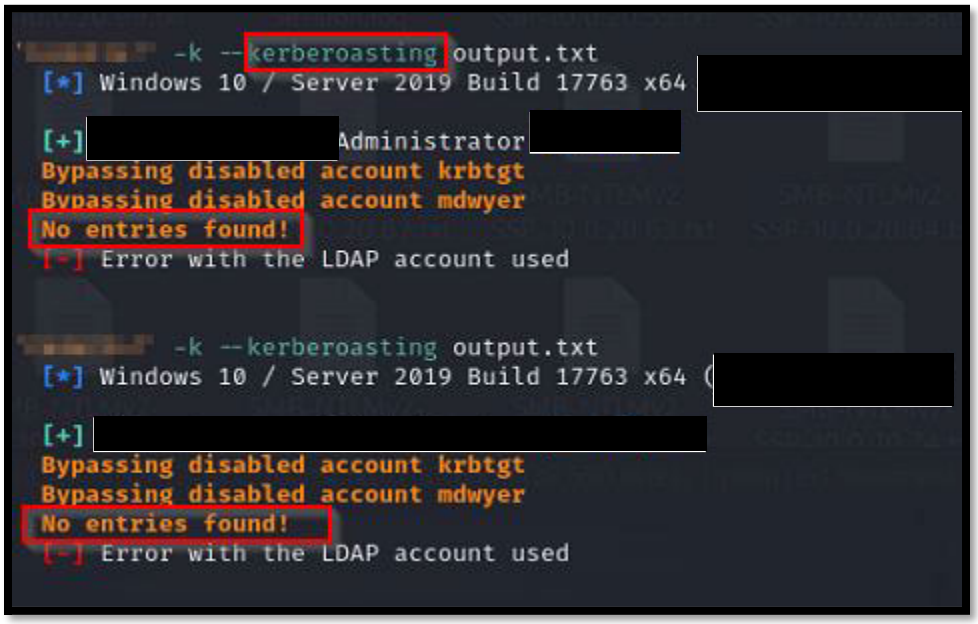
NetExec – Enumerating trusted delegations via [redacted] VM-DC



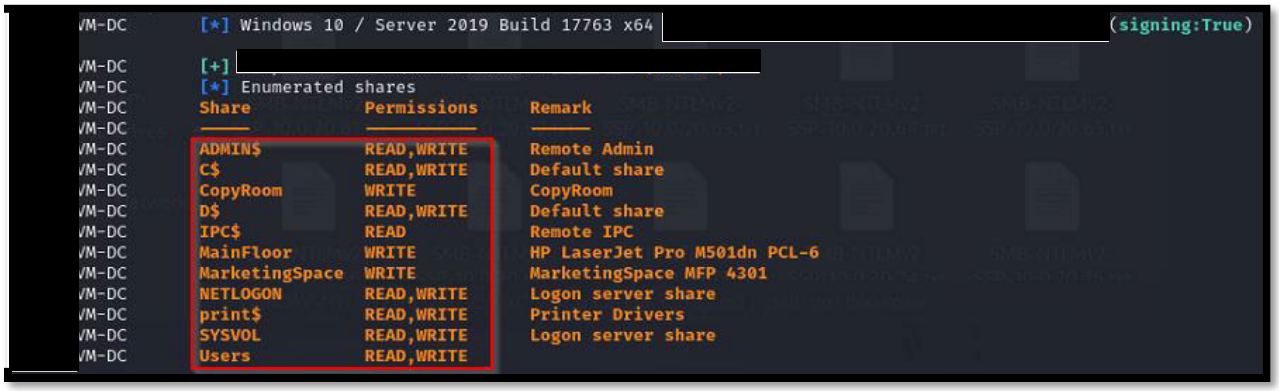
NetExec – Enumerating Unconstrained Delegation capabilities via [redacted] VM-DC



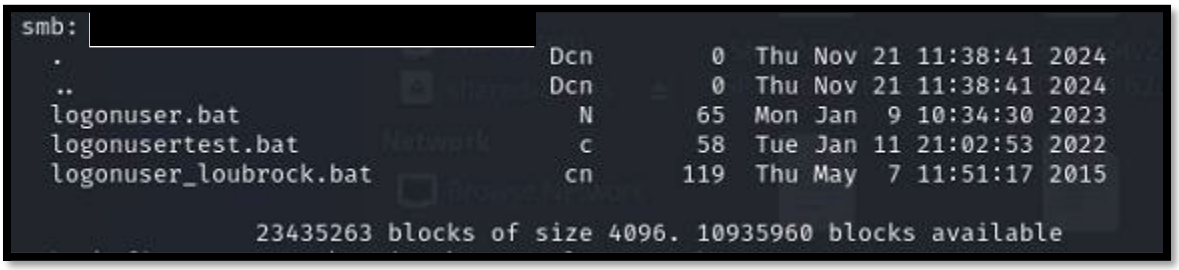
NetExec – Attempted ASREPROASTING via Administrator utilizing Kerberos authentication



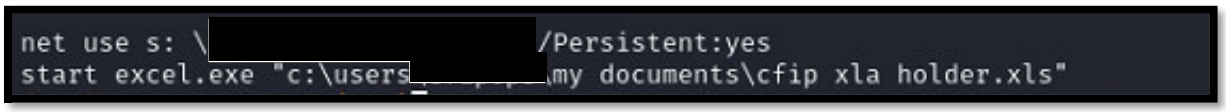
NetExec – Attempted Kerberoasting via Administrator utilizing Kerberos authentication



NetExec – Enumerating READ/WRITE access on VM-DC

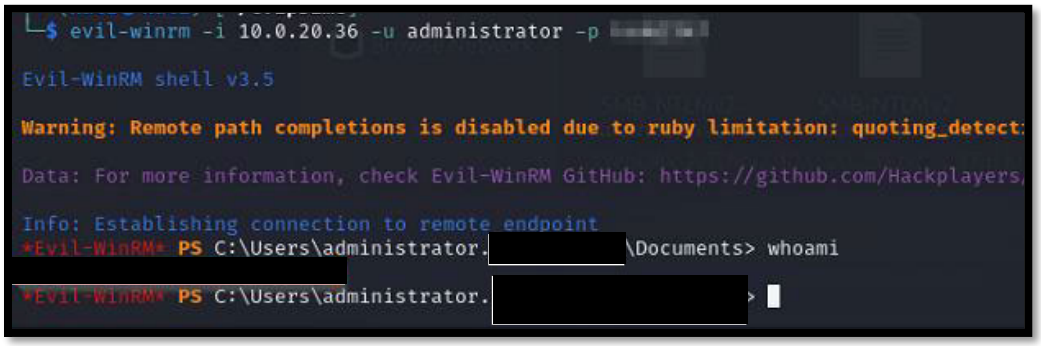


SMBCLIENT – Enumerating access of shares on VM-DC

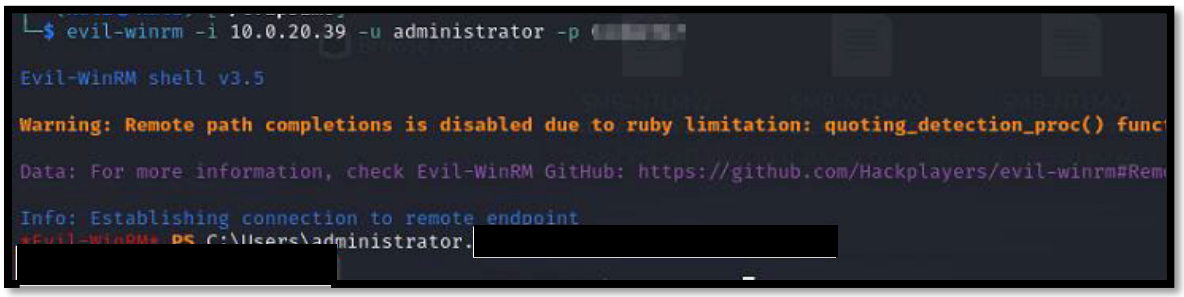


SMBCLIENT – Enumerating contents of logonuser_loubrock.bat

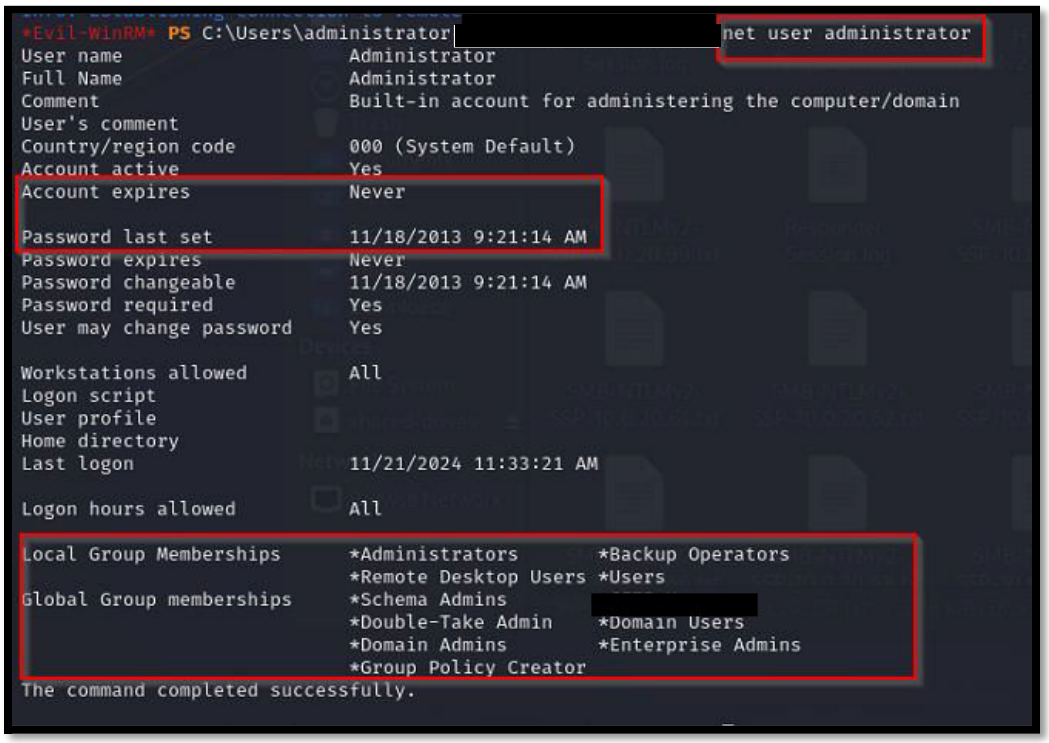
Abacus Group engineers finished credentialed exploitation and shifted into lateral movement within the environment. Abacus Group utilized tools such as Evil-WinRM, which operates off the ability to establish remote shell access via Windows Management Instrumentation (WMI) and Windows Remote Management (WinRM).



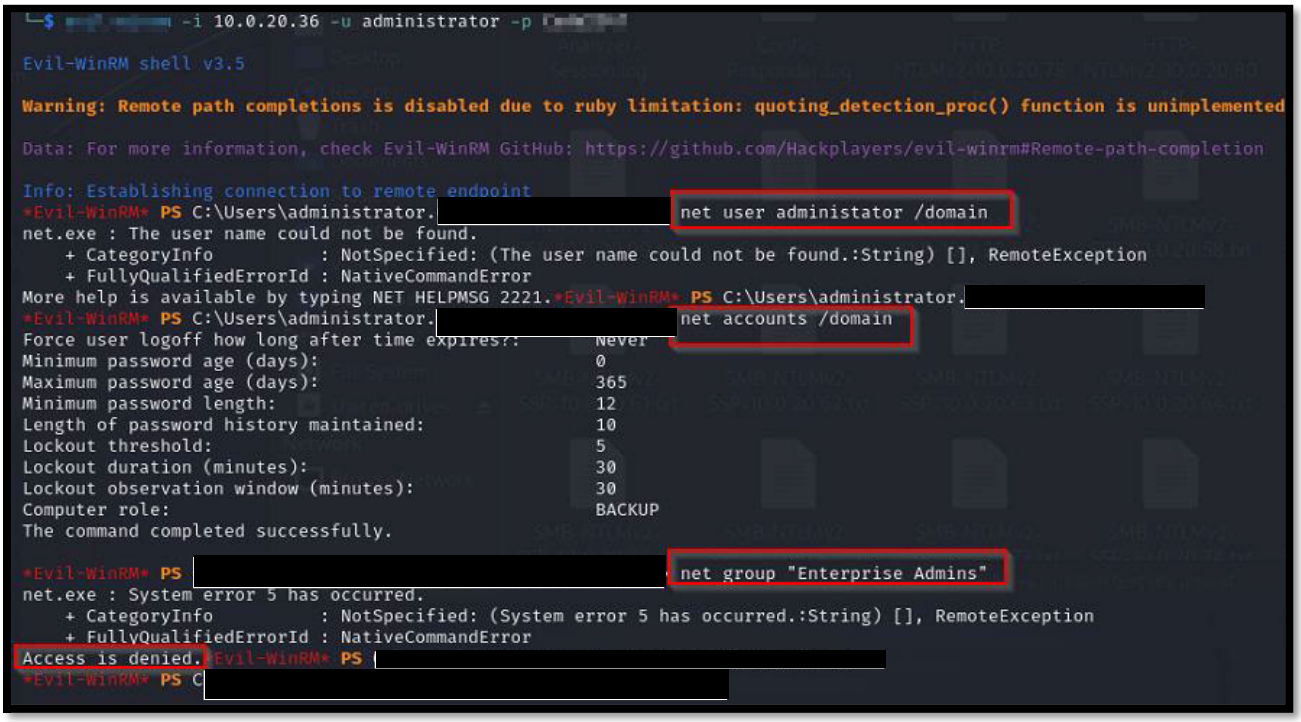
Evil-WinRM – Confirming lateral movement success utilizing user Administrator on [redacted] VM-DC



Evil-WinRM – Confirming lateral movement success utilizing user Administrator on [redacted] SV-AD

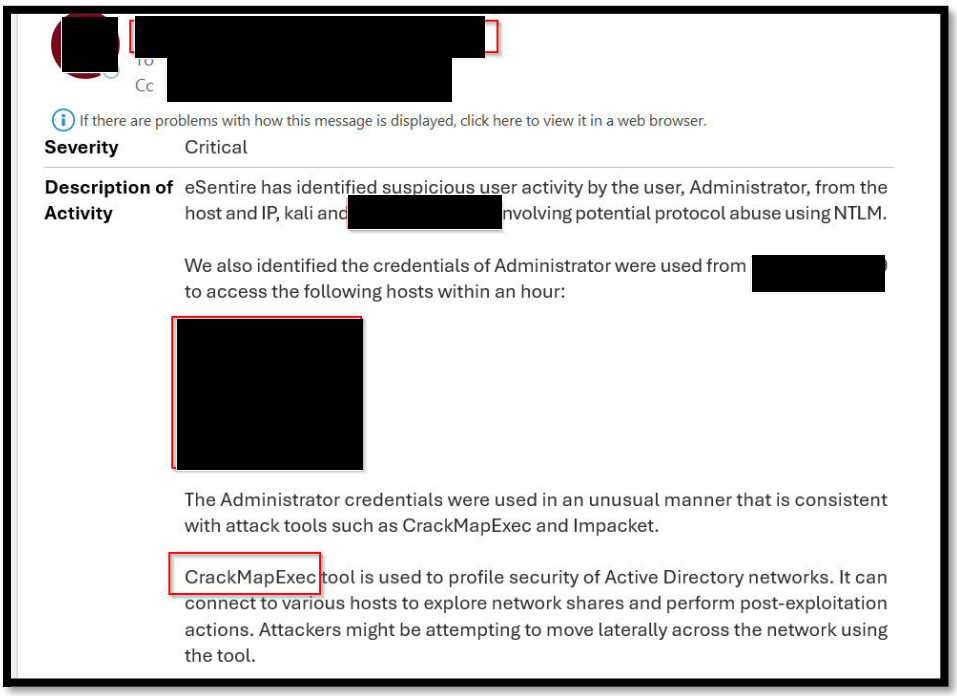


Evil-WinRM – Confirming user enumeration of Administrator

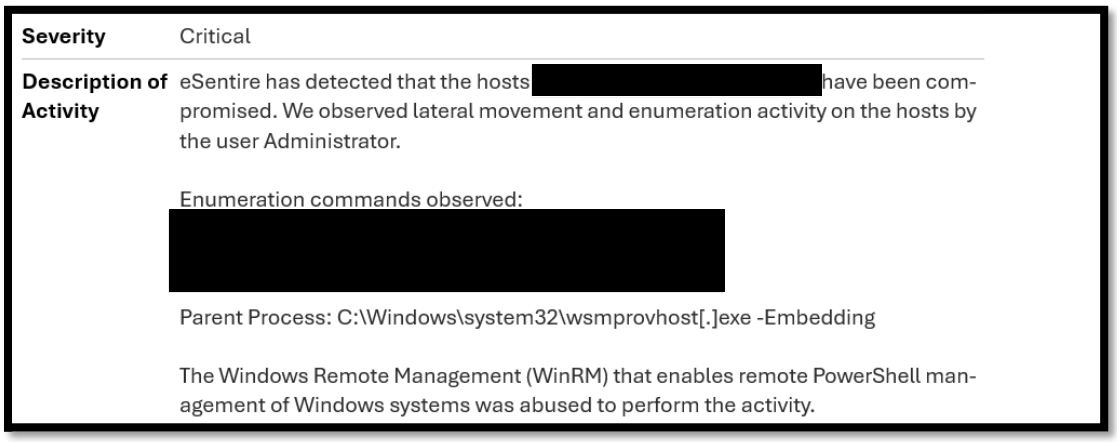


Evil-WinRM – Denying access for user Administrator

During the engagement, [redacted] security vendor reached out to [redacted] to confirm abnormal activity for the user Administrator. The security vendor identified that CrackMapExec, and Impacket were being utilized within the environment across multiple hosts via the security testing appliance IP address. Following this initial notification, a secondary notification was sent regarding lateral movement within the network utilizing the WinRM protocol.



Security Notification – Informing [redacted] of potentially suspicious activity



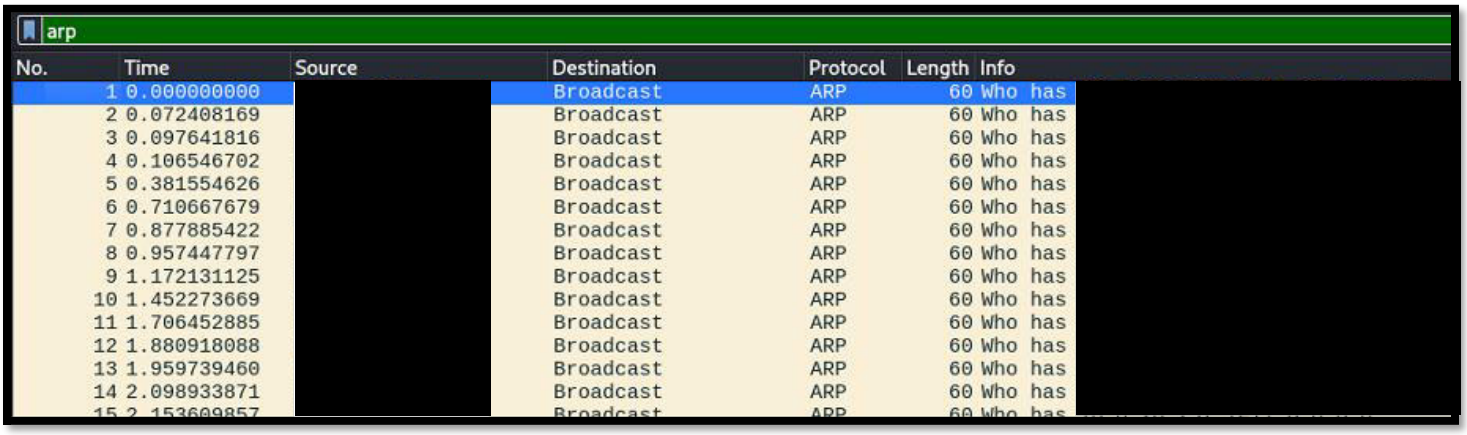
Security Notification – Informing [redacted] of potentially suspicious activity

After the security vendor alerted [redacted] of suspicious activity, Abacus Group engineers then attempted to pivot into the cloud since on-premises Active Directory methods had been detected. To do this, Abacus Group engineers attempted to utilize credentialed access from the user Administrator but were unsuccessful in this attempt due to the account being listed as locked out.

Microsoft Entra – Attempted login with the user Administrator

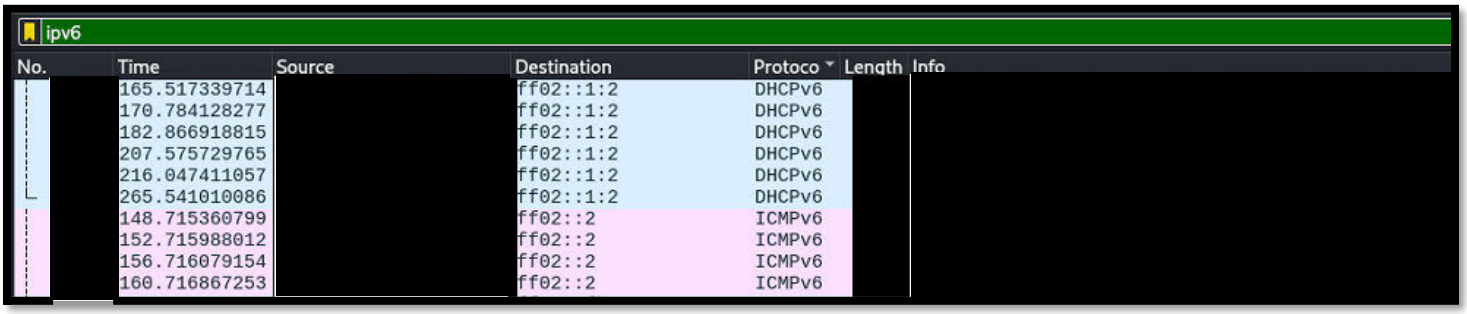
During this phase of testing, Abacus Group was able to demonstrate the ability to capture 11 NLTMv2 user hashes, resulting in the successful cracking of the hash for a domain administrator. With this, Abacus Group engineers operated within the [redacted] network with minimal detection. Once initial access was confirmed, Abacus Group was able to enumerate SMB shares and view files within them. Abacus Group attempted Kerberoasting, though this was unsuccessful in gathering information. Ultimately, once these common indicators of compromise were presented, Abacus Group was quickly locked out of the administrator account.

