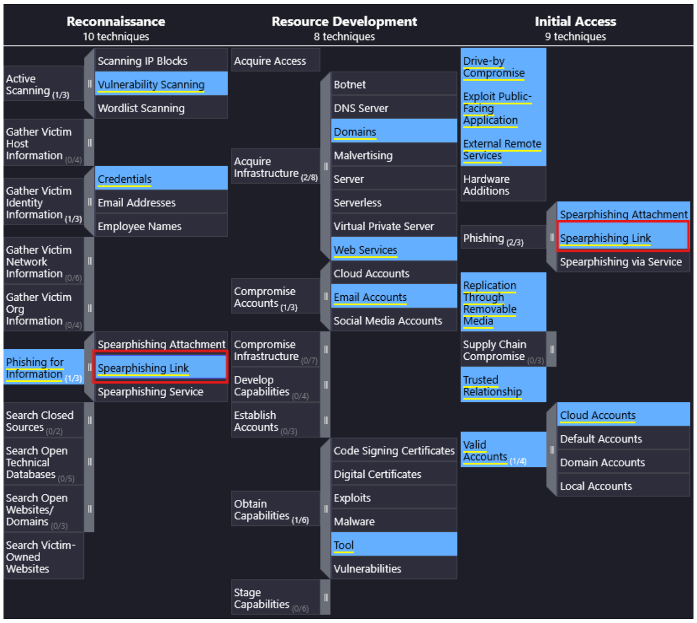
THM Challenge: Eviction
Difficulty: Easy
Ron

Eviction

Q1: What is a technique used by the APT to both perform recon and gain initial access?
Checking the *Reconnaissance* and Initial *Access stages* of the APT28 group in the MITRE ATT&CK Navigator, we see that in both stages the "Spearphishing Link"(T1598.003) sub-technique was used to harvest and later take advantage of the harvested credentials to gain access to the target network.



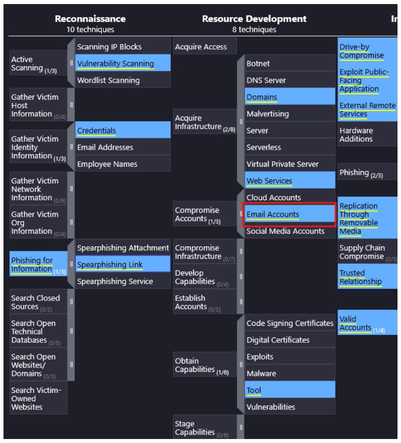
Reconnaissance
10 techniques
- Active Scanning (1/3)
  - Scanning IP Blocks
  - Vulnerability Scanning
  - Wordlist Scanning
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (1/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing Service
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/ Domains (0/3)
- Search Victim-Owned Websites

Resource Development
8 techniques
- Acquire Access
- Acquire Infrastructure (2/8)
  - Botnet
  - DNS Server
  - Domains
  - Malvertising
  - Server
  - Serverless
  - Virtual Private Server
  - Web Services
- Compromise Accounts (1/3)
  - Cloud Accounts
  - Email Accounts
  - Social Media Accounts
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (1/6)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
  - Tool
  - Vulnerabilities
- Stage Capabilities (0/6)

Initial Access
9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

ANSWER: *Spearphishing link*

Q2: Sunny identified that the APT might have moved forward from the recon phase. Which accounts might the APT compromise while developing resources?
Looking at the *Resource Development* tactic, we see that "Email Accounts"(T1586.002) sub-technique was utilized, and used compromised email accounts to send credential phishing emails and potentially send malicious spam.