Continued analysis focused on identifying other forms of layer two traffic. Address resolution protocol (ARP) traffic was analyzed to determine the potential viability of VLAN hopping to bypass any identified network segmentation controls.



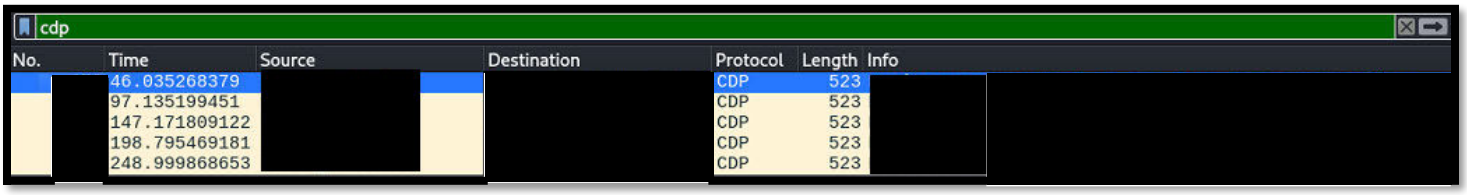
Analyzing ARP traffic via Wireshark

IPv6 traffic with a lack of first-hop security is a problematic networking vulnerability, as it introduces relatively easy attack vectors for malicious actors, such as leveraging IPv6 DNS takeover. It would be prudent for the security team to assess, from a white-box perspective, the configuration of such implemented security controls to ensure protection from common IPv6-based attacks.



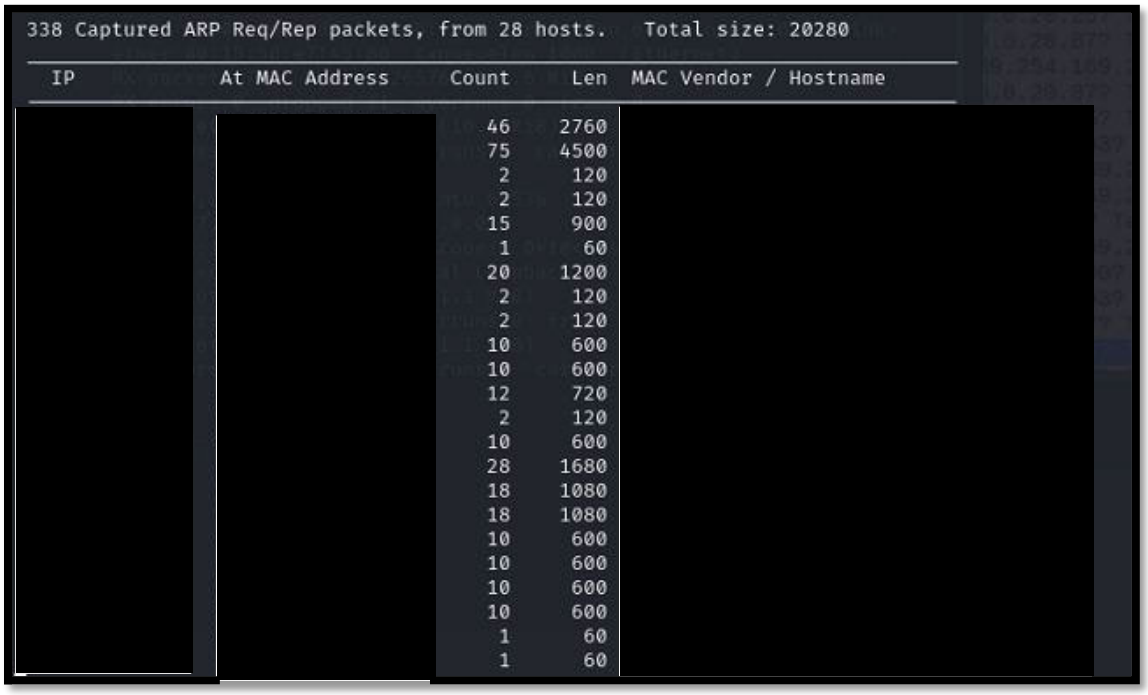
Analysis of IPv6 traffic via Wireshark indicated a dual-stack environment

Passive network analysis via Wireshark also identified the Cisco Discovery Protocol (CDP). The presence of these protocols is not indicative of a network vulnerability; however, it provided Abacus Group with the context that Cisco devices were used within [redacted] network.



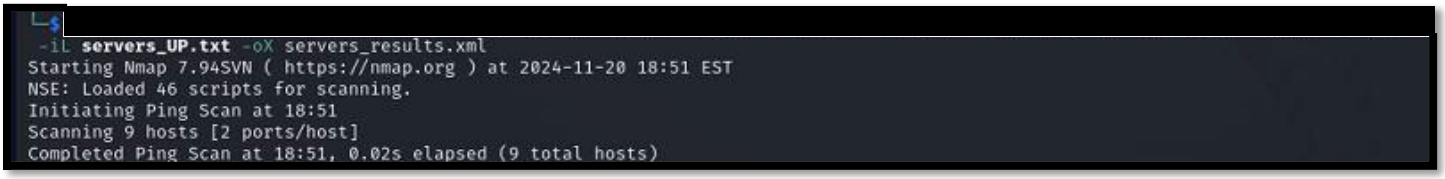
Passive network analysis via Wireshark identified CDP traffic

Next, Abacus Group systematically leveraged passive and active measures to map the internal attack surface. This reconnaissance began with a passive ARP scan of the local subnet to identify hosts for further analysis.



Passive ARP scanning via Netdiscover

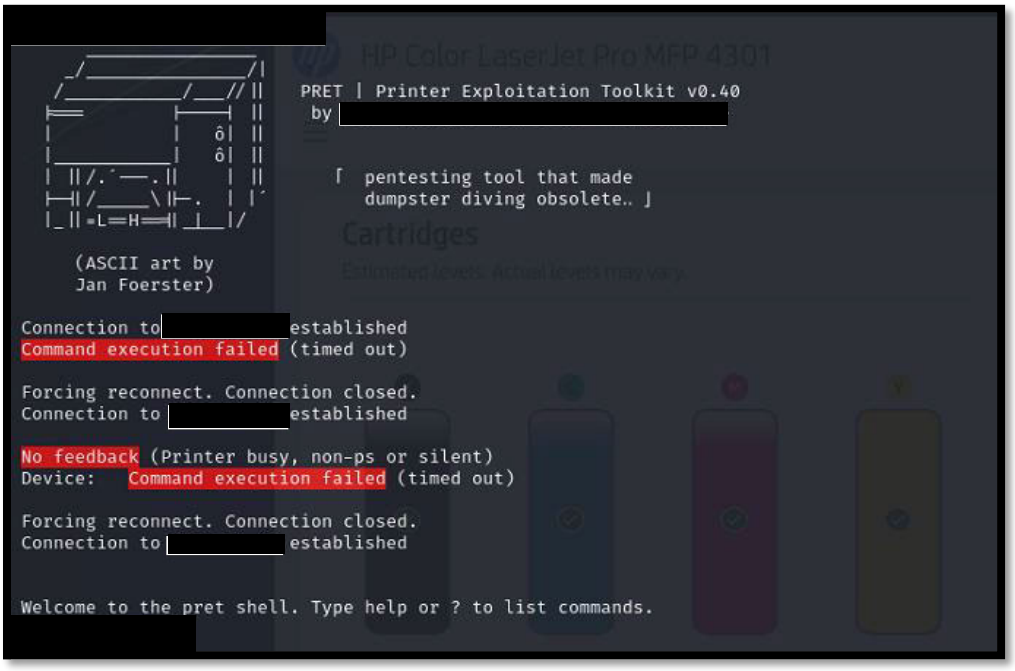
Once an initial understanding of the local VLAN was obtained, Abacus Group leveraged a highly obfuscated Nmap scan to gather information across the scope of systems on open ports and services, operating systems, and version information. This scan provided Abacus Group engineers a high-level view of the attack surface and allowed for the identification of systems and subnets to prioritize for deeper analysis using tools such as Legion, Nikto, Metasploit auxiliary modules, OpenVAS, and more. Once combined with these additional tools, a comprehensive attack surface mapping was established.



Nmap - Attack surface mapping and analysis

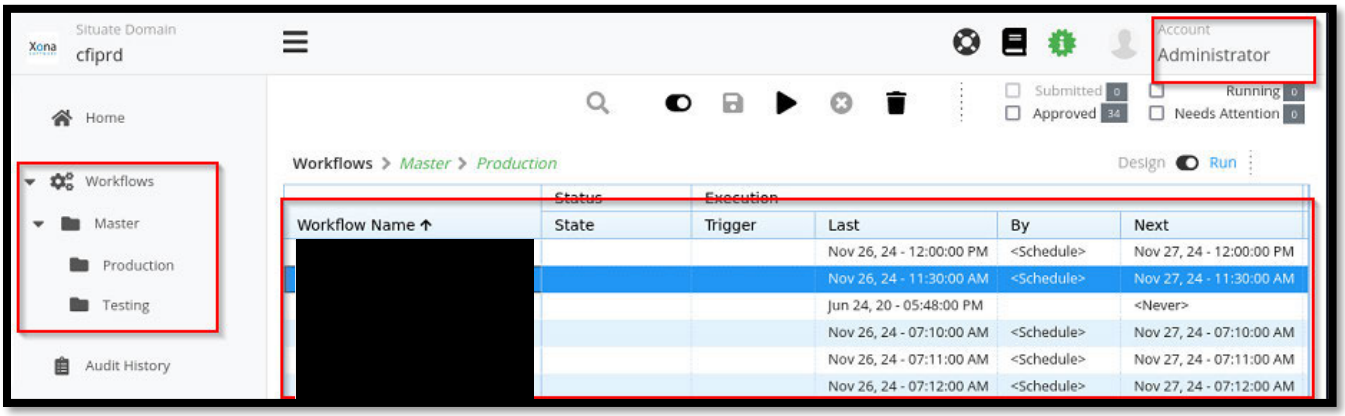
Further analysis into identified printers noted port 9100 (jetdirect) being open; this allowed Abacus Group to leverage an open-sourced tool called Printer Exploitation Toolkit to establish a remote connection to the device. This tool exploits features of several implemented printer languages (in this case, PJL), enabling system enumeration, denial of service attacks, configuration modification, and even limited directory traversal. This is possible because the jetdirect protocol prioritizes speed by stripping off any TCP/IP headers present in requests, allowing malicious print requests to be submitted directly in the applicable printer language. Abacus Group leveraged this tool to establish a limited shell connection, providing greater capabilities.

Some models of printers that leverage jetdirect are also susceptible to a path traversal vulnerability, which leverages jetdirect to gain arbitrary code execution by writing a shell script that is loaded on startup to /etc/profile. This exploit was attempted against 10.0.20.24 and 10.0.20.25 but was ultimately unsuccessful. While jetdirect was still exploitable in a limited capacity via pret.py, a greater killchain to maintain persistence was not established.



Demonstrating establishing a limited shell via PRET.py

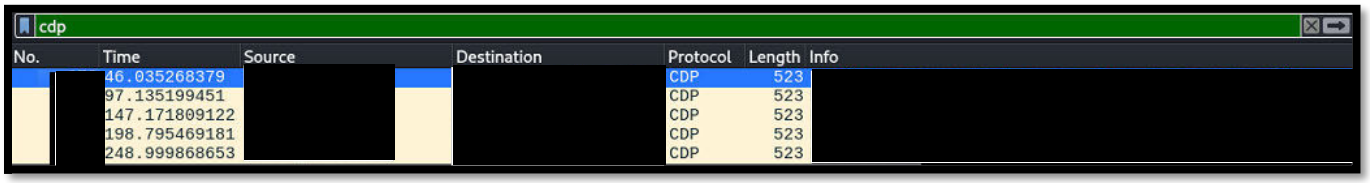
Abacus Group continued penetration testing by focusing on specific protocols and services that are often susceptible to manipulation, such as workflow automation and SSH. With regards to workflow automation, Abacus Group re-used user Administrator credentials to view automations within the environment. Furthermore, analysis of SSH protocols identified four devices running various versions of SSH, which are vulnerable to CVE-2024-6387, commonly known as regreSSHion.



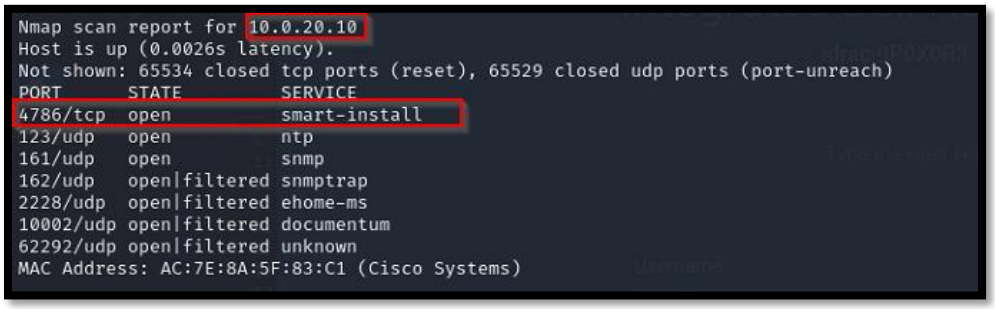
Situate – Accessing automations via credential re-use of Administrator on 10.0.20.34

SSH - Demonstrating likely vulnerability to CVE-2024-6387 commonly known as regreSSHion

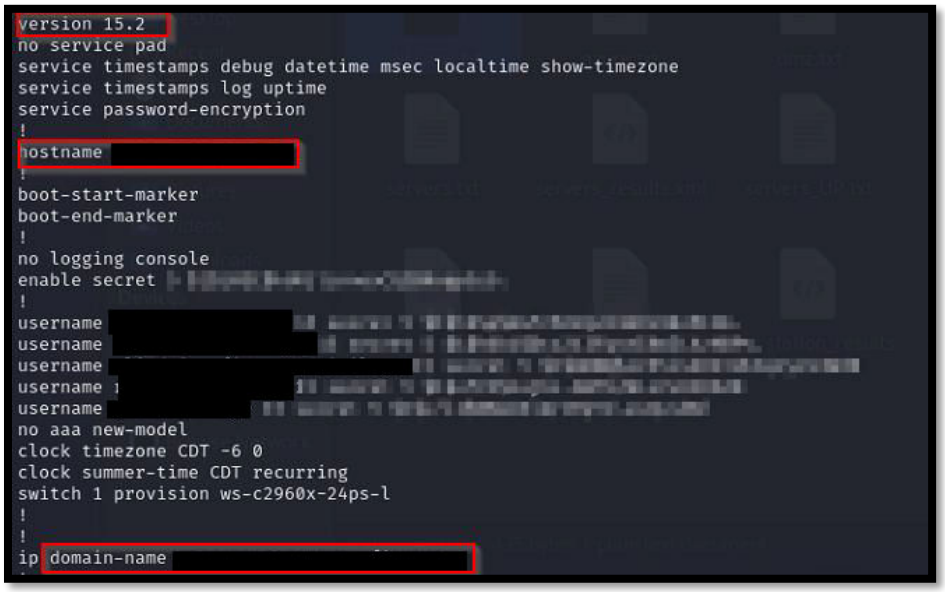
Abacus Group ultimately returned to an earlier observation, which was packet captures from the Cisco Discovery Protocol. This protocol showed that there was active Cisco infrastructure within the environment. Once the discovery of Cisco infrastructure was identified, further enumeration into this host showed the presence of Cisco Smart Install on multiple hosts. Cisco Smart Installer is a Cisco installer that is designed to automate the initial configuration and loading of an operating system image for new Cisco hardware. Further enumeration and execution utilizing the Smart Install Exploitation Tool (SIET) were leveraged to read network configuration files that led to the discovery of Cisco Privilege 15 hashed credentials.



Wireshark – Passive analysis of CDP within the environment



Nmap – Discovery of Cisco Smart Install on endpoint 10.0.20.10



SIET - Demonstrating successful exploitation and gathering of Cisco Privilege 15 password hashes

Throughout the comprehensive internal network penetration testing conducted by Abacus Group, numerous attack vectors were meticulously identified and rigorously tested. After exhausting all viable in-scope attack avenues, the testing activities were successfully concluded. The assessment revealed three high-risk findings, five moderate-risk findings, and three low-severity risk findings, each of which has been documented for further action.

Social Engineering Reconnaissance

Social engineering reconnaissance began by leveraging a variety of tools to collect employee information and identify possible login portals for exploitation and spoofing, and then build target lists. Abacus Group first began collecting employee information through social media sites, such as LinkedIn, by sending connection requests and viewing profiles belonging to individuals in departments such as finance, legal and human resources. Abacus Group used a sock puppet account named Sebastian Schtigletz to connect with various [redacted] employees. Abacus Group sent connection requests to numerous employees with no message body or context.

For social engineering reconnaissance, profiles on LinkedIn were analyzed to gather the following information:

- List of company employees
- Confirmation of employment
- Employee's full name
- Employee position/title
- Employee tenure
- Employee geographical location
- Organizational hierarchy
- Potential access to specific confidential systems

Abacus Group's controlled sock puppet LinkedIn user

LinkedIn – Out of the numerous sent connection requests, only one was accepted

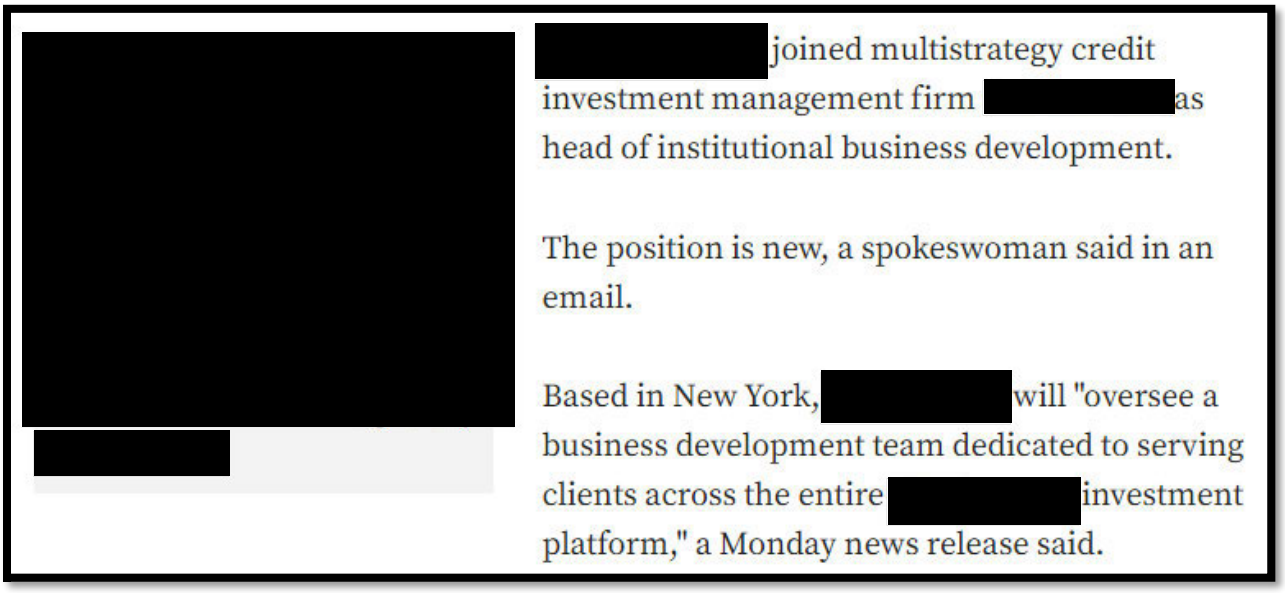
Abacus Group continued social media reconnaissance by analyzing job and media posts to obtain information that could be leveraged in the campaigns. During this phase of reconnaissance, Abacus Group identified key information that was subsequently leveraged in the social engineering campaigns.

First, Abacus Group identified a strategic partnership with an organization known as The Academy Group. This relationship was more closely examined, and it was identified that [redacted] supports The Academy Group's mission by assisting financially. Frequently, malicious actors look to exploit these relationships as there is an established trust between the two organizations. [redacted] and The Academy Group should be aware that malicious actors may attempt wire fraud or other financially motivated social engineering campaigns due to the type of relationship. Abacus Group devised a campaign that sought to take advantage of this strategic partnership, specifically involving finances. More information can be seen in Social Engineering Campaign 3.

Analyzing the strategic partnership between [redacted] and The Academy Group

Abacus Group continued OSINT by analyzing new articles, general media posts, and more. Abacus Group sought to continue to understand more about [redacted] and those who worked at the organization. Abacus Group successfully identified additional information through this phase of the engagement and through what had been uncovered in the external network penetration testing portion of the engagement.

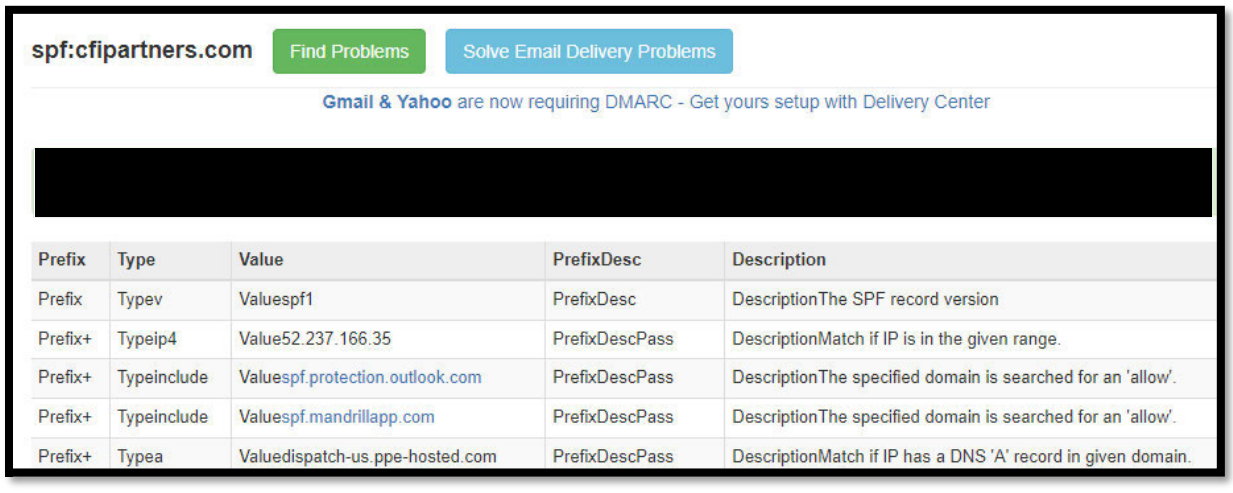
Job posting analysis led to the identification of an email, which provided Abacus Group with the email syntax



Demonstrating media analysis for an assessed former employee of [redacted]

Abacus Group then looked for login portals related to [redacted] information systems. This stage of the reconnaissance process aimed to identify any portals that could be spoofed and then subsequently used to harvest credentials during the social engineering campaigns. A common tactic employed by malicious actors is to spoof a user login portal with the goal of luring employees to a malicious portal through email or other communication. A direct login portal was identified during subdomain enumeration as being associated with [redacted] However, this portal is for investors and was thus deemed as out of scope. Abacus Group identified the use of Office 365 through mail record analysis, which was subsequently used for campaign creation.

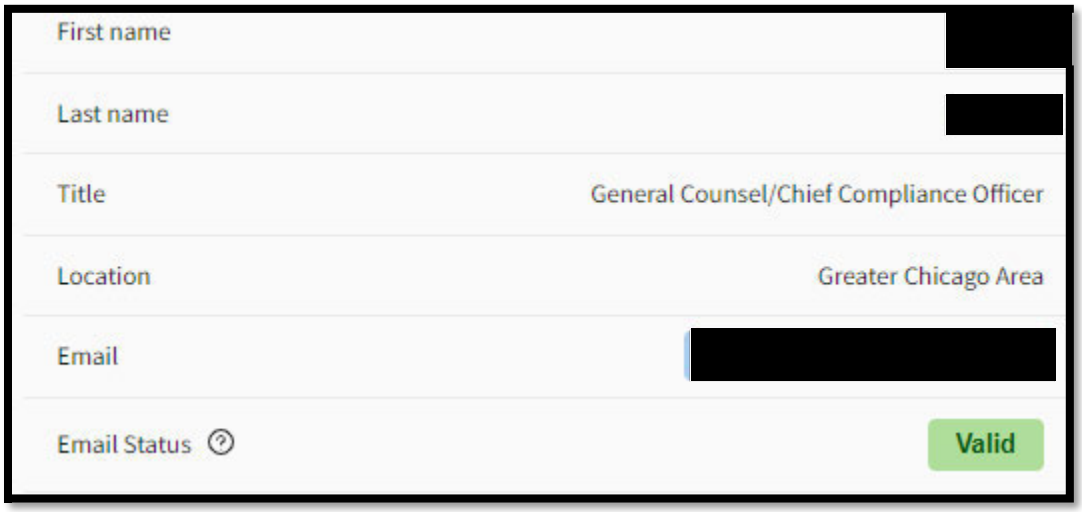
Demonstrating the investor portal



Prefix	Type	Value	PrefixDesc	Description
Prefix	Typev	Valuespf1	PrefixDesc	DescriptionThe SPF record version
Prefix+	Typeip4	Value52.237.166.35	PrefixDescPass	DescriptionMatch if IP is in the given range.
Prefix+	Typeinclude	Valuespf.protection.outlook.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix+	Typeinclude	Valuespf.mandrillapp.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix+	Typea	Valuedispatch-us.ppe-hosted.com	PrefixDescPass	DescriptionMatch if IP has a DNS 'A' record in given domain.

Demonstrating the use of Office 365 via the mail records

With an outline of possible social engineering campaigns, Abacus Group transitioned to creating target lists tailored to each campaign. A list of employee emails was constructed using a set of scripts, including Linkedin2username and Skrapp.io, both of which scrape LinkedIn data. This analysis was paired with manual validation and then screened using a set of email verification techniques. Through completely blind analysis, Abacus Group was able to produce a list of 45 employee email addresses. Abacus Group was provided with a complete list of email addresses from the project [redacted] which contained 49 email addresses.

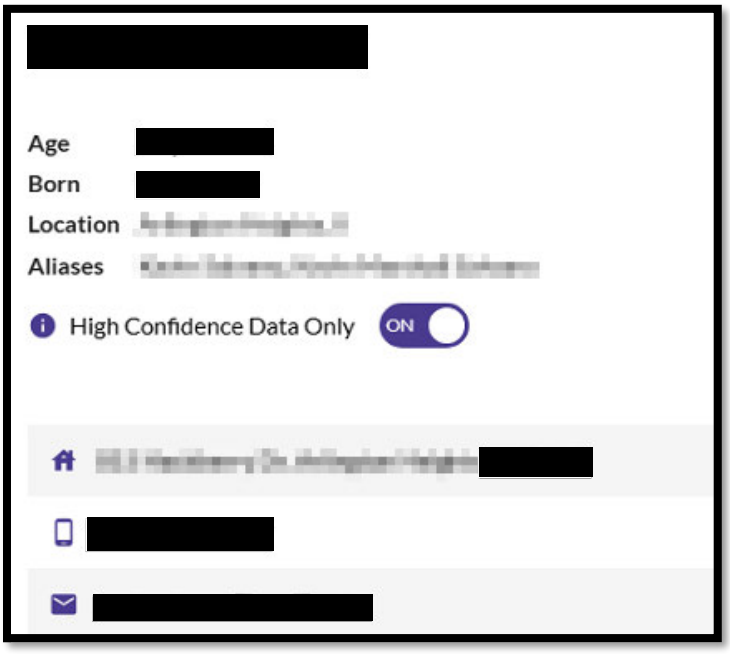


Demonstrating the identification of an employee email address with Skrapp.io

Further information was compiled on individuals using services such as pipl.com, whitepages.com, and truepeoplesearch.com. These resources are commonly used for reverse phone number lookups and general "people searching". Abacus Group used the information gathered to aggregate a list of possible cell phone numbers for select [redacted] employees.

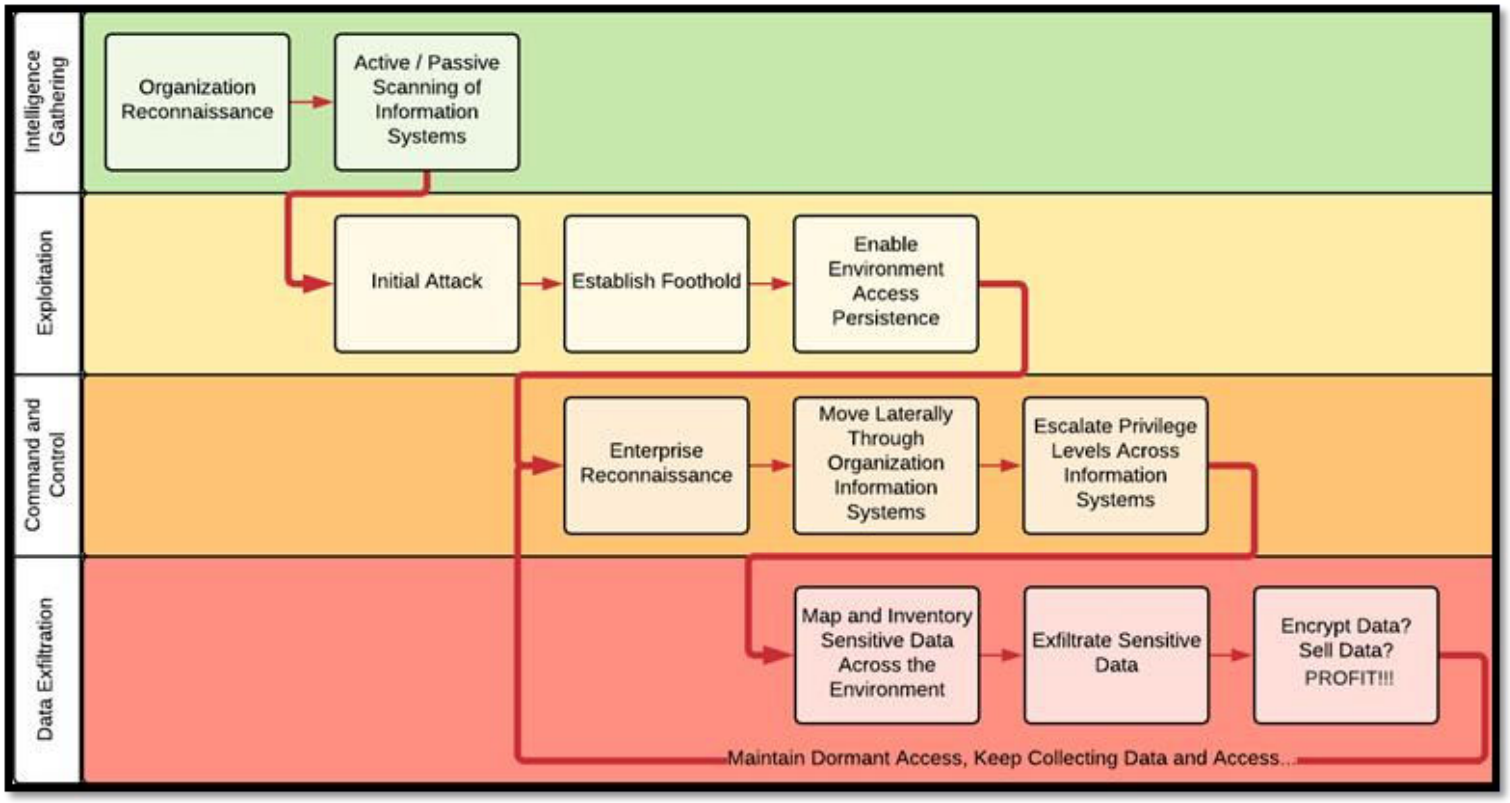
It is worth noting that Abacus Group was provided with a complete list of cell phone numbers by the project [redacted] This was requested only after proof of concept had been shown to the project [redacted] Additionally, this information was requested due to time limitations and to ensure accuracy in possible vishing or smishing campaigns. Given enough time and resources, it is highly likely that a malicious actor would be able to compile a list of work and/or mobile numbers for members of [redacted] Abacus Group leveraged 47 personnel's mobile numbers in a smishing campaign. Finally, [redacted] should consider data sanitization services like OneRep or DeleteMe for the organization. Services such as these scrub publicly available data, which limits what is exposed to possible malicious actors.

Abacus Group leveraged the email contained within the bio of the individual who connected with the sock puppet account to search for additional contact information



Using the aforementioned email address, Abacus Group identified complete information about the target with a service known as BeenVerified

Having analyzed the aggregate of all collected information, Abacus Group crafted a social engineering strategy with multiple distinct campaigns designed to test both end-user security awareness and the technical controls in place. Four separate social engineering campaigns were executed to closely emulate a malicious actor of moderate sophistication attempting to monetize an attack against [redacted] Abacus Group utilized custom campaigns that were in alignment with the most current and prevalent social engineering campaigns being used by malicious actors. In doing so, Abacus Group purchased two domains, [redacted] and [redacted], which were used to create an impersonated email account and host controlled phishing portals. These campaigns followed a malicious actor's typical ransomware attack process, as illustrated below.



Social Engineering Campaign 1: O365 Password Spray + Credential Stuffing with MFA Bypass

Targets: All identified and approved staff
Campaign Execution Date: November 22nd – December 6th. The spray was not executed from November 27th to 29th in observance of Thanksgiving.
Objective: Identify target Office365 credentials and bypass MFA.
Compromised Employees: 0

Summary: Password spraying is a type of social engineering campaign where Abacus Group leveraged particularly insecure passwords, like [redacted], against all approved targets. Each user account had only one login attempt per iteration, which made the risk of accidentally locking out any users very unlikely. Another feature of this campaign was leveraging previously breached credentials in Credential-Stuffing attempts. In the event that Abacus Group was able to successfully identify a password, an attempt to log in with those credentials, including bypassing any MFA, would be executed.

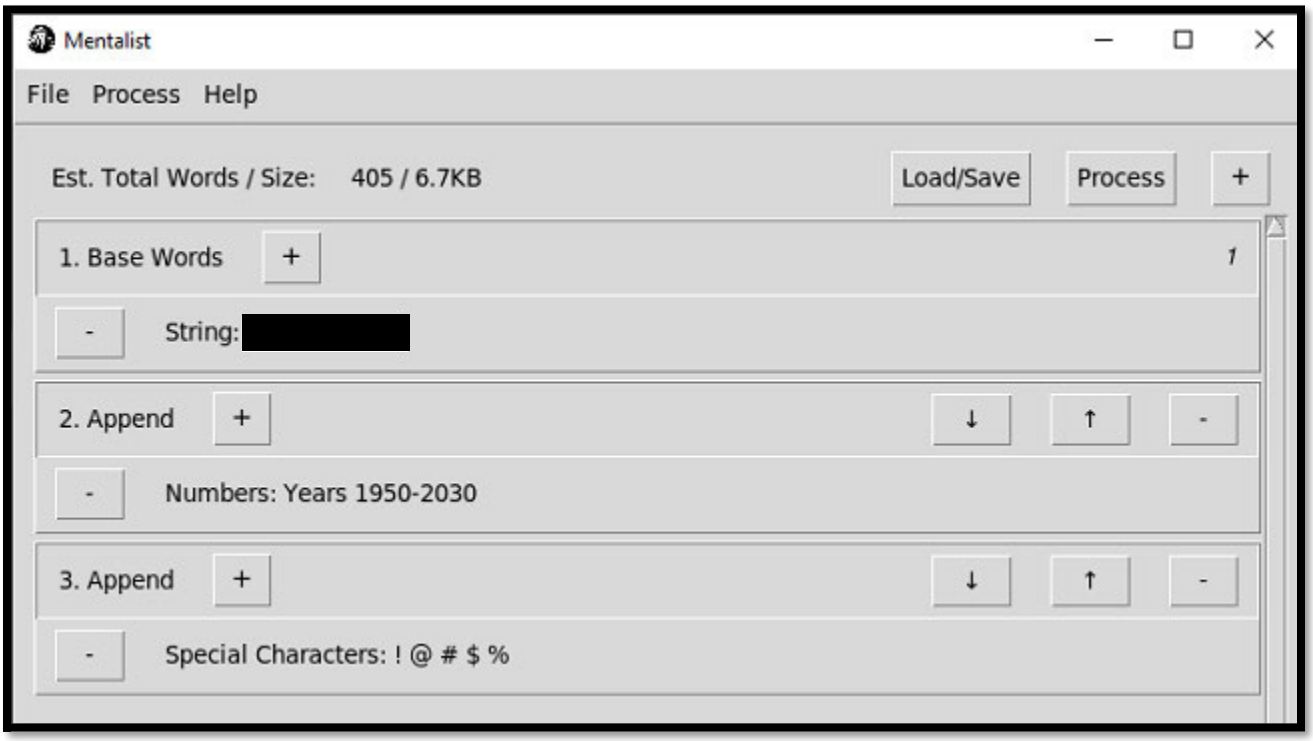
Results: This campaign did not result in the full compromise of any identified staff members. This exercise demonstrated the likelihood that [redacted] staff generally have robust passwords. While this may be true, Abacus Group still recommends the implementation and enforcement of a password policy as a security best practice (should one not already be in place). This includes not permitting the use of easily guessable passwords like [redacted]

Finally, while Abacus Group did identify previously breached credentials, none were attempted in credential stuffing attacks. One breached credential belonged to an assessed former employee, and all of the passwords would not have met general complexity requirements. Still, it is important to note that password reuse should be prevented as this could allow malicious actors to identify previously breached credentials and attempt them in other login portals.

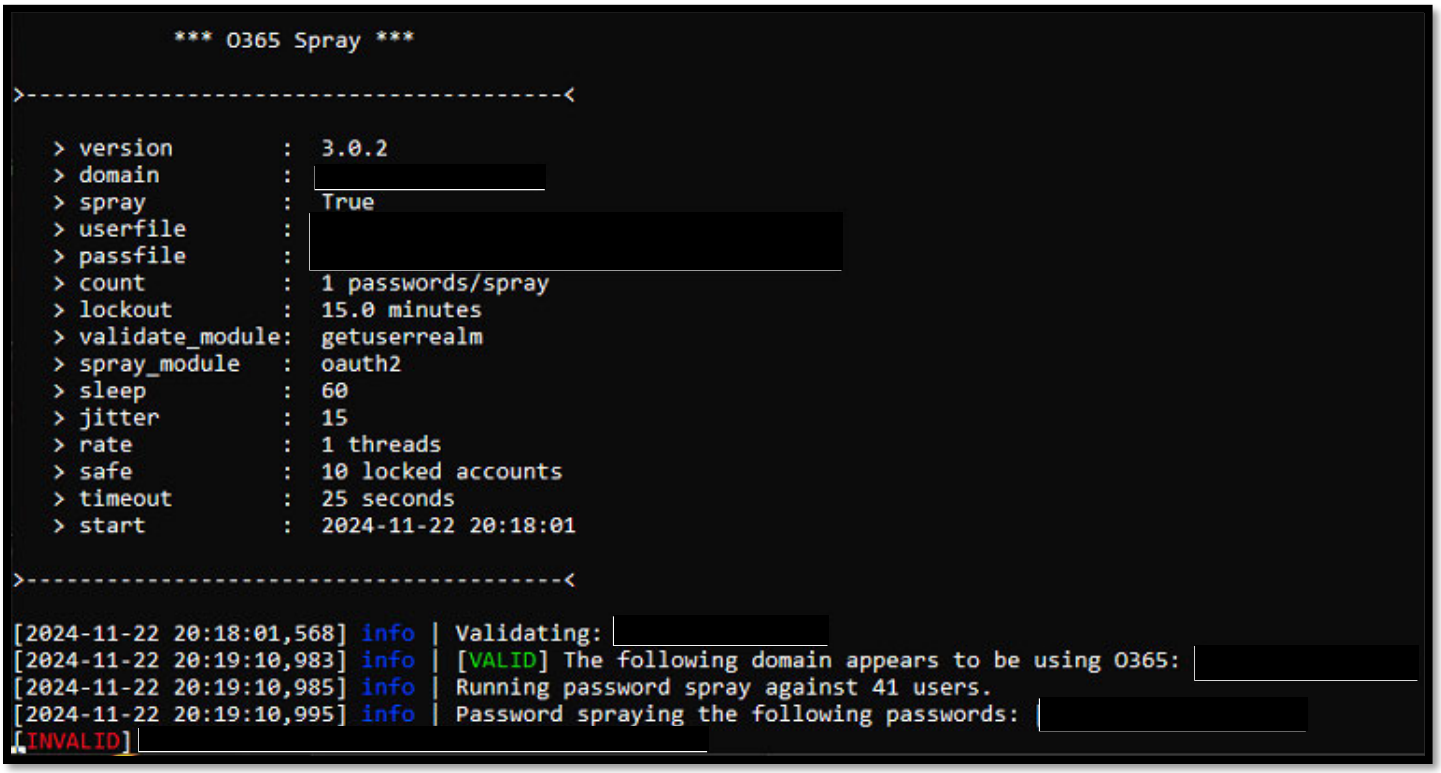
A brief narrative, with a selection of some of the passwords used, can be seen below.

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

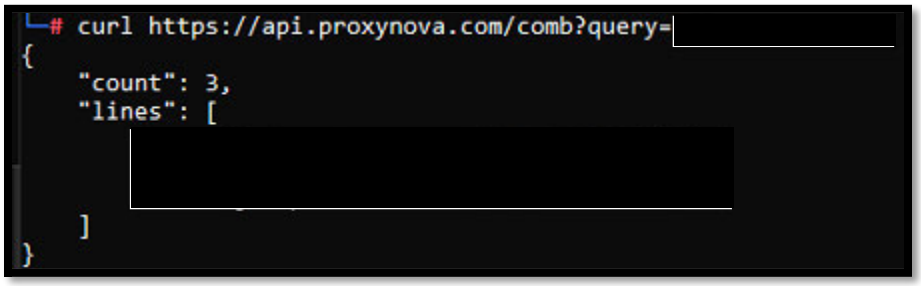
An example of some of the passwords attempted



Mentalist – Creating an insecure password list for the spray



O365 Spray – An example of the spray in action



Demonstrating previously breached credentials, which did not meet general password complexity requirements

Social Engineering Campaign 2: SMS Phishing (Smishing)

Targets: All identified and approved staff
From: Abacus Group controlled phone numbers
Campaign Execution Date: November 26th
Objective: Harvest target credentials and bypass MFA via an Office365 login portal.
Compromised Employees: 1

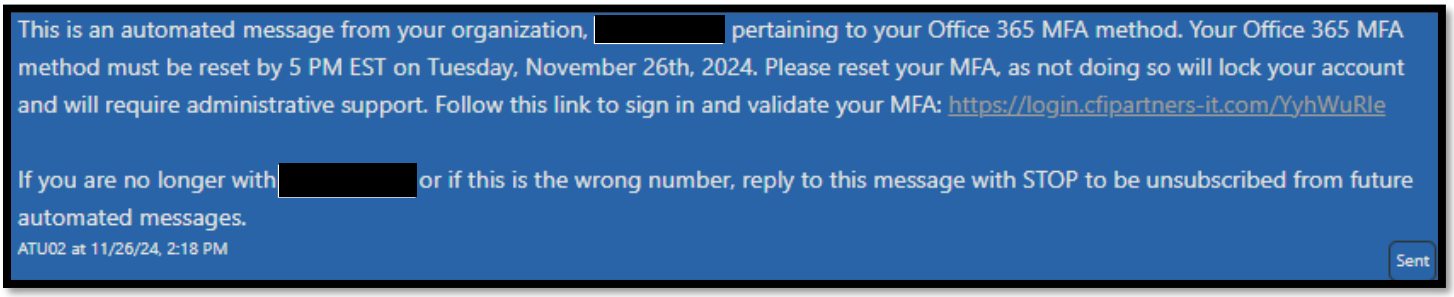
Summary: Abacus Group sent a smishing message to all identified and approved staff. Specifically, the smishing message informed targets that they would need to validate their MFA details in Office 365. To validate these details, targets would be directed to an Office 365 phishing portal, which was controlled by Abacus Group. Leveraging the phishing portal, Abacus Group would attempt to harvest user Office 365 details and bypass MFA.