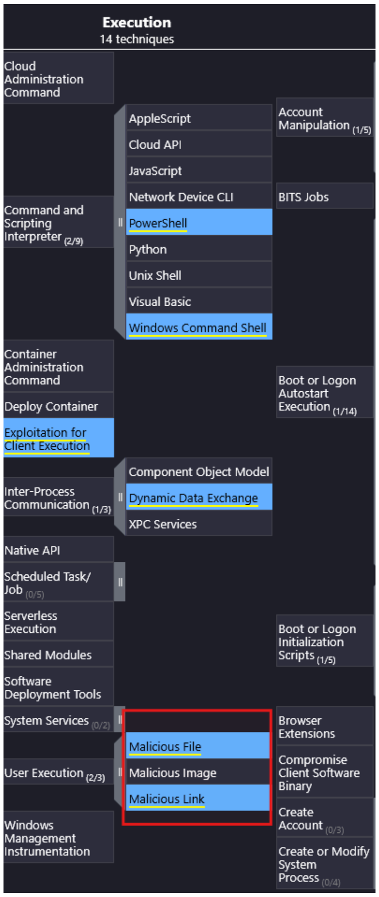
Reconnaissance
10 techniques
- Active Scanning (1/3)
  - Scanning IP Blocks
  - Vulnerability Scanning
  - Wordlist Scanning
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (1/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing Service
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/ Domains (0/3)
- Search Victim-Owned Websites

Resource Development
8 techniques
- Acquire Access
- Acquire Infrastructure (2/8)
  - Botnet
  - DNS Server
  - Domains
  - Malvertising
  - Server
  - Serverless
  - Virtual Private Server
  - Web Services
- Compromise Accounts (1/3)
  - Cloud Accounts
  - Email Accounts
  - Social Media Accounts
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (1/6)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
  - Tool
  - Vulnerabilities
- Stage Capabilities (0/6)

Ir
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts (1/4)

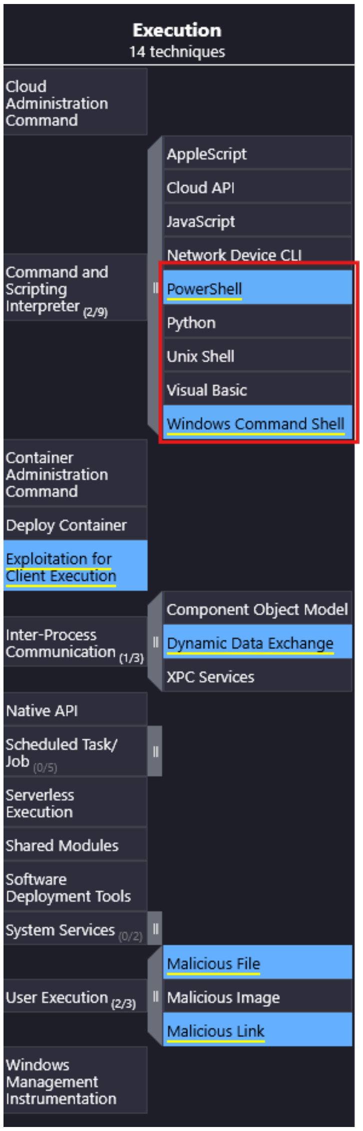
ANSWER: *Email accounts*

Q3: E-corp has found that the APT might have gained initial access using social engineering to make the user execute code for the threat actor. Sunny wants to identify if the APT was also successful in execution. What two techniques of user execution should Sunny look out for? (Answer format: <technique 1> and <technique 2>)
Reading through the “Email Accounts” technique we learn that “*adversaries may target compromising well-known email accounts or domains from which malicious spam or emails may evade reputation-based email filtering rules”*. Assuming that a user had already executed malicious code, it could have been in the form of a “Malicious Link”(T1204.001) or a “Malicious File”(T1204.002) that was sent to the victim.