Results: This campaign resulted in the full compromise of one [redacted] staff member. Abacus Group was able to successfully harvest this target's Office 365 credentials and bypass MFA. Through this access, Abacus Group was able to access the target's OneDrive, Outlook email, Teams environment, and much more. Abacus Group identified sensitive material that could have been leveraged in follow-on attacks, such as extortion-based attacks. Furthermore, and possibly even more severe, Abacus Group could have executed a Business Email Compromise or BEC attack. This type of attack would have leveraged access to the target's email. Abacus Group could have crafted an email directed at external investors in an effort to steal money. Furthermore, with access to the target's email and Teams environment, Abacus Group could have sent malicious messages or more sophisticated social engineering campaigns to both external and internal personnel. This level of access could have had a severe impact on [redacted] reputation, internal information, and even external and internal personnel.

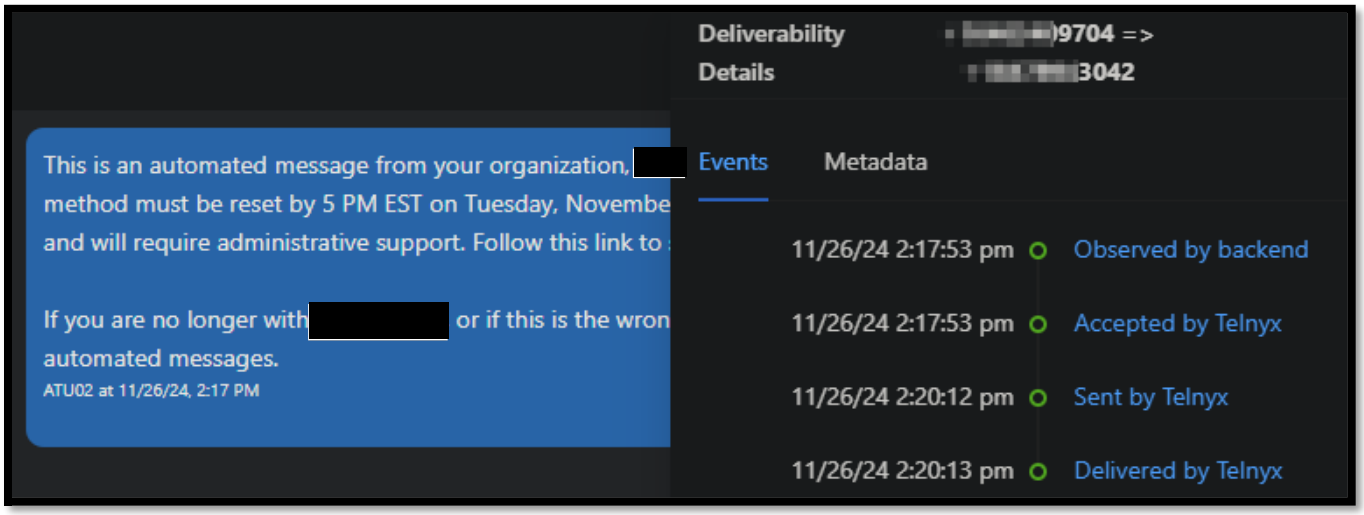
While the above could have been possible, it is important to recognize other elements that stemmed from this campaign. First, numerous other users reported this campaign either to the project PoC, the organization's system administrator, or the organization's helpdesk. Second, the target who was compromised reported the compromise to the organization's system administrator. The password was subsequently changed, and the session was revoked. Abacus Group had roughly an hour of active time before losing access. Both of the aforementioned elements of this campaign demonstrate end-user security awareness and a relatively swift response to triaging this compromise. It should also be noted that Abacus Group first attempted to establish persistence with an additional form of multi-factor authentication (MFA); however, this was unsuccessful. Additional security measures were needed prior to being able to change a password or add alternative forms of MFA. This demonstrates a strong internal configuration, which would limit the ability of a malicious actor to remain within the compromised environment.

Finally, it is Abacus Group's recommendation that [redacted] consider additional conditional access policies in Office 365. Abacus Group was able to bypass MFA through a successfully timed DUO push notification. The target was expecting the DUO push after credentials had been entered into the controlled phishing portal, at which point Abacus Group entered the Office 365 credentials and triggered the push notification. After the confirmation of the push notification, Abacus Group was able to simply authenticate to the target's Office 365 environment. [redacted] should consider conditional access policies that are device or network based. This way, even if MFA is bypassed, full authentication is not possible as the device or network based conditions would not be met. More information can be found in the Risk Details section, where Abacus Group outlines additional policies that can be considered.

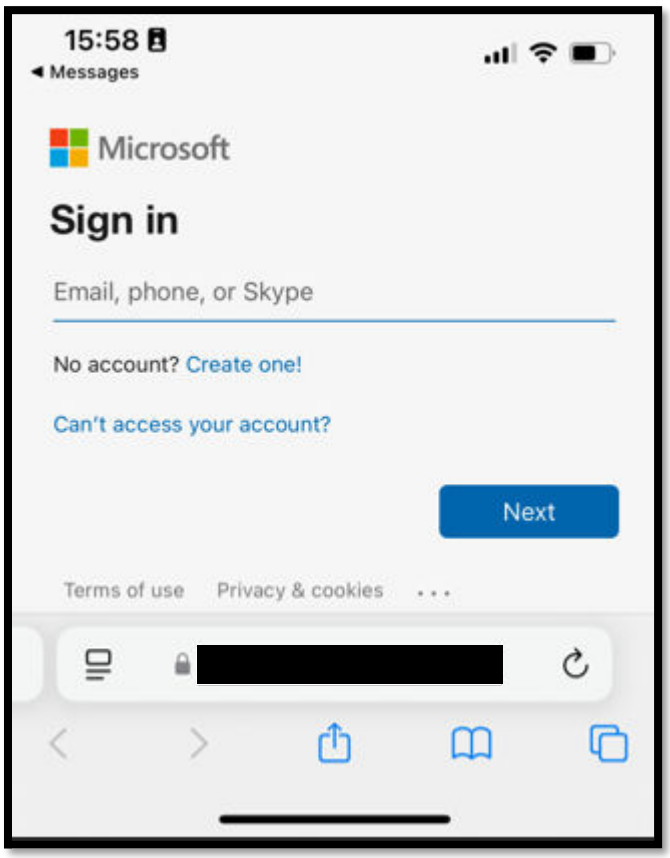
A brief narrative of evidence can be found below.



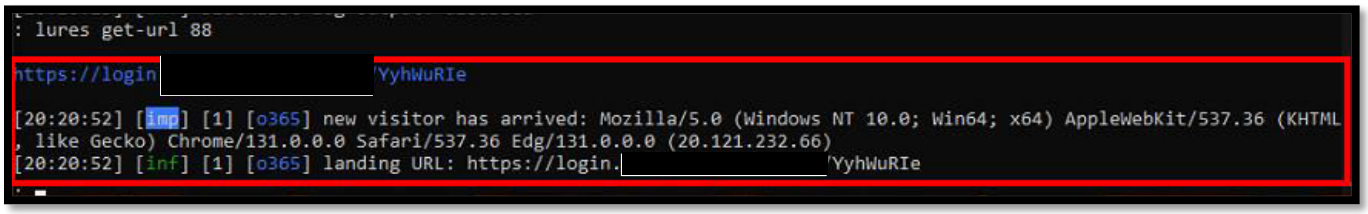
Demonstrating the text message that was sent to all staff



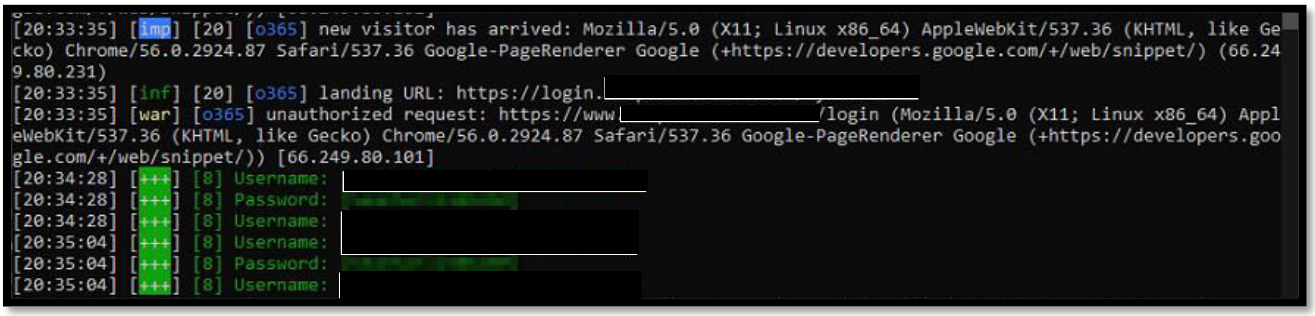
Demonstrating the delivery of the smishing message



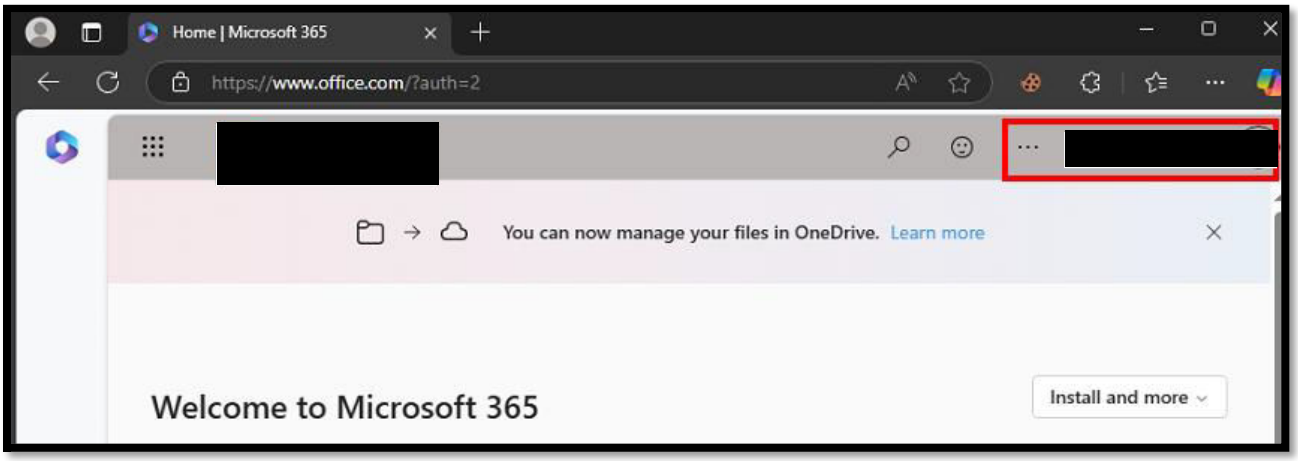
Demonstrating the login portal as seen through the Safari browser on iOS



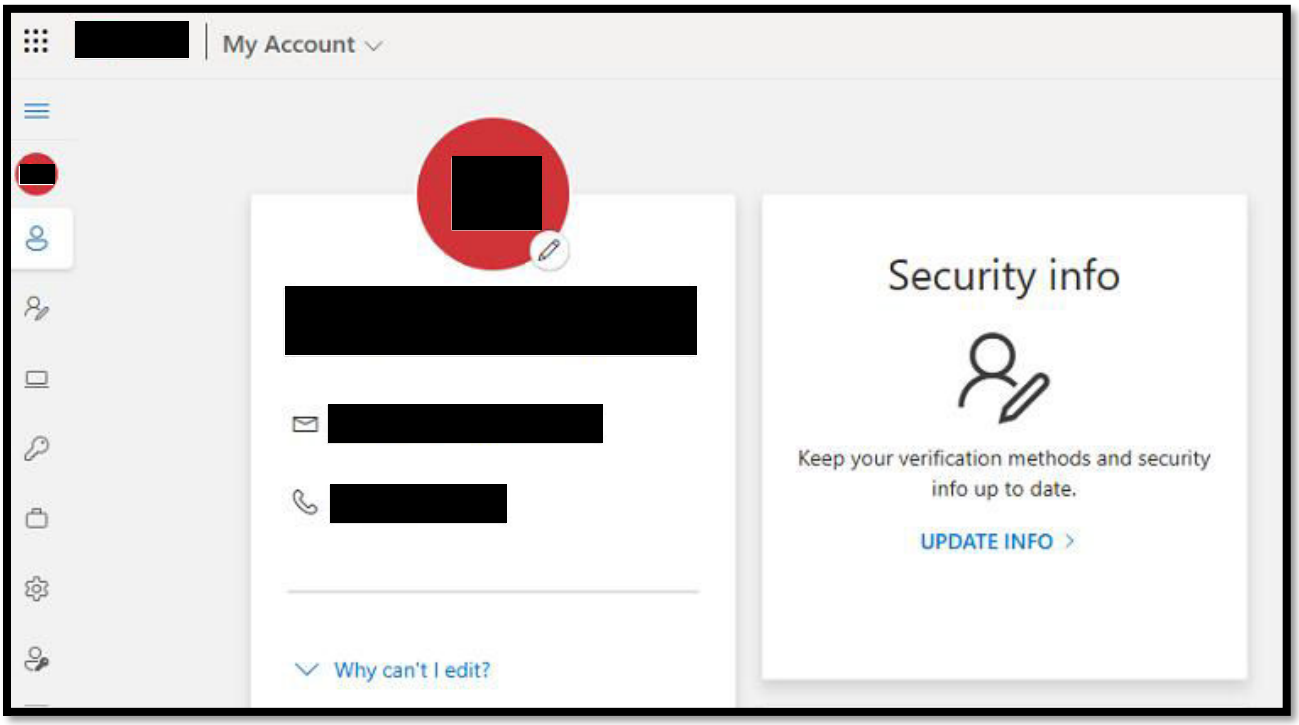
Evilginx – Creating the lure and monitoring for activity



Evilginx – Capturing the target's credentials, which were entered numerous times

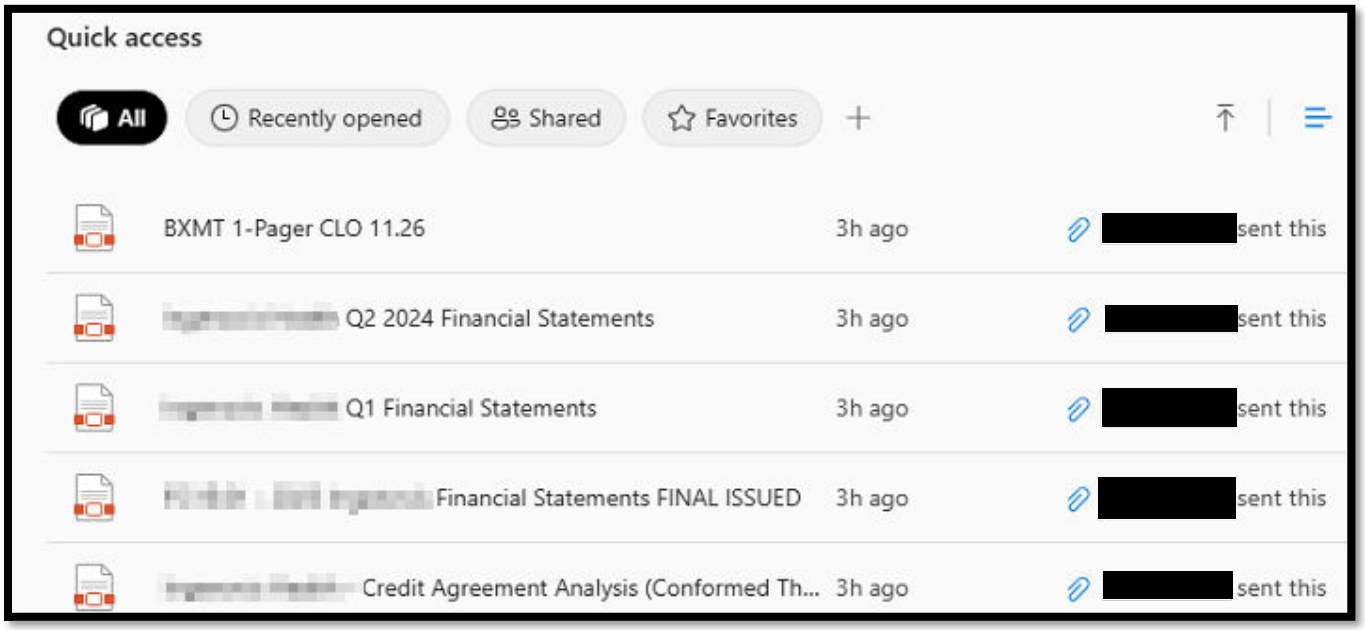


Authentication to the target's Office 365 environment after having successfully bypassed MFA



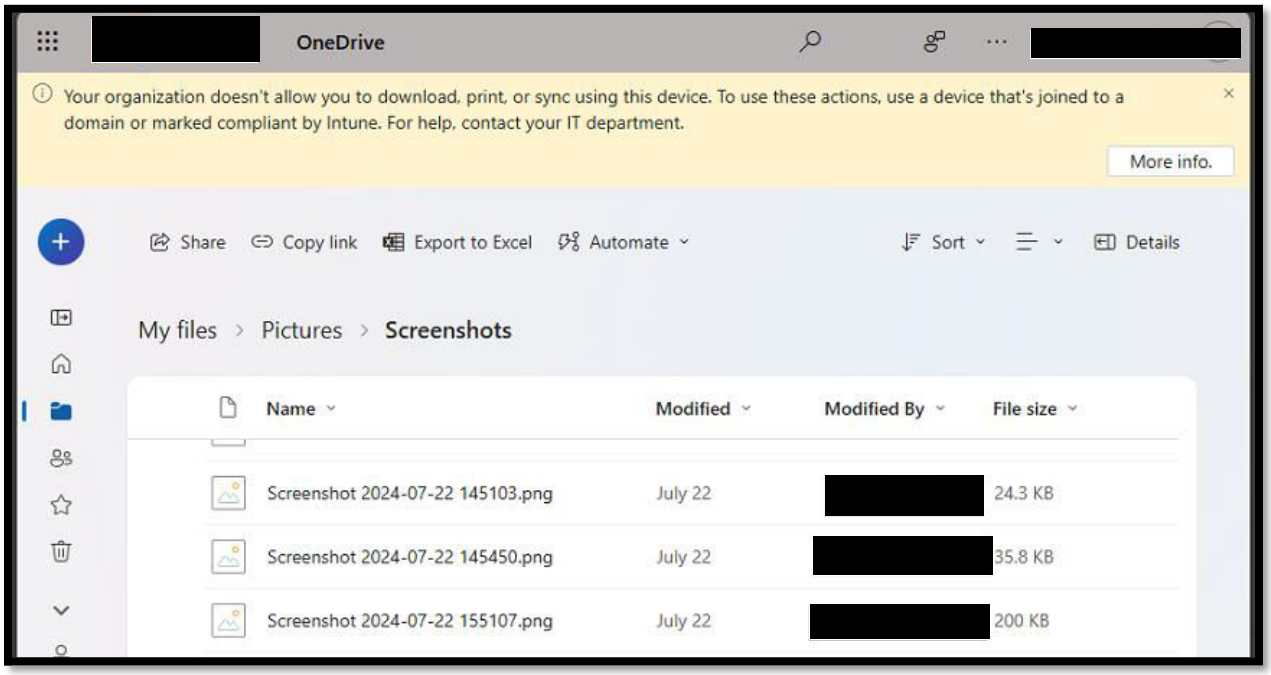
Attempting to establish persistence with alternative MFA methods was not possible as additional security information was required (1 of 2)

Attempting to establish persistence with alternative MFA methods was not possible as additional security information was required (2 of 2)

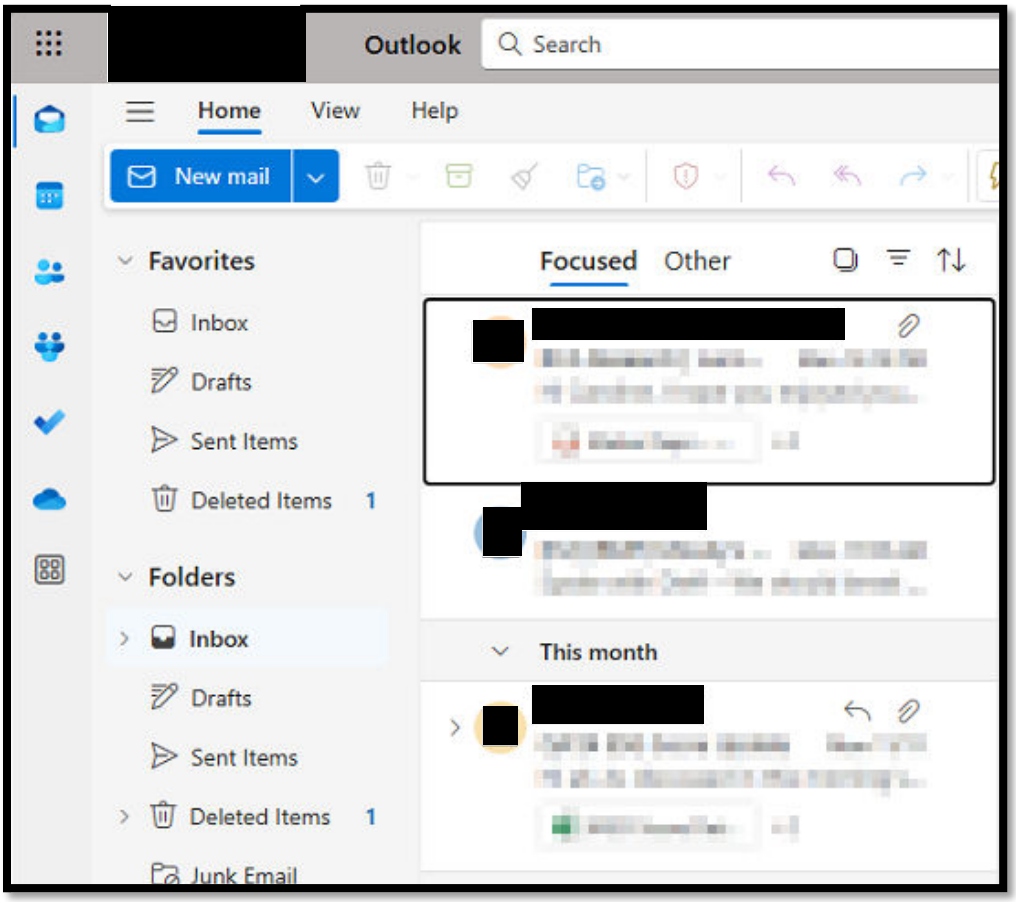


Recent documents identified in the "Quick access" contained sensitive financial information (1 of 2)

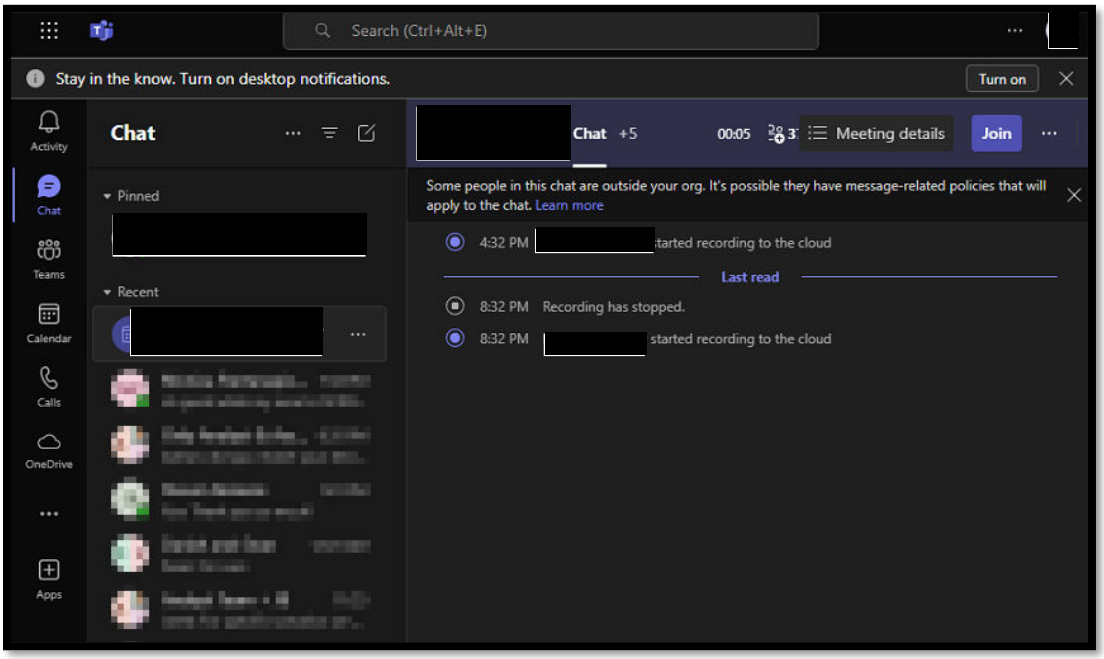
Recent documents identified in the "Quick access" contained sensitive financial information (2 of 2)



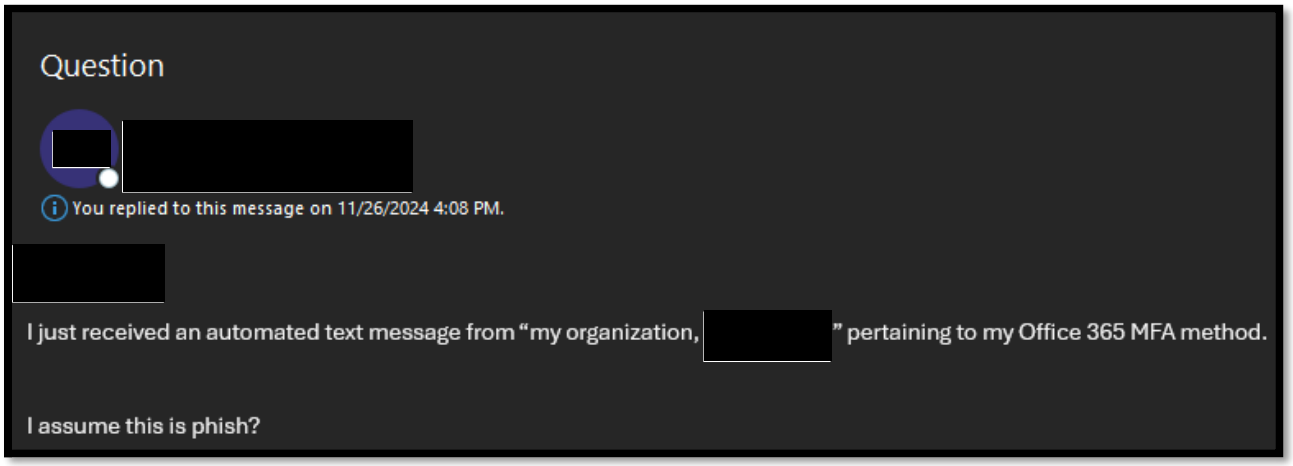
Reviewing material within the target's personal files, with this analysis centering on the target's screenshots



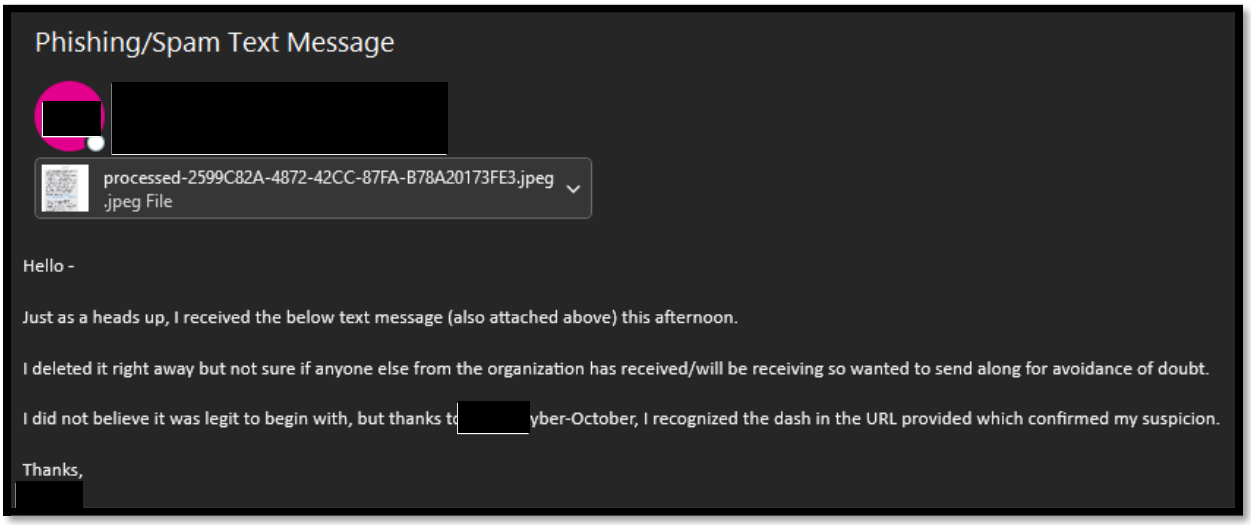
Demonstrating access to the target's Outlook email inbox



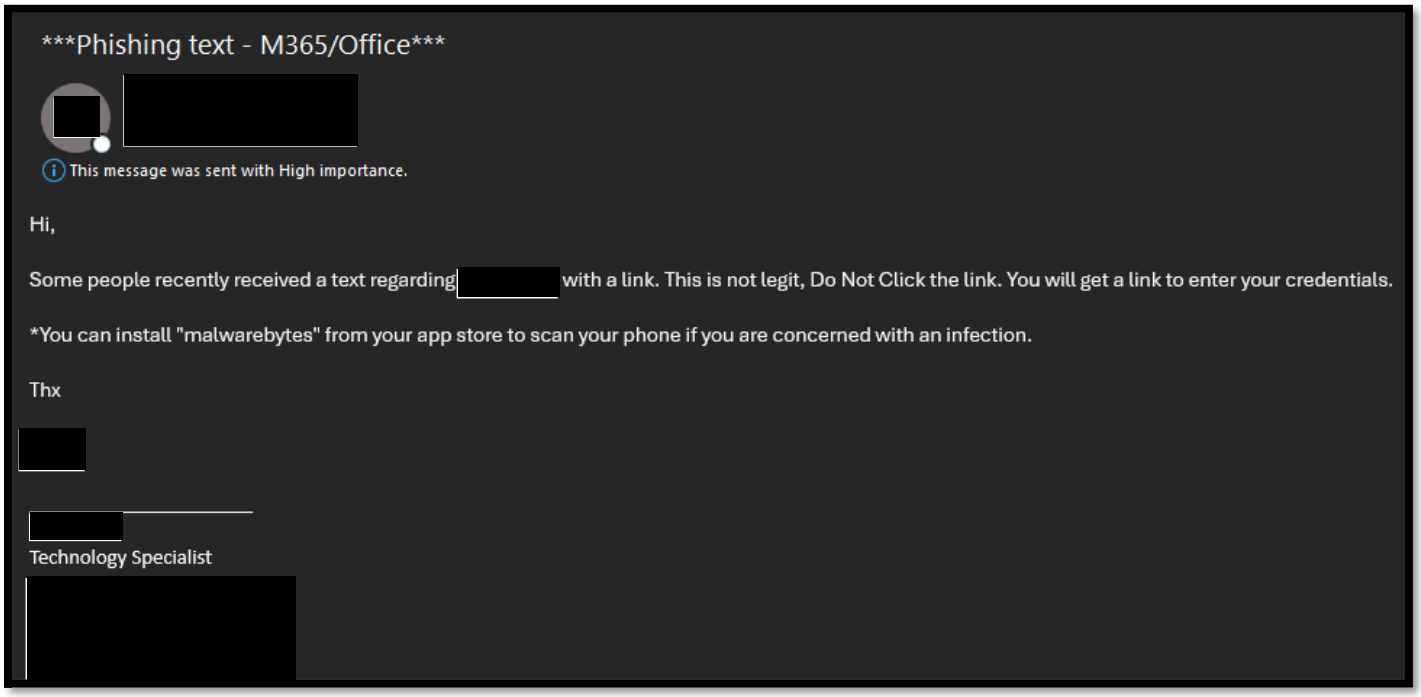
Demonstrating access to the target's Microsoft Teams environment



Evidentiary material provided by the project PoC (1 of 3)



Evidentiary material provided by the project PoC (2 of 3)



Evidentiary material provided by the project PoC (3 of 3)

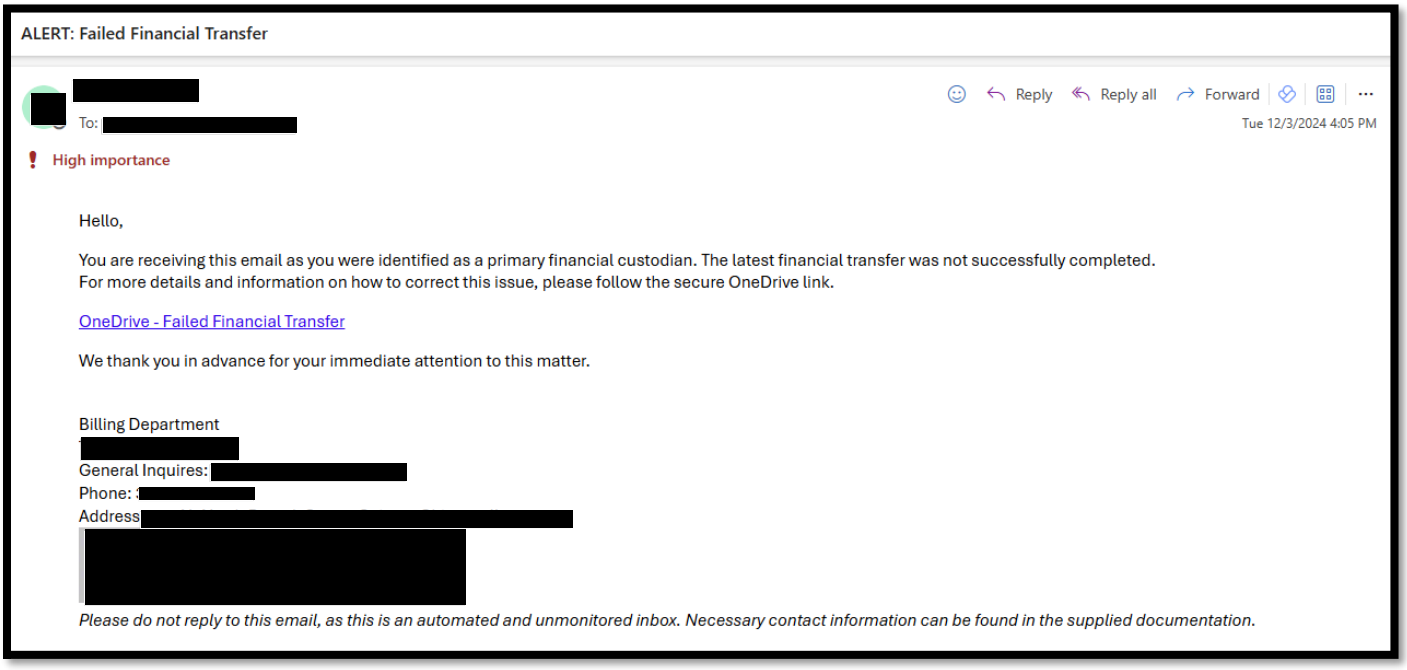
Social Engineering Campaign 3: Spearphishing via Impersonation of the Academy Group

Targets: [redacted]
From: [redacted]
Subject: ALERT: Failed Financial Transfer
Campaign Execution Date: December 3rd
Objective: Harvest target credentials and bypass MFA via an Office 365 login portal.
Compromised Employees: 0

Summary: Through OSINT, Abacus Group identified a key relationship and strategic partnership between [redacted] and The Academy Group. Through this relationship, Abacus Group impersonated The Academy Group with a typo-squatted domain (theacadamy.group - switch the e for an a in academy). More specifically, Abacus Group sent an email to Stephon Barnes and Gavin Cross from "[redacted]". [redacted] were chosen as targets due to their role within [redacted] ([redacted], respectively). In this email, which appeared to be automated, it was stated that there was a financial issue with the latest investment payment. The targets were instructed to follow a secure OneDrive link, which contained information about the financial issue that must be analyzed prior to rectifying the problem. The OneDrive link, however, would lead the targets to a phishing portal hosted by Abacus Group.

Results: This campaign did not result in the compromise of either target. Abacus Group did not receive any interaction with this campaign, thus leading Abacus Group to believe that a combination of end-user security awareness and technical controls defeated this campaign. This was later confirmed by the [redacted] project [redacted]. It was stated that both targets had flagged the email as suspicious. [redacted] used the phish alert button and emailed the helpdesk and [redacted] emailed both the project [redacted] and organizational systems administrator. [redacted] also reached out to The Academy Group to warn them of a possible ongoing social engineering campaign whereby their organization was being impersonated. This campaign demonstrated strong end-user security awareness. Additional security controls were also seen as effective in removing email from inboxes.

A brief narrative of evidence can be found below.


ALERT: Failed Financial Transfer

[redacted]

To: [redacted]

Reply Reply all Forward

Tue 12/3/2024 4:05 PM

High importance

Hello,

You are receiving this email as you were identified as a primary financial custodian. The latest financial transfer was not successfully completed.
For more details and information on how to correct this issue, please follow the secure OneDrive link.

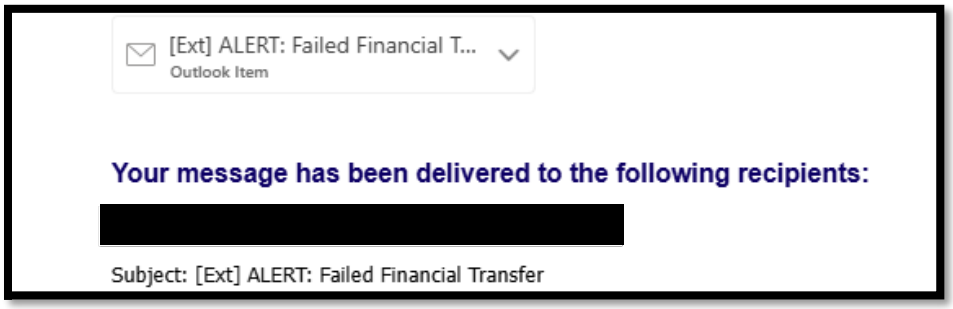
OneDrive - Failed Financial Transfer

We thank you in advance for your immediate attention to this matter.

Billing Department
[redacted]
General Inquires: [redacted]
Phone: [redacted]
Address [redacted]
[redacted]

Please do not reply to this email, as this is an automated and unmonitored inbox. Necessary contact information can be found in the supplied documentation.

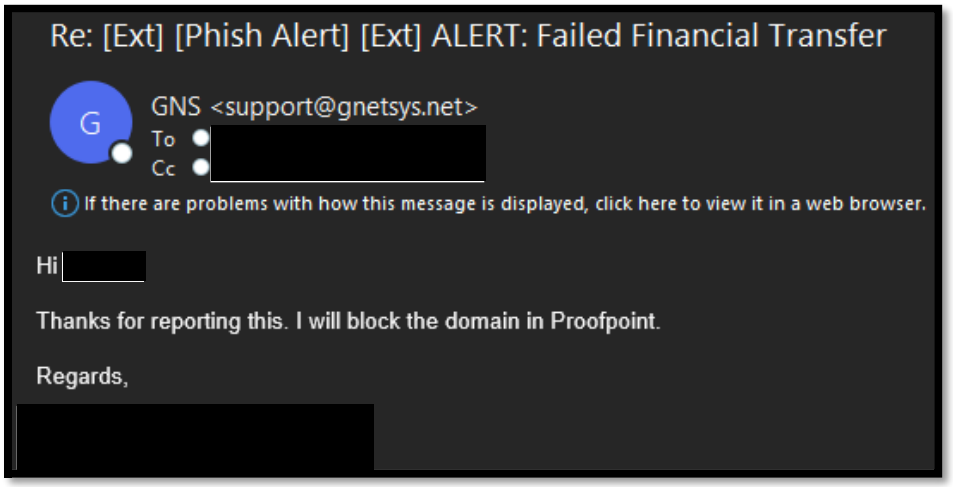
Demonstrating the email that was sent



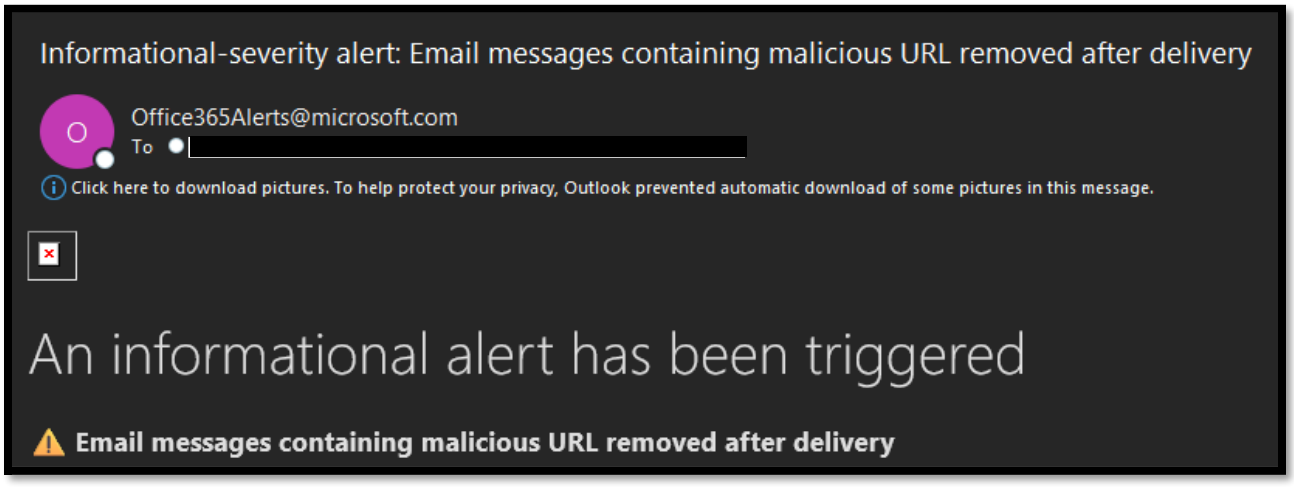
Demonstrating a delivery receipt

```
: lures get-url 90

https://login.theacadamy.group/vKDeQeKD

[21:05:22] [imp] [1] [o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0 (20.121.232.66)
[21:05:22] [inf] [1] [o365] landing URL: https://login.theacadamy.group/vKDeQeKD
[21:05:34] [imp] [2] [o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
, like Gecko) Chrome/125.0.6422.114 Safari/537.36 (40.94.25.65)
[21:05:34] [inf] [2] [o365] landing URL: https://login.theacadamy.group/vKDeQeKD
```

Evilginx – No verifiable user interaction was identified



Evidentiary material provided by the project PoC (1 of 2)



Evidentiary material provided by the project PoC (2 of 2)

Social Engineering Campaign 4: General Phishing - LifeLock

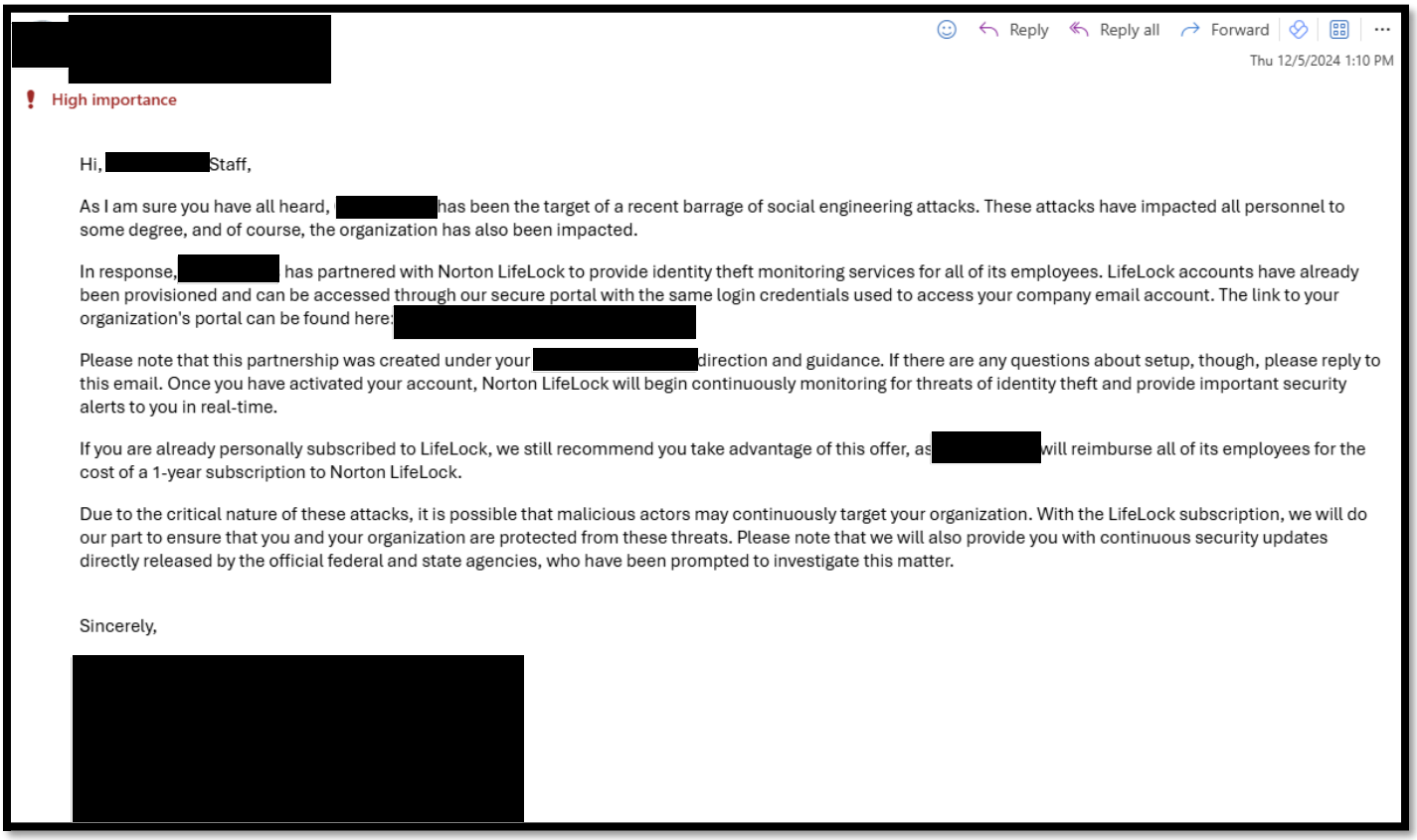
Targets: All identified and approved staff
From: [redacted]
Subject: Our Response to Recent Social Engineering Attacks
Campaign Execution Date: December 5th
Objective: Harvest target credentials and bypass MFA via a fake LifeLock SSO portal.
Compromised Employees: 0

Summary: Abacus Group sent a phishing email from a fictitious account manager from LifeLock [redacted]). The email leveraged pretext from the previously executed campaigns, stating that due to a rise in social engineering attacks against [redacted] everyone was provided a LifeLock account. It was also stated that this established partnership was under the direction of [redacted] the organization's [redacted]. The email further stated that all staff should log in to their accounts, which were federated with Office 365.