Execution
14 techniques
Cloud Administration Command
AppleScript
Cloud API
JavaScript
Network Device CLI
PowerShell
Python
Unix Shell
Visual Basic
Windows Command Shell
Account Manipulation (1/5)
BITS Jobs
Command and Scripting Interpreter (2/9)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Boot or Logon Autostart Execution (1/14)
Component Object Model
Dynamic Data Exchange
XPC Services
Inter-Process Communication (1/3)
Native API
Scheduled Task/ Job (0/5)
Serverless Execution
Shared Modules
Software Deployment Tools
Boot or Logon Initialization Scripts (1/5)
System Services (0/2)
Malicious File
Malicious Image
Malicious Link
User Execution (2/3)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Windows Management Instrumentation
Create or Modify System Process (0/4)

ANSWER: *Malicious file and malicious link*

Q4: If the above technique was successful, which scripting interpreters should Sunny search for to identify successful execution? (Answer format: <technique 1> and <technique 2>)
Assuming the previously mentioned technique was successful, we should search for the “Powershell”(T1059.001) interpreter that is used to download and execute PowerShell scripts and perform PowerShell commands, as well as the “Windows Command Shell”(T1059.003) interpreter, that uses a cmd.exe and batch script to run a payload of a trojan.

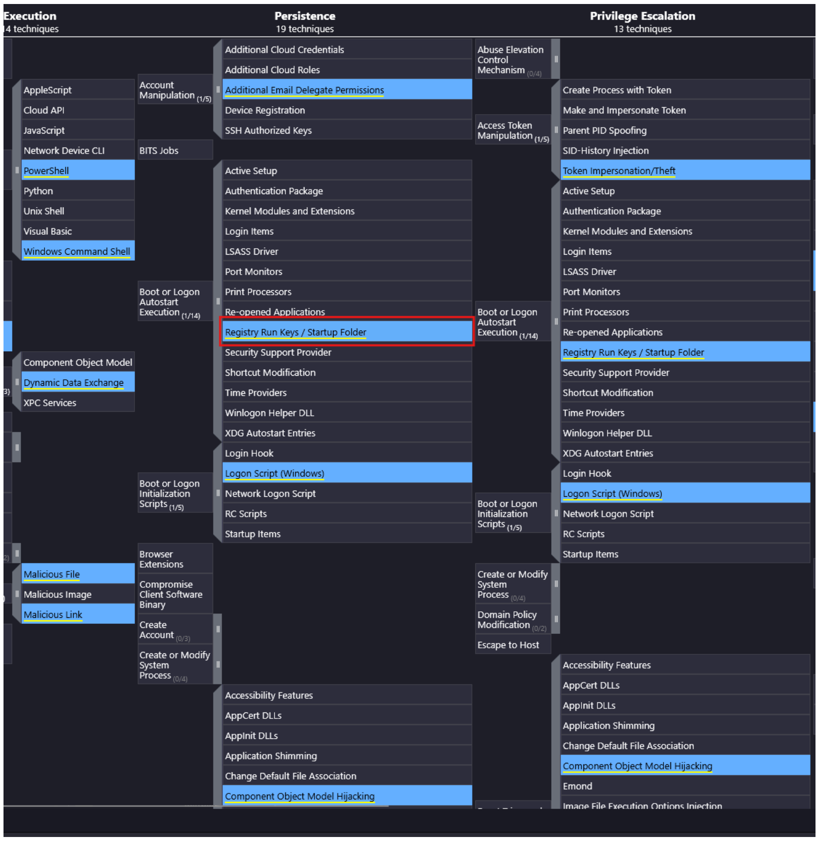


Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (2/9)
  - AppleScript
  - Cloud API
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (1/3)
  - Component Object Model
  - Dynamic Data Exchange
  - XPC Services
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)
  - Malicious File
  - Malicious Image
  - Malicious Link
- Windows Management Instrumentation

ANSWER: *Powershell and Windows Command shell*

Q5: While looking at the scripting interpreters identified in Q4, Sunny found some obfuscated scripts that changed the registry. Assuming these changes are for maintaining persistence, which registry keys should Sunny observe to track these changes?
Assuming the adversary obfuscated scripts that changed the registry to maintain persistence, we move forward to the “Persistence” tactic, there we can find that APT28 often takes advantage of “Registry Run Keys / Startup Folder”(T1547.001) sub-technique, to use the entries that allow programs to automatically execute when a user logs on.