Results: This campaign did not result in the full compromise of any identified staff members. Abacus Group received no interaction with the emails or the phishing portal, and it was believed that a combination of end-user security awareness and technical security controls had defeated this campaign. This was later confirmed by the project [redacted]

All emails were blocked by Proofpoint, [redacted] email security solution. The project [redacted] and team notified Abacus Group of this and then released the emails so that further testing could commence. After the release, one individual clicked on the link, though Proofpoint prevented any further action as the URL was deemed to be malicious. Aside from this individual clicking on the link, numerous others reported the email as phishing. This campaign demonstrated both strong end-user security awareness and technical security controls.

A brief narrative of evidence can be found below.


[redacted]

Reply Reply all Forward ···

Thu 12/5/2024 1:10 PM

High importance

Hi, [redacted] Staff,

As I am sure you have all heard, [redacted] has been the target of a recent barrage of social engineering attacks. These attacks have impacted all personnel to some degree, and of course, the organization has also been impacted.

In response, [redacted] has partnered with Norton LifeLock to provide identity theft monitoring services for all of its employees. LifeLock accounts have already been provisioned and can be accessed through our secure portal with the same login credentials used to access your company email account. The link to your organization's portal can be found here: [redacted]

Please note that this partnership was created under your [redacted] direction and guidance. If there are any questions about setup, though, please reply to this email. Once you have activated your account, Norton LifeLock will begin continuously monitoring for threats of identity theft and provide important security alerts to you in real-time.

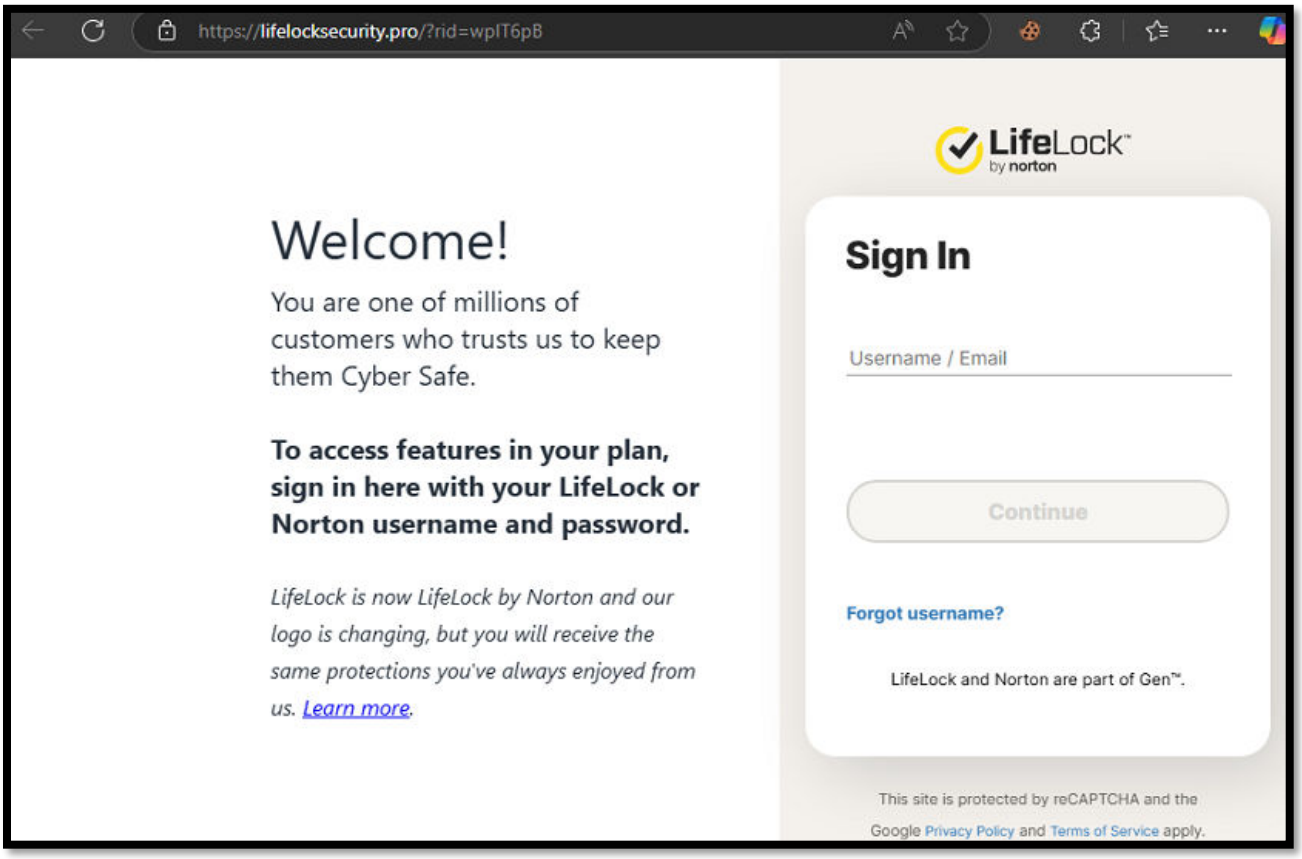
If you are already personally subscribed to LifeLock, we still recommend you take advantage of this offer, as [redacted] will reimburse all of its employees for the cost of a 1-year subscription to Norton LifeLock.

Due to the critical nature of these attacks, it is possible that malicious actors may continuously target your organization. With the LifeLock subscription, we will do our part to ensure that you and your organization are protected from these threats. Please note that we will also provide you with continuous security updates directly released by the official federal and state agencies, who have been prompted to investigate this matter.

Sincerely,

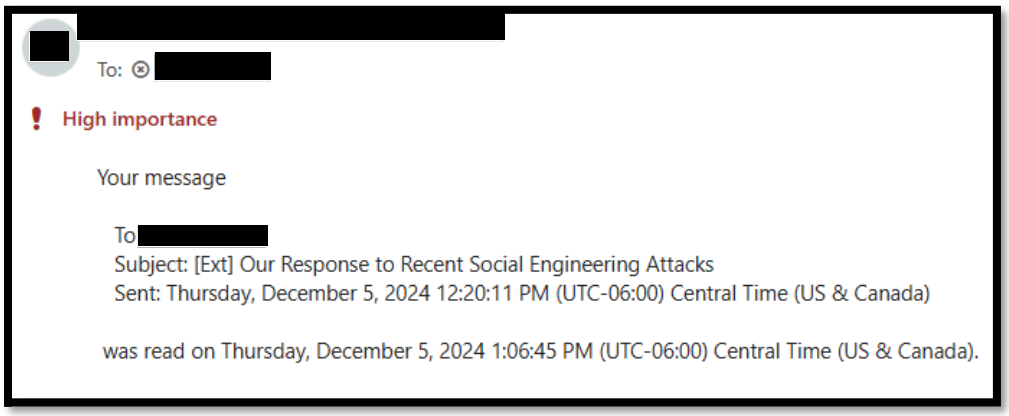
[redacted]

Demonstrating the email that was sent

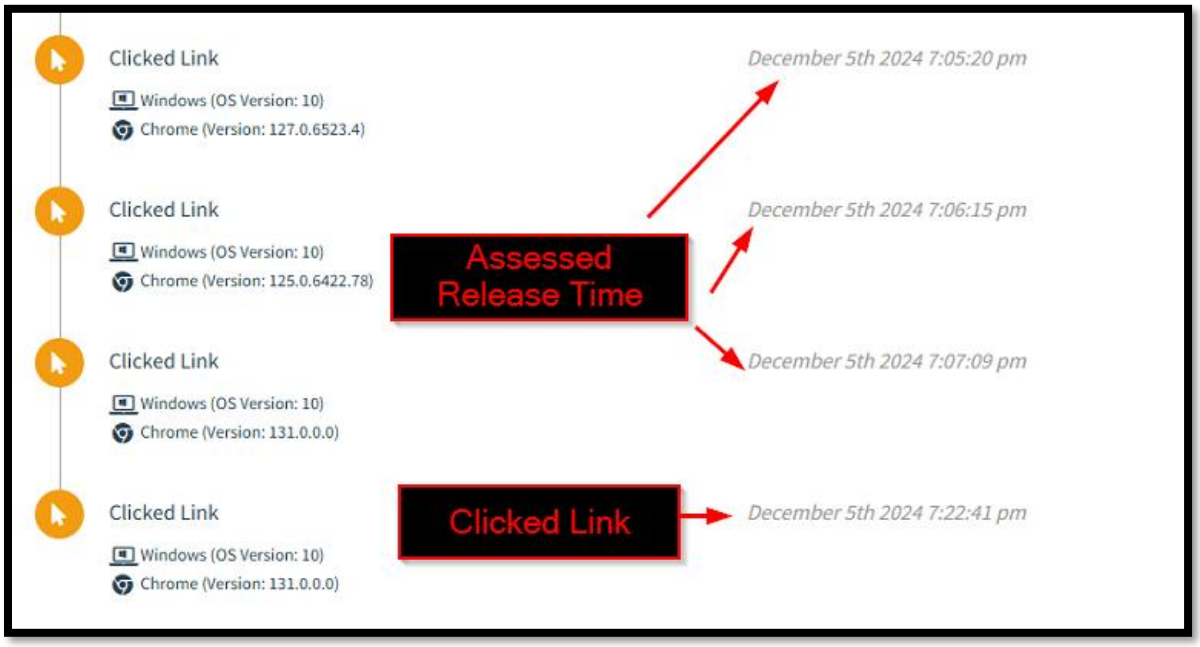


Demonstrating the phishing portal (1 of 2)

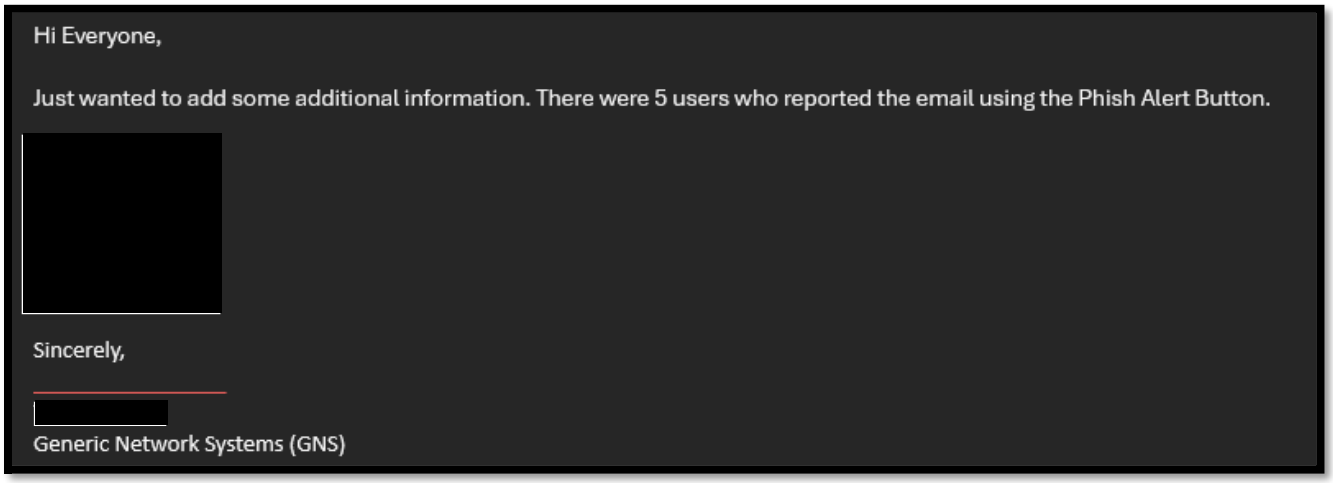
Demonstrating the phishing portal (2 of 2)



Demonstrating the return of a read receipt, which is not warranted as a security finding and was only possible after the emails were released from Proofpoint



Demonstrating activity on the phishing portal, with only one result indicative of human interaction



Evidentiary material demonstrating that even after the release, numerous users reported the campaign

Risk Details

NBNS, LLMNR, and/or mDNS Service Poisoning
MITRE ATT&CK Tactic: TA0008-Lateral Movement
Exploited – **Impact**: High – **Ease**: High – **Risk**: High

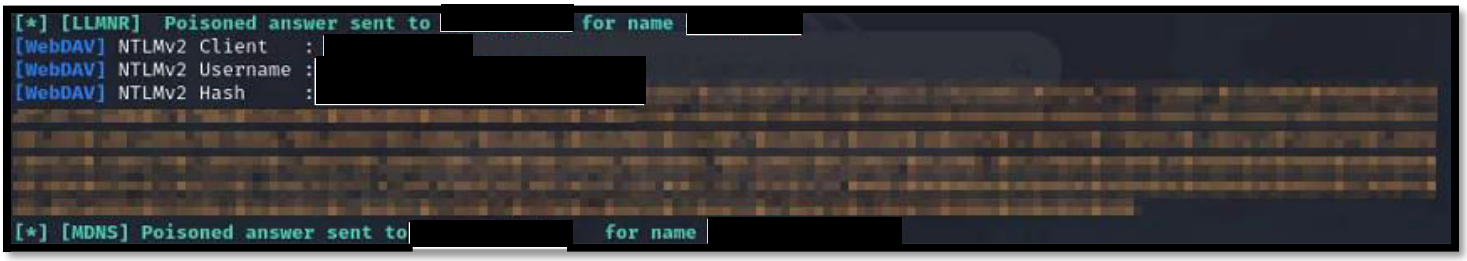
Summary:
As unauthenticated protocols, NetBIOS Name Service (NBNS), Link-Local Multicast Name Resolution (LLMNR) and Multicast Domain Name Service (mDNS) are subject to spoofing and Man-in-the-Middle (MitM) attacks whereby an attacker can impersonate another system and misdirect the associated network traffic. Using free, open-source tools such as Metasploit or Responder, a malicious actor can perform NBNS/LLMNR/mDNS spoofing to forward traffic to a fake SMB service listener, which would collect LM and NTLMv1/v2 authentication hashes.

NetBIOS Name Service (NBNS) and Link-Local Multicast Name Resolution (LLMNR) are broadcast name resolution protocols. Network-connected systems often use them to identify hosts on the local subnet when DNS fails. If the DNS name does not resolve, the client broadcasts to the local network asking if any other system has the IP address for the name it is looking for. The fact that this process is unauthenticated and broadcasted to the whole network allows any machine on the network to respond and claim to be the DNS resolution destination.

When a device tries to resolve the IP address for a given name, it tries, in order, the following lookup methods:
- Local Hosts File
- DNS
- NBNS/LLMNR/mDNS

Any mistyped internal server name, a laptop looking for its domain network resources while on another network, or a would-be web search would generate an NBNS query that a malicious NBNS responder can answer to misdirect associated network traffic.
Moreover, NTLM hashes do not even have to be reversed in order to be used. An attacker can “pass the hash,” authenticating with the NTLM hash against a system using crackmapexec and similar tools.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Disable the use of NBNS across all corporate devices via AD GPOs.
  NetBios can also be disabled using DHCP option 001, “Microsoft Disable NetBios,” with the setting of 0x2. Note that Microsoft’s original DHCP option for disabling NBNS is not RFC 2132 compliant, so following their original implementation instructions may not actually work on networking vendors that only accept RFC 2132 compliant DHCP options. Microsoft has also implemented a way to disable NBNS on Windows DHCP clients by using the RFC 2132 compliant option 43 “Vendor Specific Information”.

- NBNS can be disabled using PowerShell with the following commands:
  $regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
  Get-ChildItem $regkey |foreach { Set-ItemProperty -Path "$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}

- LLMNR can be disabled using PowerShell with the following commands:
  REG ADD “HKLM\Software\policies\Microsoft\Windows NT\DNSClient”
  REG ADD “HKLM\Software\policies\Microsoft\Windows NT\DNSClient” /v ” EnableMulticast” /t REG_DWORD /d “0” /f

- NBNS can also be disabled via Registry by navigating to the registry key at:
  Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\
  Then adjusting the NetbiosOption value from the default of 0 to a value of 2.|

- mDNS can be disabled using Powershell with the following command:
  set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\" -Name EnableMDNS -Value 0 -Type DWord
- mDNS using the following reg command:
  REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters" /v " EnableMDNS" /t REG_DWORD /d "0" /f

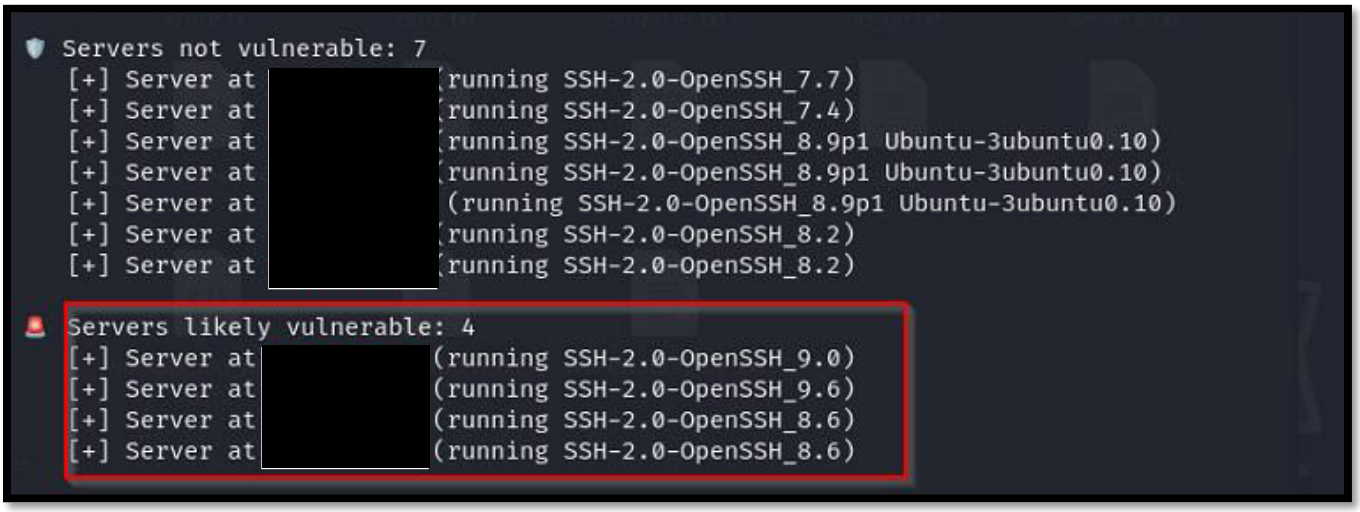
Reference(s):
https://attack.mitre.org/techniques/T1557/001/
https://technet.microsoft.com/en-us/library/cc940063.aspx
https://github.com/lgandx/Responder/
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-dhcpe/ef7676b1-5568-4afc-836a-7eca63a10a3a
https://community.infoblox.com/t5/DNS-DHCP-IPAM/Disable-NETBIOS-via-DHCP-Options/td-p/16086
https://infinitelogins.com/2020/11/23/disabling-llmnr-in-your-network/

Affected Endpoint(s):
[redacted]

OpenSSH Susceptible to CVE-2024-6387
MITRE ATT&CK Tactic: TA0004-Privilege Escalation
Detected: (QoD 75%) – **Impact**: High – **Ease**: High – **Risk**: High

Summary:
The affected endpoints were fingerprinted as utilizing OpenSSH with specific versions known to be susceptible to CVE-2024-6387 also known as regreSSHion. This vulnerability was publicly disclosed in July of 2024 and can be exploited by malicious actors to achieve unauthenticated remote code execution (RCE) as the root account.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):
- Ensure all instances of OpenSSH are upgraded to the most recent version, which at the time of writing is version 9.9 released in September of 2024.