Execution
4 techniques

AppleScript
Cloud API
JavaScript
Network Device CLI
PowerShell
Python
Unix Shell
Visual Basic
Windows Command Shell
Component Object Model
Dynamic Data Exchange
XPC Services
Malicious File
Malicious Image
Malicious Link

Persistence
19 techniques

Account Manipulation (1/5)
Additional Cloud Credentials
Additional Cloud Roles
Additional Email Delegate Permissions
Device Registration
SSH Authorized Keys

BITS Jobs

Boot or Logon Autostart Execution (1/14)
Active Setup
Authentication Package
Kernel Modules and Extensions
Login Items
LSASS Driver
Port Monitors
Print Processors
Re-opened Applications
Registry Run Keys / Startup Folder
Security Support Provider
Shortcut Modification
Time Providers
Winlogon Helper DLL
XDG Autostart Entries

Boot or Logon Initialization Scripts (1/5)
Login Hook
Logon Script (Windows)
Network Logon Script
RC Scripts
Startup Items

Browser Extensions
Compromise Client Software Binary
Create Account (0/3)

Create or Modify System Process (0/4)
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Change Default File Association
Component Object Model Hijacking

Privilege Escalation
13 techniques

Abuse Elevation Control Mechanism (0/4)

Access Token Manipulation (1/5)
Create Process with Token
Make and Impersonate Token
Parent PID Spoofing
SID-History Injection
Token Impersonation/Theft

Boot or Logon Autostart Execution (1/14)
Active Setup
Authentication Package
Kernel Modules and Extensions
Login Items
LSASS Driver
Port Monitors
Print Processors
Re-opened Applications
Registry Run Keys / Startup Folder
Security Support Provider
Shortcut Modification
Time Providers
Winlogon Helper DLL
XDG Autostart Entries

Boot or Logon Initialization Scripts (1/5)
Login Hook
Logon Script (Windows)
Network Logon Script
RC Scripts
Startup Items

Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host

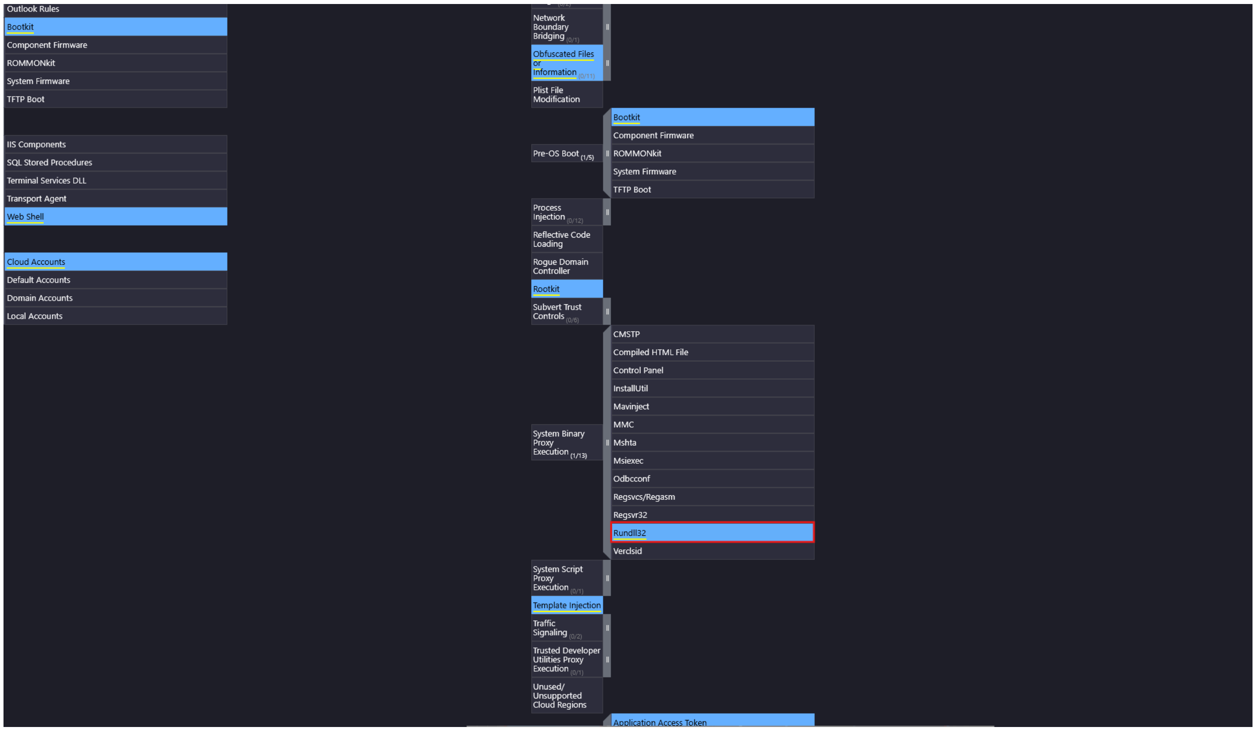
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Change Default File Association
Component Object Model Hijacking
Emond
Image File Execution Options Injection

ANSWER: *Registry run keys*

Q6: Sunny identified that the APT executes system binaries to evade defences. Which system binary's execution should Sunny scrutinize for proxy execution?

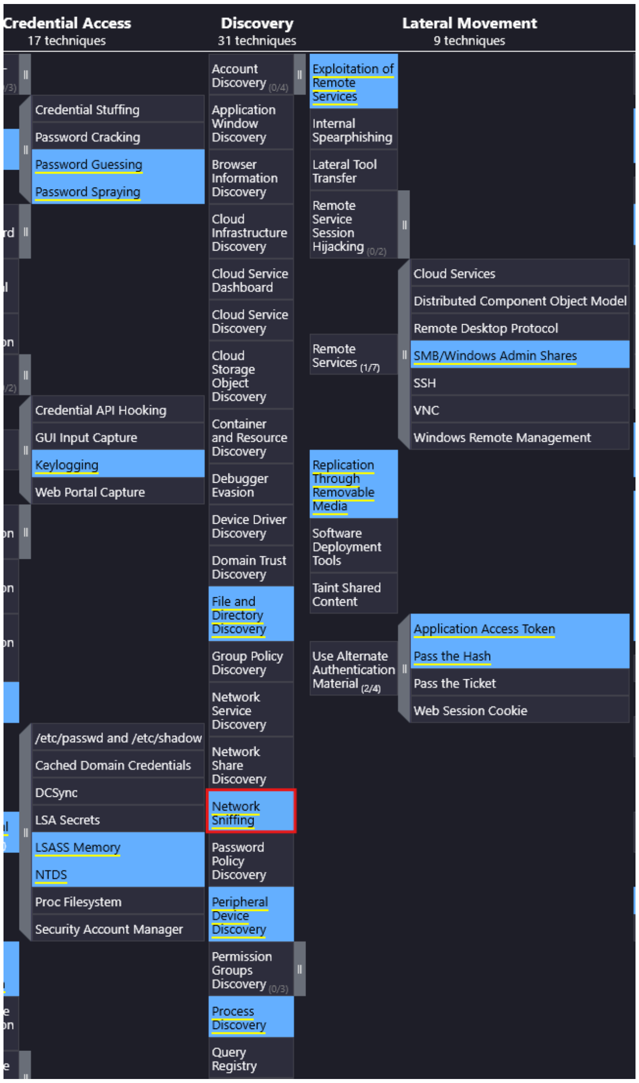
According to MITRE - *"Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries."*

Moving to the *Defense Evasion* tactic to look for a technique that could've been used for that, we see the Rundll32(T1218.011) sub-technique. adversaries abuse the Rundll32.exe file to avoid triggering security tools that may not monitor its execution.