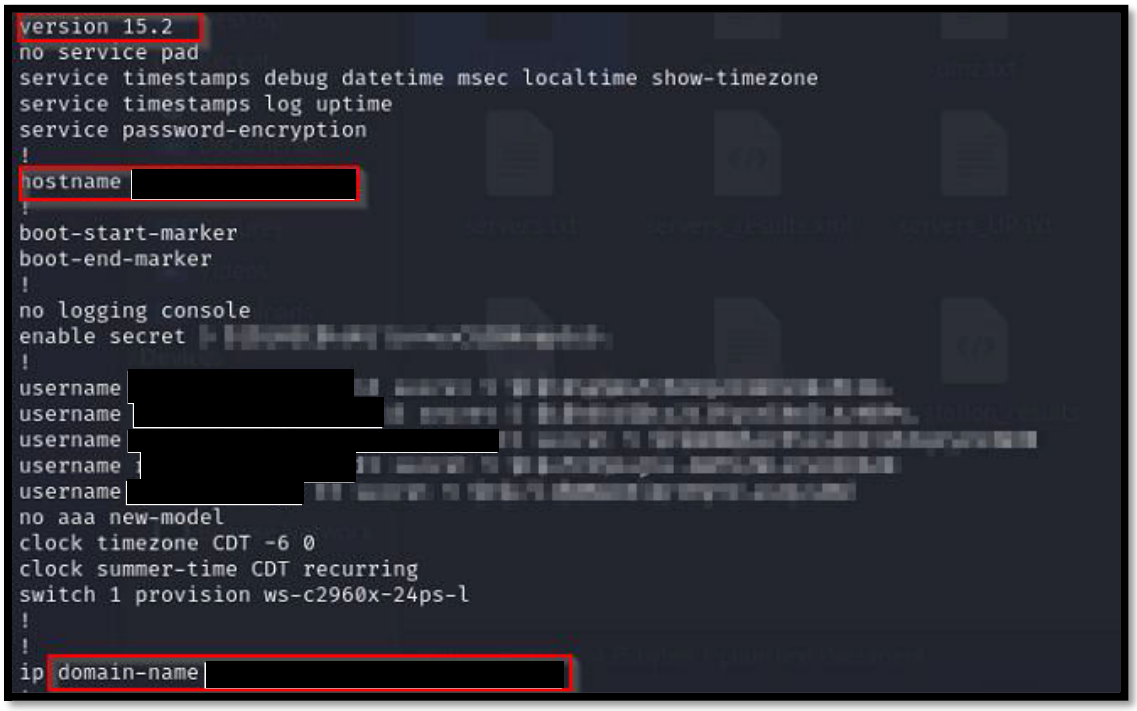
Reference(s):
https://nvd.nist.gov/vuln/detail/CVE-2016-1908
https://nvd.nist.gov/vuln/detail/CVE-2023-38408
https://www.openssh.com/releasenotes.html

Affected Endpoint(s):
[redacted]

Cisco Smart Install (SMI) Remote Code Execution
MITRE ATT&CK Tactic: TA0002-Execution
Exploited – **Impact**: High – **Ease**: High – **Risk**: High

Summary:
A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device. The vulnerability is due to improper validation of packet data. An attacker could exploit this vulnerability by sending a crafted Smart Install message to an affected device on TCP port 4786. A successful exploit could allow the attacker to cause a buffer overflow on the affected device, which could have the following impacts: Triggering a reload of the device, Allowing the attacker to execute arbitrary code on the device, causing an indefinite loop on the affected device that triggers a watchdog crash.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):
- Ensure Cisco Catalyst Infrastructure is updated to the current supported software versions and included in routine patch management.

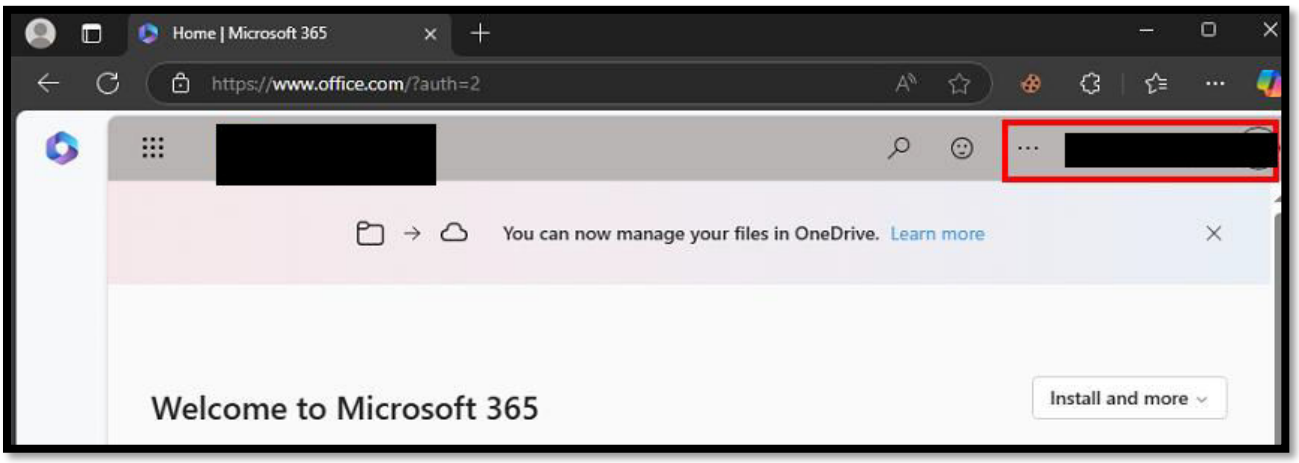
Reference(s):
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2
https://nvd.nist.gov/vuln/detail/cve-2018-0171

Affected Endpoint(s):
[redacted]

Insufficient Conditional Access Policies
MITRE ATT&CK Tactic: TA0001 – Initial Access
Exploited – **Impact**: High – **Ease**: Moderate – **Risk**: Moderate

Summary:
Through social engineering, Abacus Group successfully harvested a user's Office 365 credentials and bypassed MFA. As such, Abacus Group assesses that while conditional access policies may exist, the current policies are not sufficient to prevent malicious actors from obtaining full authentication to Office 365. [redacted] should consider conditional access policies that are contingent upon network location and device compliance. With these policies, Abacus Group would not have had a successful compromise even with bypassing MFA.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):
- Consider adding conditional access policies that are contingent upon network location (named locations) or device specificity.
    - Leverage report-only prior to full implementation.

Reference(s):
https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-by-location
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network
https://learn.microsoft.com/en-us/mem/intune/protect/create-conditional-access-intune
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-condition-filters-for-devices

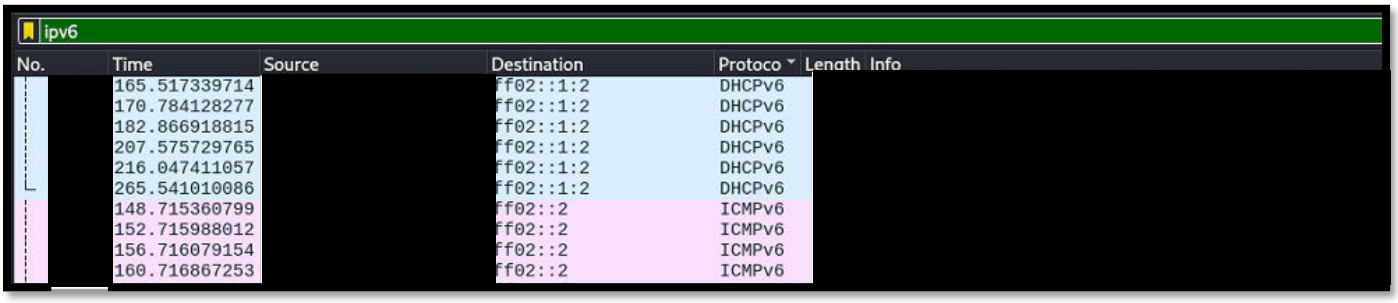
Affected Endpoint(s):
Organization-Wide

IPv4/IPv6 Dual Stack Environment Without First Hop Security
MITRE ATT&CK Tactic: TA0006-Credential Access
Detected: (QoD 60%) – **Impact**: Moderate – **Ease**: Moderate – **Risk**: Moderate

Summary:
IPv6 security has some unexpected complications for network engineers who are accustomed to IPv4 networks. One such under-mentioned problem is the need to lock down or turn off IPv6 services that might be running on an IPv4 or a dual IPv4/IPv6 network. Most modern devices have IPv6 enabled alongside IPv4 by default. Without IPv6 First Hop Security controls enabled several points of exploitation pivoting exist within the network infrastructure that make all devices connected to the internal network vulnerable.

Due to possible unknown implemented security controls to ensure protection from common IPv6-based attacks, this finding's QoD has been reduced to 60%.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Assess networking device configurations to implement IPv6 First Hop Security. Alternatively, if IPv6 is not required, consider disabling IPv6 across all devices via an Active Directory Group Policy Object (GPO).

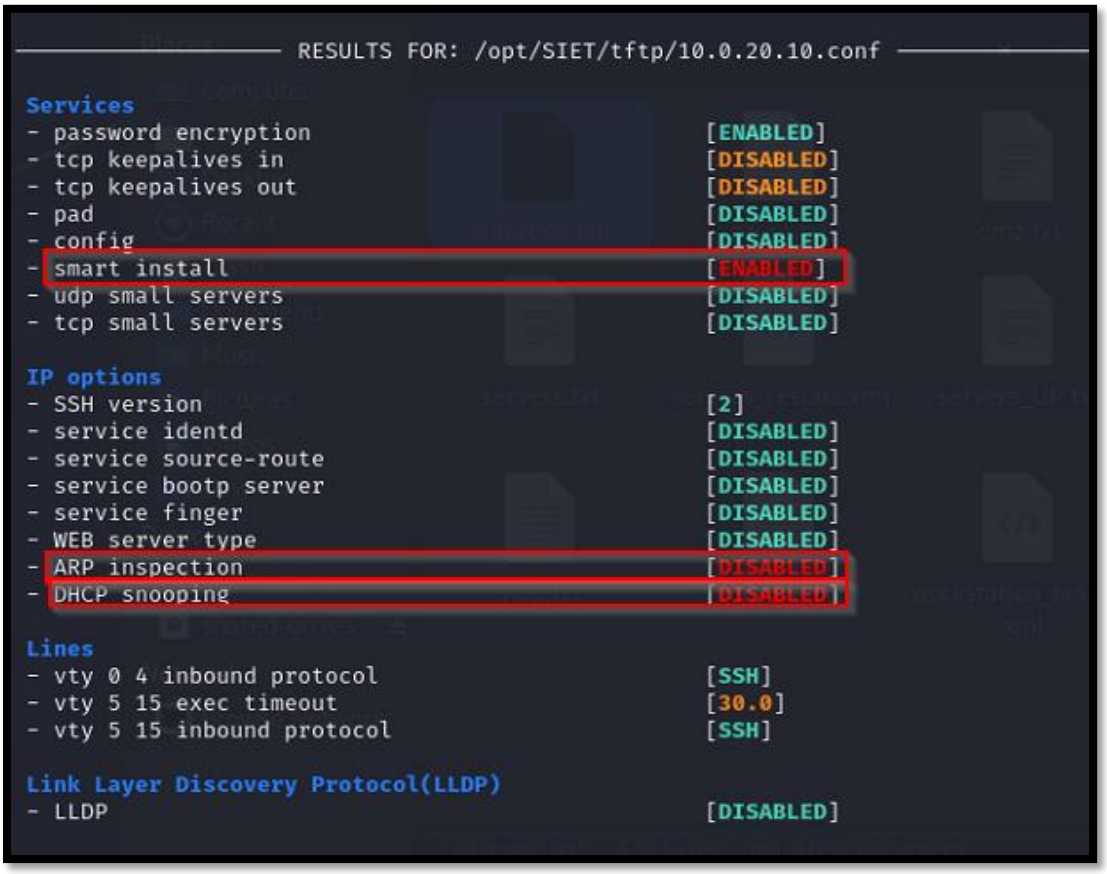
Reference(s):
https://www.juniper.net/documentation/us/en/software/junos/transport-ip/topics/task/ipv6-configure-features.html

Affected Endpoint(s):
[redacted]

Lack of Dynamic ARP Inspection
MITRE ATT&CK Tactic: TA0042-Resource Development
Detected: (QoD 85%) – **Impact**: Moderate – **Ease**: Moderate – **Risk**: Moderate

Summary:
Dynamic ARP inspection (DAI) is a security feature that protects networks against Man-in-the-Middle (MITM) ARP spoofing attacks. ARP spoofing is an attack vector by which a malicious actor will poison the ARP caches of network devices and redirect traffic to the attacking machine, thus intercepting traffic intended for other hosts. DAI inspects ARP packets on the LAN and leverages the DHCP snooping table on the switch to validate these ARP packets; any inconsistencies between the packet and the snooping table are then dropped.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Enable DAI on a VLAN by using the CLI:
  [edit bridge-domains bridge-domain-name forwarding-options dhcp-security]
  user@device# set arp-inspection

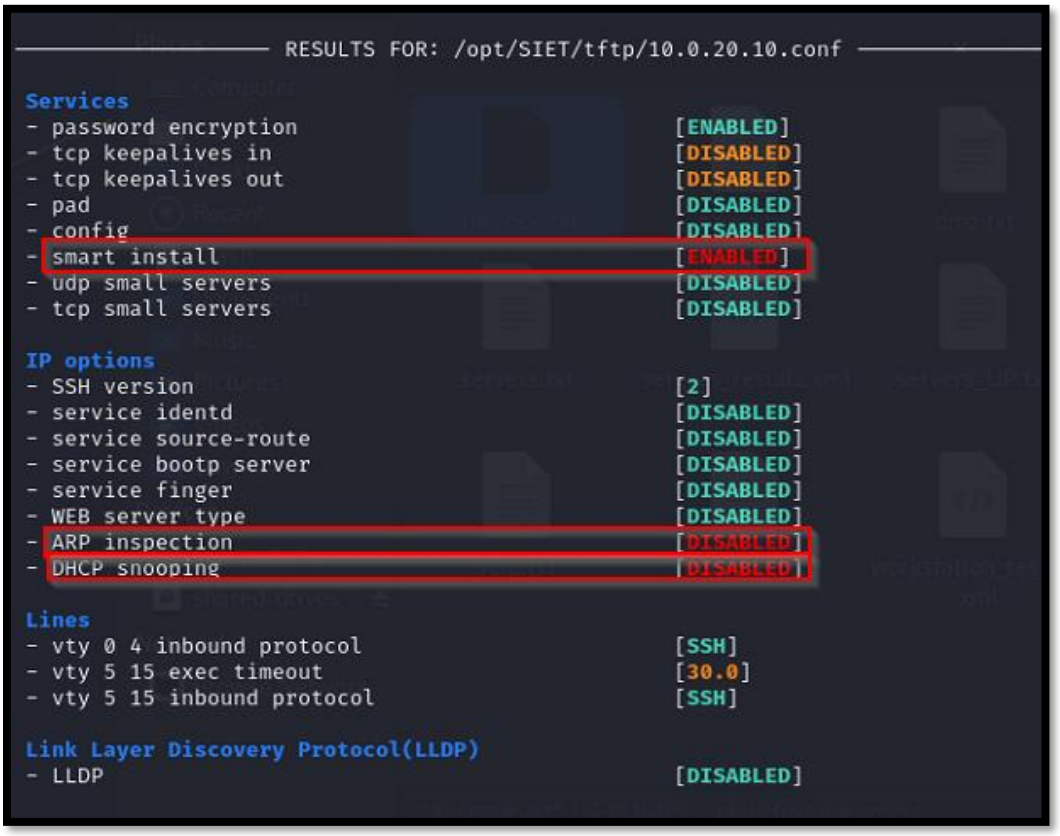
Reference(s):
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html

Affected Endpoint(s):
[redacted]

Lack of DHCP Snooping
MITRE ATT&CK Tactic: TA0006-Credential Access
Detected: (QoD 85%) – **Impact**: Moderate – **Ease**: Moderate – **Risk**: Moderate

Summary:
DHCP snooping will drop DHCP messages from a DHCP server that is not trusted. Trusted DHCP servers are identified by configuring a switchport's DHCP snooping trust state. DHCP server messages can flow through switchports that have a DHCP snooping trusted state. DHCP server messages will be dropped if attempting to flow through a switchport that is not trusted.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- On Cisco OS devices, DHCP snooping is enabled in a routing instance when you configure the following options in that routing instance:
  - dhcp-relay statement at the [edit forwarding-options] hierarchy level
  - dhcp-local-server statement at the [edit system services] hierarchy level

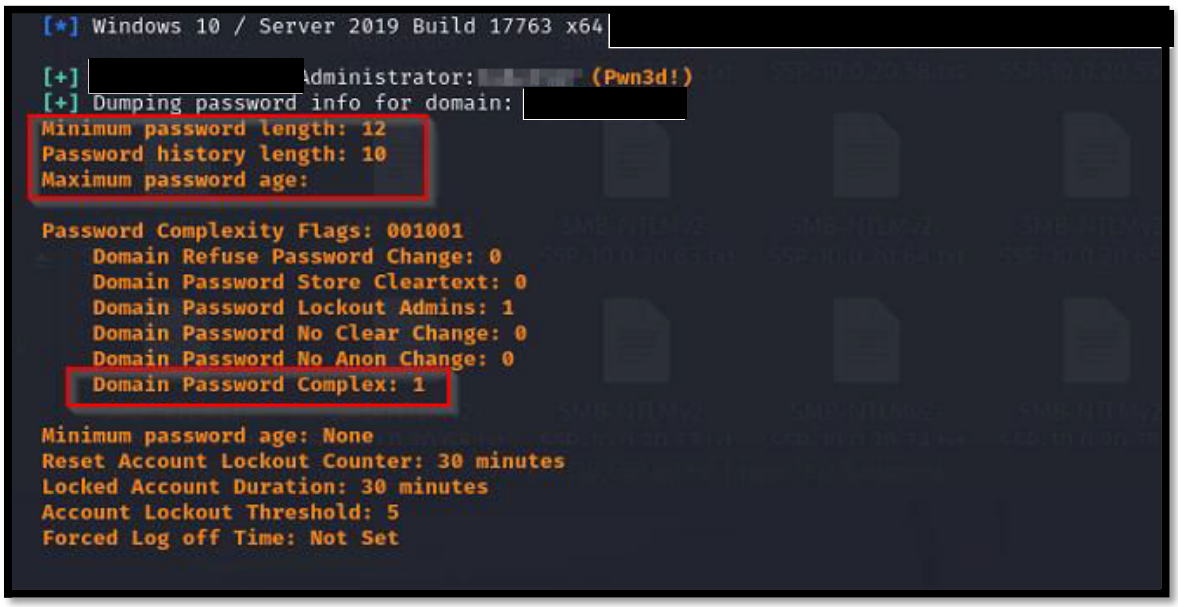
Reference(s):
https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus3548/103x/configuration/security/cisco-nexus-3548-nx-os-security-configuration-guide-103x/m-configuring-dhcp-snooping.pdf

Affected Endpoint(s):
[redacted]

Weak User & Admin Password Complexity Requirements
MITRE ATT&CK Tactic: TA0006-Credential Access
Exploited – Impact: Moderate – **Ease:** Moderate – **Risk:** Moderate

Summary:
A single user account was identified with an easily guessable password based on dictionary words with the use of one special character. Specifically, the compromised AD domain admin account password was identified to be only 8 characters long with very little complexity, which ultimately contributed to domain compromise. It is assessed that this is more than likely a result of a legacy password that had not been changed to meet the minimum password length set within the domain.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Consider setting password complexity and length requirements directive in AD by utilizing Pass Filter implant as described in the provided references.
- It is important to note that if [redacted] is leveraging Microsoft Entra ID (Formally Azure Active Directory (AAD)) with AADSync/AADConnect back to conventional AD there are additional considerations. If [redacted] does not have password complexity enforced in AAD, then when someone sets their password, the password writeback from AAD to AD may result in a weak password for the AD user (even though password complexity is set in AD GPOs).
    - As a result, it is recommended to first check and ensure AAD password complexity is enforced (https://docs.microsoft.com/en-us/azure/active-directory-b2c/password-complexity).

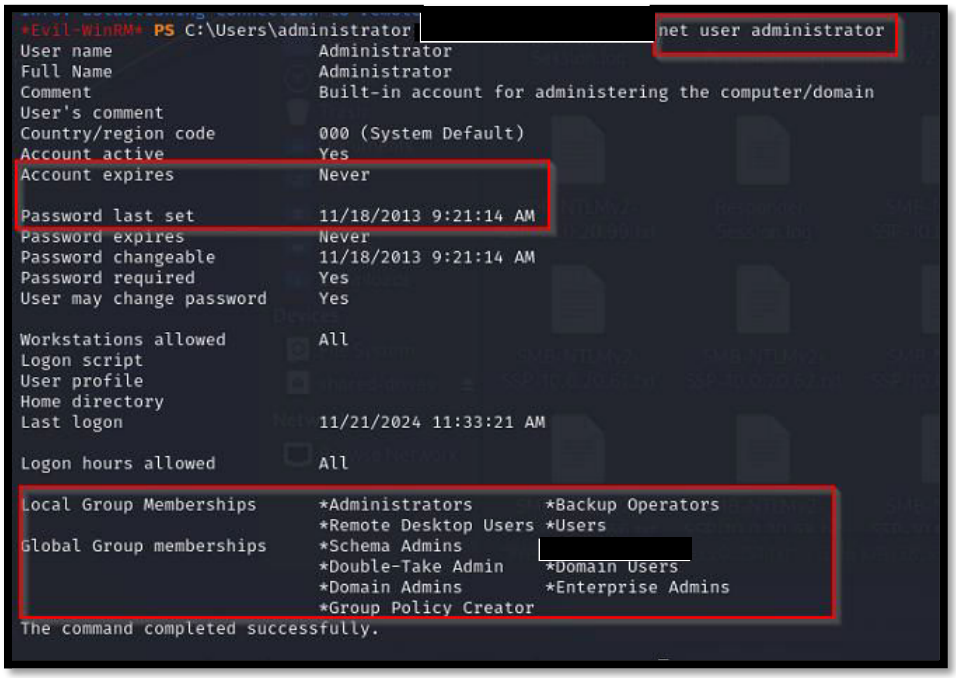
Reference(s):
https://docs.microsoft.com/en-us/windows/win32/secmgmt/installing-and-registering-a-password-filter-dll?redirectedfrom=MSDN
https://github.com/GoSecure/DLLPasswordFilterImplant
https://github.com/jephthai/OpenPasswordFilter

Affected Endpoint(s):
[redacted]

Lateral Movement via Windows Remote Management (WinRM)
MITRE ATT&CK Tactic: TA0008-Lateral Movement
Exploited – **Impact**: Moderate – **Ease**: Moderate – **Risk**: Moderate

Summary:
Windows Remote Management (WinRM) is a protocol developed by Microsoft for remotely managing hardware and operating systems on Windows machines. It is a component of the Windows Management (WMI) Framework and implements the WS-Management Protocol, which is a standard web services protocol designed for remote management of software and hardware. WinRM uses port 5985 for HTTP transport and 5986 for HTTPS Transport. Adversaries may use valid accounts to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user such as account enumeration/creation, uploading/downloading files for persistence/privilege escalation and exfiltration.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):
- Disable the WinRM service if not necessary.
  - If the service is necessary, lock down critical enclaves with separate WinRM infrastructure and follow WinRM best practices on use of host firewalls to restrict WinRM access to allow communication only to/from specific devices.
- Monitor executed commands and arguments that may invoke a WinRM script to correlate it with other related events.
- Monitor for user accounts logging into the system via Valid Accounts to interact with remote systems using Windows Remote Management (WinRM).
- Monitor for newly constructed network connections using Windows Remote Management (WinRM), such as remote WMI connection attempts (typically over port 5985 when using HTTP and 5986 for HTTPS).