ANSWER: *Rundll32*

Q7: Sunny identified tcpdump on one of the compromised hosts. Assuming this was placed there by the threat actor, which technique might the APT be using here for discovery?
Based on the findings, we proceed to the *Discovery* tactic where we can find “Network Sniffing”(T1040) which can be used to monitor network traffic to capture information about the environment.



Credential Access
17 techniques

- Credential Stuffing
- Password Cracking
- Password Guessing
- Password Spraying
- Credential API Hooking
- GUI Input Capture
- Keylogging
- Web Portal Capture
- /etc/passwd and /etc/shadow
- Cached Domain Credentials
- DCSync
- LSA Secrets
- LSASS Memory
- NTDS
- Proc Filesystem
- Security Account Manager

Discovery
31 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry

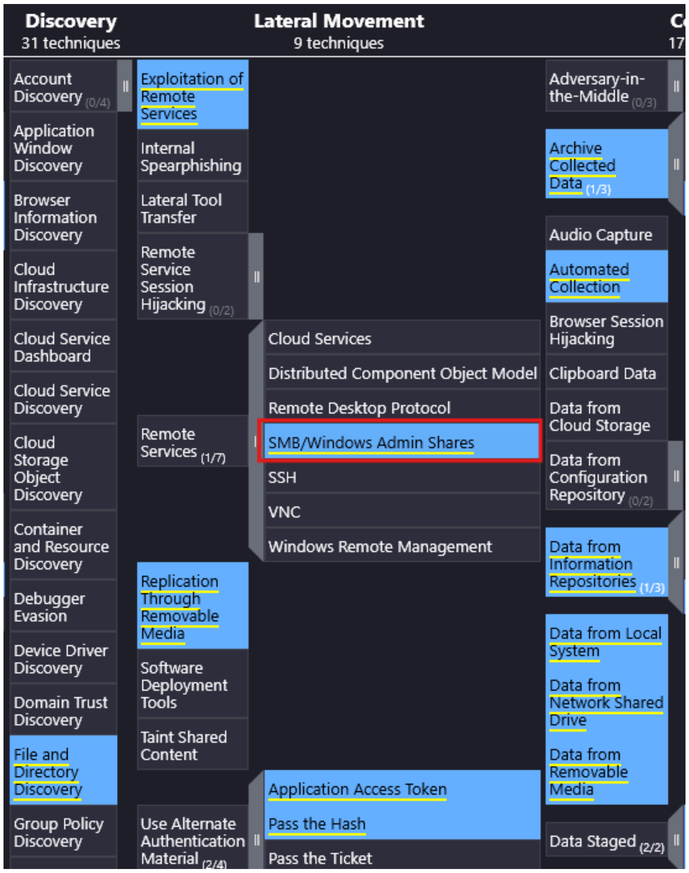
Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (1/7)
  - Cloud Services
  - Distributed Component Object Model
  - Remote Desktop Protocol
  - SMB/Windows Admin Shares
  - SSH
  - VNC
  - Windows Remote Management
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (2/4)
  - Application Access Token
  - Pass the Hash
  - Pass the Ticket
  - Web Session Cookie

ANSWER: *Network sniffing*

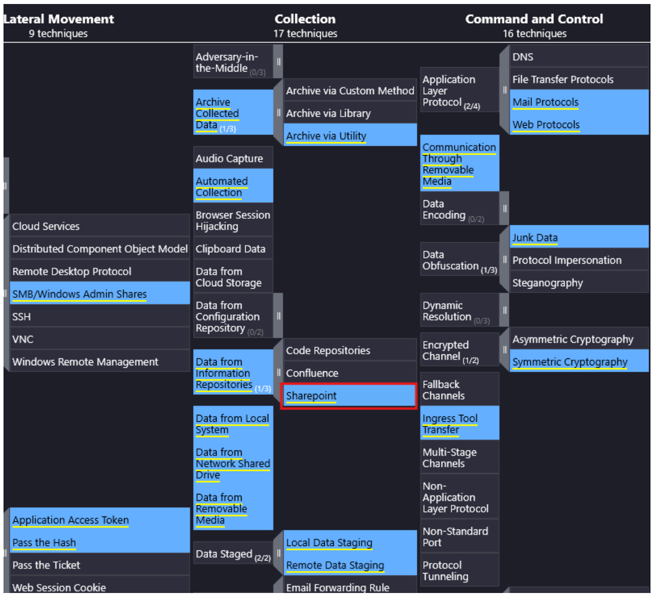
Q8: It looks like the APT achieved lateral movement by exploiting remote services. Which remote services should Sunny observe to identify APT activity traces?