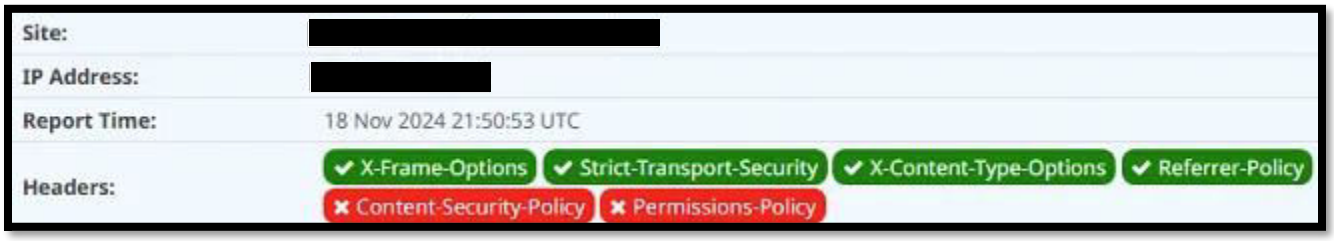
Reference(s):
https://attack.mitre.org/tactics/TA0008/
https://13cubed.s3.amazonaws.com/downloads/impacket_exec_commands_cheat_sheet.pdf

Affected Endpoint(s):
[redacted]

Content-Security-Policy (CSP) Not Implemented
MITRE ATT&CK Tactic: TA0042-Resource Development
Detected: (QoD 85%) – **Impact**: Low – **Ease**: Low – **Risk**: Low

Summary:
The affected web applications did not implement the Content-Security-Policy (CSP) HTTP header. A strong CSP adds an additional layer of protection against client-side attacks such as cross-site scripting (XSS), clickjacking, and form jacking.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):
- Implement the 'default-src', 'base-uri', 'script-src', 'style-src', and 'object-src' directives for all websites, and do not allow for 'unsafe-inline' or 'unsafe-eval' script execution without a nonce.
- Implement form jacking protection for all websites via the 'form-src' directive, which should be set to 'self' or 'none'.
- Implement the 'frame-ancestors' directive across all websites to protect against clickjacking.
- Consider implementing the 'upgrade-insecure-requests' directive to better protect against man-in-the-middle attacks.
- Consider implementing the 'report-uri' directive for reporting CSP violations

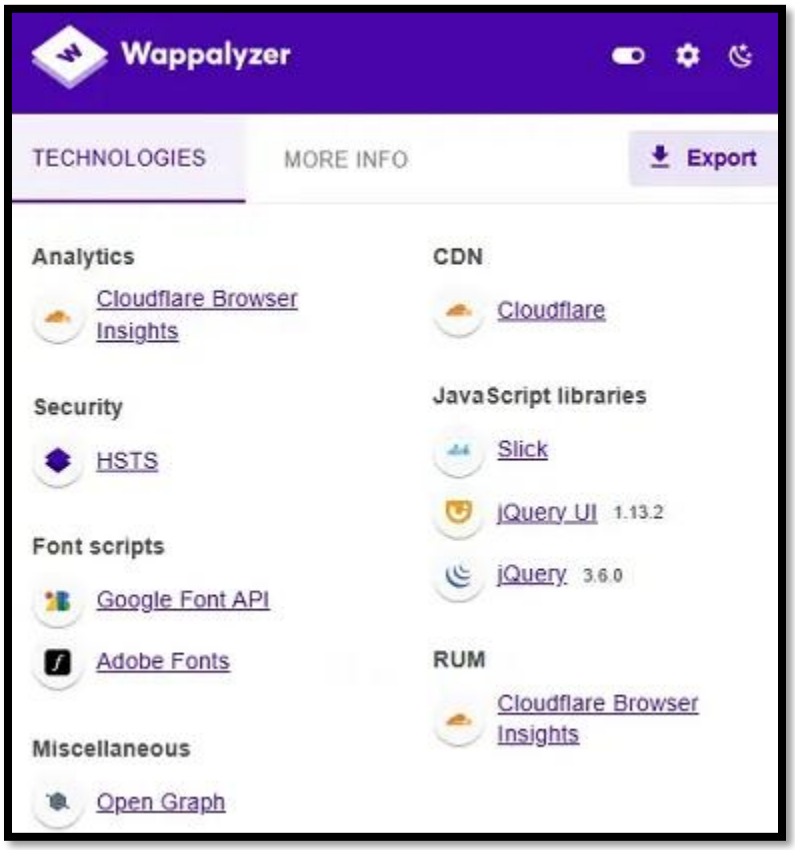
Reference(s):
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Content_Security_Policy_Cheat_Sheet.md

Affected Endpoint(s):
[redacted]

Out of Date jQuery Potentially Susceptible to Multiple Vulnerabilities
MITRE ATT&CK Tactic: TA0042-Resource Development
Detected: (QoD 85%) – **Impact**: Low – **Ease**: Low – **Risk**: Low

Summary:
Out-of-date jQuery was discovered on the affected web applications. These versions are associated with multiple Cross-Site Scripting (XSS) and Prototype Pollution attacks, which may allow a malicious actor to execute untrusted code in a client-side browser.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):
- JavaScript libraries should always be kept up to date. The latest version of jQuery is currently version 3.7.1.

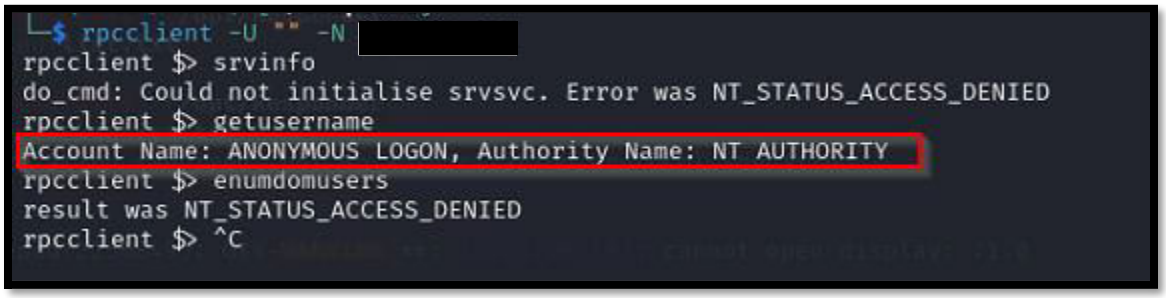
Reference(s):
https://jquery.com/download/

Affected Endpoint(s):
[redacted]

SMB/MSRPC Null Session
MITRE ATT&CK Tactic: TA0002-Execution
Detected: (QoD 85%) – **Impact**: Low – **Ease**: Low – **Risk**: Low

Summary:
Null sessions, which allow connections without authentication (no login/password), can be exploited to gather sensitive information from a system. This includes user lists, group memberships, and other details that can be used for further attacks, such as brute force or password spraying.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- To mitigate this risk, it's important to disable null sessions and ensure that proper authentication mechanisms are in place. This can be done by configuring your system to require credentials for accessing RPC services and by following best practices for securing SMB and RPC endpoints.
- Disable Null Sessions:Open the Group Policy Management Console (GPMC).
  Navigate to Computer Configuration Windows Settings Security Settings Local Policies Security Options.

  Find and set the following policies:
  Network access: Allow anonymous SID/Name translation: Set to Disabled.
  Network access: Do not allow anonymous enumeration of SAM accounts and shares: Set to Enabled.
  Network access: Restrict anonymous access to Named Pipes and Shares: Set to Enabled.

  Registry Changes:
  Open the Registry Editor (regedit).
  Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.

  Create or modify the following DWORD values:
  RestrictAnonymous and set it to 1.
  RestrictAnonymousSAM and set it to 1.
  EveryoneIncludesAnonymous and set it to 0

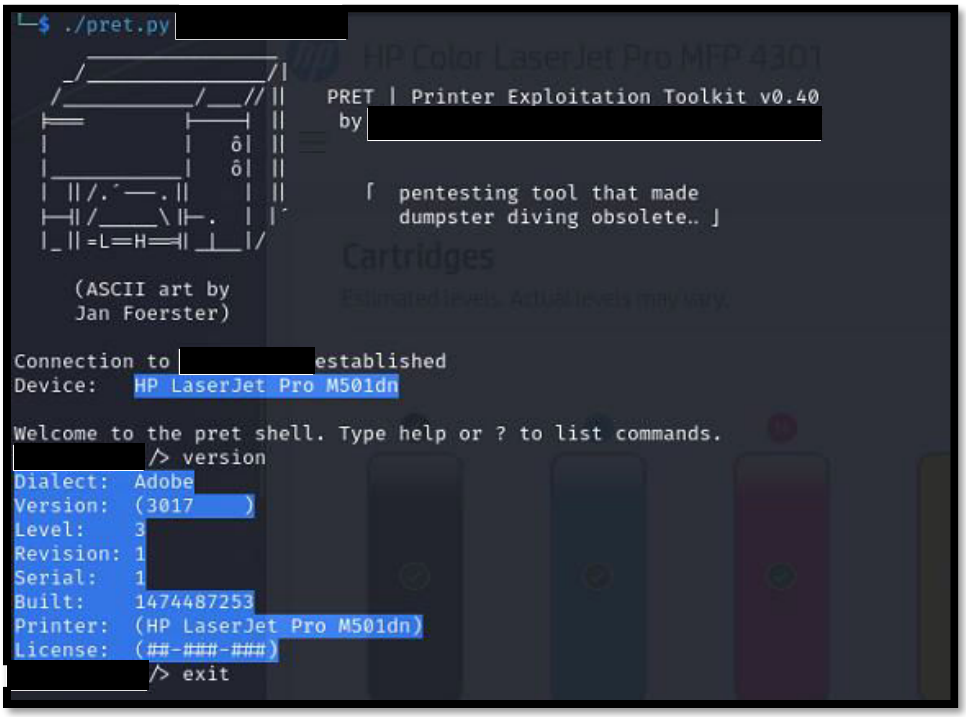
Reference(s):
https://dirteam.com/sander/2021/09/22/hardening-smb-on-domain-controllers-step-3-disabling-smb-null-sessions/

Affected Endpoint(s):
[redacted]

Printers With Jetdirect Are Accessible and Exploitable
MITRE ATT&CK Tactic: TA0042-Resource Development
Detected: (QoD 85%) – **Impact**: Low – **Ease**: Low – **Risk**: Low

Summary:
The affected endpoints were identified utilizing Jetdirect, a common and inherently vulnerable protocol common with laser printers. Jetdirect strips off all TCP/IP headers in requests that are sent to the device in favor of processing requests at a higher speed in enterprise environments. However, this lack of verification introduces the possibility of a malicious actor submitting malicious print jobs (known as print hijacking), which may execute a limited set of commands in the specific printing language utilized by the endpoint. Abacus Group exploited this using an open-source tool called Printer Exploitation Toolkit to enumerate additional system information.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):
- Leverage Windows Print Server to manage ACLs and printer access rather than sending print jobs directly to the affected endpoints.
- Alternatively, if Jetdirect is required for the functioning of the device, consider restricting access by establishing an access control list to limit IP addresses making connections over port 9100.
- Consider removing the default (0.0.0.0) gateway from the administrative networking panel. This will prevent responses from being returned to remote subnets.

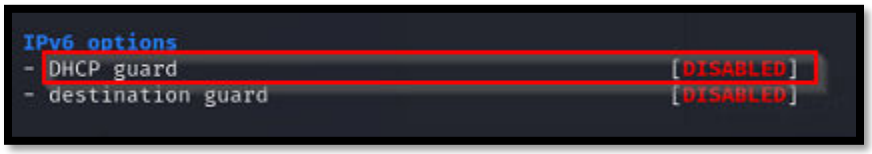
Reference(s):
http://h10032.www1.hp.com/ctg/Manual/c00746792.pdf
https://learn.microsoft.com/en-us/troubleshoot/windows-server/printing/install-configure-file-print-server

Affected Endpoint(s):

DHCP Guard Not Enabled
MITRE ATT&CK Tactic: TA0006-Credential Access
Detected: (QoD 85%) – **Impact**: Low – **Ease**: Low – **Risk**: Low

Summary:
DHCP guard is a feature that can help prevent malicious DHCP servers from assigning maliciously configured IP Addresses, Gateway settings, and DNS Server settings, which can be leveraged to conduct man-in-the-middle (MITM) attacks against endpoints.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Consider enabling a DHCP guard within Cisco Catalyst Switch to add an additional layer of protection against DHCP-based attacks.

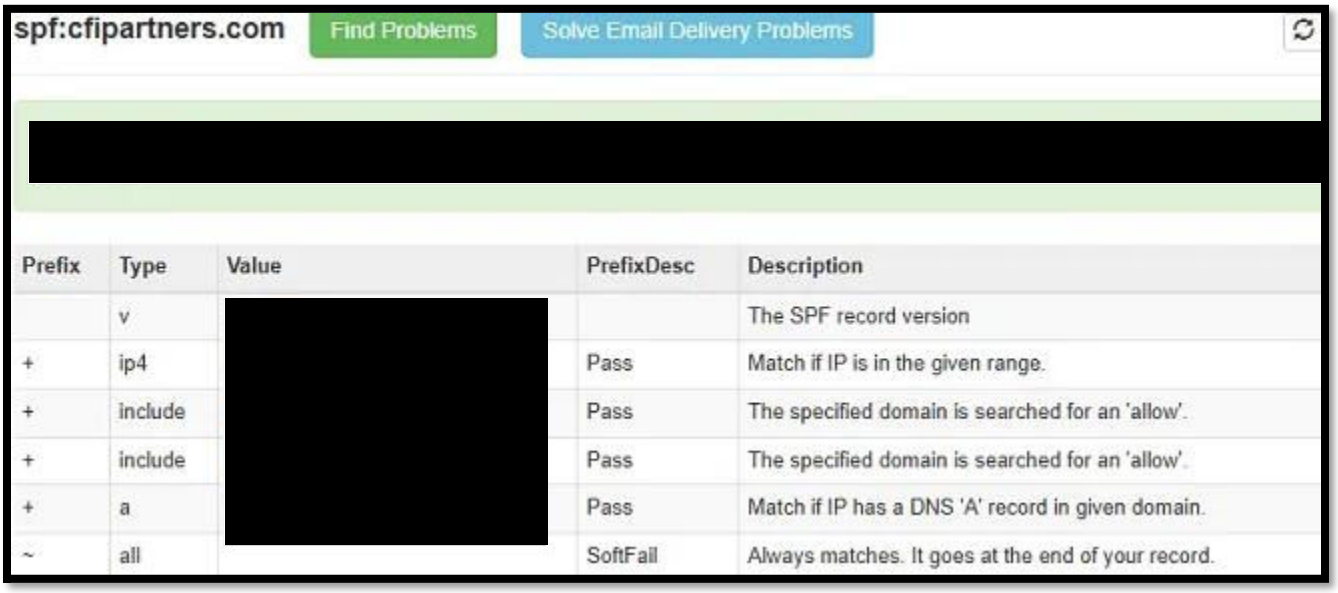
Reference(s):
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sga/configuration/guide/config/dhcp.html

Affected Endpoint(s):
[redacted]

Overly Permissive SPF Mail Record Is Susceptible to Social Engineering Exploitation
MITRE ATT&CK Tactic: TA0042-Resource Development
Informational

Summary:
The sender policy framework (SPF) record includes a specific entry for [redacted] Having such SPF entries can be particularly concerning as that means anyone on those identified networks (including anyone on guest Wi-Fi) could potentially spoof email for impersonating legitimate employees. Such a vulnerability would be a potential attack vector for a sophisticated internal social engineering attack.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- Reassess the necessity of included IPs to be specifically permitted within the SPF record. If any IP addresses are not needed, then the best practice would be to remove them from the record.
- It is possible that this vulnerability exists with regards to the office network because the IT department has multifunctional printers configured for 'scan to email' or network equipment setup with email alerts. The [redacted] team should consider utilizing authenticated SMTP rather than overly permissive SPF records or unauthenticated SMTP. Once authenticated SMTP is set up, the SPF record can be updated to have office IP addresses removed.

Reference(s):
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-spf-in-office-365-to-help-prevent-spoofing?view=o365-worldwid

Affected Endpoint(s):
[redacted]

Conclusion

While Abacus Group makes a best effort to rank the severity of vulnerabilities, it is not possible for any assessment to guarantee that low-risk issues cannot be chained together and significantly impact [redacted] systems. All risk ratings in this report are a combination of industry-standard ratings and considerations for unique business risk as identified by Abacus Group. Special consideration should also be given to the fact that multiple low-risk issues may compound into higher-risk threats.

Having exhausted all viable in-scope attack vectors, Abacus Group completed the external network penetration testing activities. Only two low-risk severity risk findings were identified. There are a few methods for ingress, and the use of social engineering would most likely be needed to obtain access to internal systems. Given the size and complexity of [redacted] attack surface, the relatively low quantity of findings indicates that it is a well-established security program. It is Abacus Group's belief that it would be challenging for a malicious actor to breach [redacted] external attack surface through purely technical means. It would likely take a yet unknown zero-day exploit or a highly sophisticated social engineering campaign for a malicious actor to infiltrate [redacted] internal network.

For the internal portion of the engagement, [redacted] has multiple avenues for improvement. Abacus Group completed the internal network penetration testing activities, identifying three high-risk, four moderate-risk, and three low-risk findings. From an internal perspective, [redacted] attack surface presented multiple avenues for practical exploitation. Given enough time, a malicious actor would be able to capture NTLMv2 hashes and take them offline to crack for credentialed access. Once credentialed access is established, a threat actor would then attempt to establish persistence and privilege escalation throughout the network to increase the availability of having re-entry into the environment should the security vendors catch the activity. A threat actor would also look to utilize credential reuse within the environment to access Microsoft Entra and, if possible, move into cloud-based resources to establish persistence. Following additional avenues of attack, a threat actor would leverage Cisco Smart Installer to conduct a buffer overflow on the current Cisco hardware to grab live network configuration files, which ultimately leads to Cisco Privilege 15 (the highest level of access that grants full administrative privileges) hashes for multiple users within the environment. This would then allow a threat actor to have easy methods of persistence and unfettered access through networking equipment, not just Active Directory and/or Entra/Cloud environments. Lastly, a threat actor could leverage [redacted], commonly known as regreSSHion, to gain privileged credential access within the network.

Through social engineering, Abacus Group successfully compromised one member of the [redacted] staff. Four separate social engineering campaigns were executed, which were created to replicate the vantage point of a moderately sophisticated actor who was intent on targeting [redacted] via social engineering. These campaigns were aimed at testing both the technical security controls and end-user security awareness. Each campaign was tailored to common tactics employed by real-world malicious actors, and the campaigns also leveraged multiple forms of communication.

Across the four campaigns, it should be recognized that [redacted] demonstrated mature technical security controls and moderately strong end-user security awareness. With that in mind, Abacus Group was able to leverage a form of communication (SMS Phishing) to bypass these controls and successfully compromise one staff member. Though this compromise lasted roughly one hour, and persistence was unable to be established, Abacus Group could have executed follow-on attacks that would have likely had a severe impact on the organization. This is especially true considering that external and internal personnel could have been targeted through access to both Outlook and Teams. [redacted] should consider bolstering technical security controls through additional conditional access policies. End-user awareness training should also be continually prioritized, with a focus on campaigns that involve other forms of communication. Organizations are always susceptible to social engineering, but it is Abacus Group's belief that with the aforementioned recommendations, it would likely be challenging for a malicious actor of moderate sophistication to succeed.

It is important to note that the risk mitigation recommendations contained in this report reflect industry best practices and Abacus Group's limited knowledge of [redacted] Abacus Group does not warrant the compatibility or operational effectiveness of the risk mitigation recommendations provided in this report, as Abacus Group does not have any understanding of the nuances and caveats of [redacted] network environment. Abacus Group highly recommends that [redacted] technology department assesses the compatibility and operational effectiveness of the risk mitigation recommendations provided in this report and uses a change management process to validate, plan and implement remediation changes in a UAT environment first.

Appendix A – MITRE ATT&CK Tactic Definitions

TA0043 – Reconnaissance
Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

TA0042 – Resource Development
Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access or stealing code signing certificates to help with Defense Evasion.

TA0001 – Initial Access
Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

TA0002 – Execution
Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

TA0003 – Persistence
Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

TA0004 – Privilege Escalation
Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

TA0005 – Defense Evasion
Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross listed here when those techniques include the added benefit of subverting defenses.

TA0006 – Credential Access
Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

TA0007 – Discovery
Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

TA0008 – Lateral Movement
Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

TA0009 – Collection
Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

TA0011 – Command and Control
Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

TA0010 – Exfiltration
Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command-and-control channel or an alternate channel and may also include putting size limits on the transmission.

TA0040 – Impact
Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.