Knowing that the adversary achieved lateral movement by exploiting remote services going over the different remote services sub-techniques we see “SMB/Windows Admin Shares”(T1021.002) which is used to interact with a remote network share using Server Message Block and falls inline with what we are looking for.


Discovery
31 techniques
Lateral Movement
9 techniques
C
17
Account Discovery (0/4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (1/7)
Cloud Services
Distributed Component Object Model
Remote Desktop Protocol
SMB/Windows Admin Shares
SSH
VNC
Windows Remote Management
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (2/4)
Application Access Token
Pass the Hash
Pass the Ticket
Adversary-in-the-Middle (0/3)
Archive Collected Data (1/3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (1/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2/2)

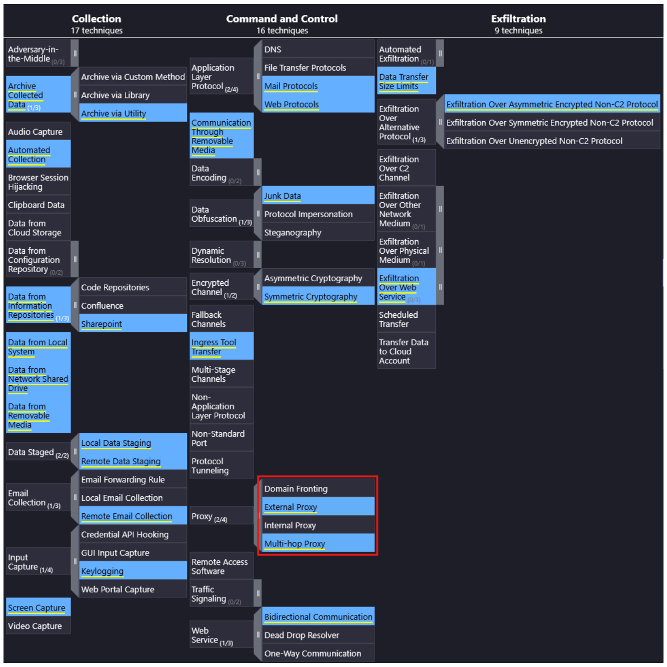
ANSWER: *SMB/Windows Admin shares*

Q9: It looked like the primary goal of the APT was to steal intellectual property from E-corp's information repositories. Which information repository can be the likely target of the APT?
This time we're looking for a certain "Data from Information Repositories" sub-technique as we suspect that stealing intellectual property was the goal of the adversary. As SharePoint allows for storage, retrieval, searching, archiving, tracking, management, and reporting on electronic documents and records, it seems like "Sharepoint(T1213.002)" sub-technique is what we're looking for, as it is often used as a source to mine valuable information.



ANSWER: *Sharepoint*

Q10: Although the APT had collected the data, it could not connect to the C2 for data exfiltration. To thwart any attempts to do that, what types of proxy might the APT use? (Answer format: <technique 1> and <technique 2>)
To manage command and control communication, the adversary might use the “External Proxy”(T1090.002) to act as an intermediary for network communications to avoid direct connections to their infrastructure. and “Multi-hop Proxy”(T1090.003) which can be used to chain together multiple proxies to disguise the source of malicious traffic.



ANSWER: *“external proxy and multi-hop proxy”*