Table Top Exercises using Backdoors and Breaches

Table of Contents

Improving Incident Response Effectiveness Using Tabletop Exercise Simulations

- Helps the blue team understand how adversaries operate
- Helps the blue team understand the effectiveness of different types of defences against each type of attack
- Helps blue team understand the effectiveness of their defence architecture and its weakness
- Helps blue team understand the effectiveness of each incident response procedure d and what can make it fail
- Helps blue team prepare for incident response by asking crucial questions needed during incident response
- Helps the blue team to document and practice response to incidents before they occur

Play Backdoors and Breaches Online

- https://play.backdoorsandbreaches.com/play.backdoorsandbreaches.com-Engine-V1/App/

Rules of Backdoors and Breaches

- Types of players:
    - Incident Master
        - Drives the game, what they say goes
        - Draws 4 cards to "build" the incident
        - Keeps the game going
    - Players
        - Draw 4 Established Procedure cards
        - Discuss and take actions
        - Roll dice on actions
- Dice – They get rolled
    - 11 and over == Success
    - 10 and lower == fail
    - +3 on Established Procedures

How Backdoors and Breaches works?

1. Incident Master builds the incident using one card from each part of the attack chain (Initial Access, Pivot and Escalate, C2 and Exfil, and Persistence) and doesn't show the attack chain to the players – Attack chain may be random or based on any incident response reports (as done below in "Scenarios" section)

2. Players choose 4 Established Procedure cards

3. Incident Master provides an initial scenarios under which the incident is discussed

4. During 10 turns to identify the attack chain, the players are allowed to ask two types of questions:

    1. Seeking Clarity Questions: These questions are aimed at gaining more information or understanding about the scenario or specific details.

    2. Analysis and Action Questions: Players propose these actions to investigate and respond to the incident further.

5. In 10 turns, the players try to identify the attack chain cards by choosing a procedure to identify any one of the incident cards, and then roll a D20 dice to verify if the procedure card is a success or a failure – +3 for established procedures

    1. In the event of success (11 or higher), Incident Master reveals if the procedure has identified any one of the incident cards and if yes, then which one – Incident Master reveals only one incident card, if there are more than one incident cards that the procedure can reveal to simulate the nature of incident response

    2. In the event of failure (10 or lower), Incident Master provides a reason for the failure of the procedure or asks the players "Can you give me a reason technologically, financially, politically, or personnel-wise why [specific procedure] would be unsuccessful at this time?" to discuss why this procedure might fail during incident response

    3. In the event of rolling a pure 1 or pure 20, or having three consecutive failures, the Incident Master picks an inject card simulating the nature of events occurring during incident response, and the players discuss how this scenario affects their incident response, the reasons for this taking place, and the steps to take to address this scenario

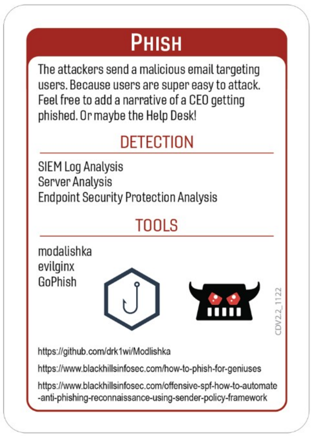
Scenarios

The attack chain can be constructed using Incident Response reports by identifying the incident cards involved in the attack, providing realistic attack scenarios and facilitating in-depth discussions.

Scenario – 1 – Black Basta Ransomware

Incident Report: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

Attack Chain:



PHISH

The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!

DETECTION

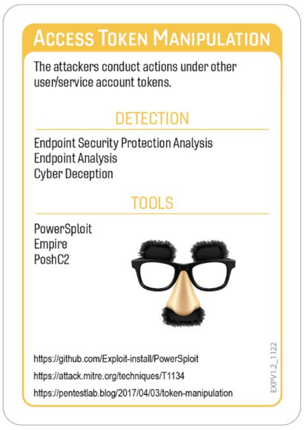
SIEM Log Analysis
Server Analysis
Endpoint Security Protection Analysis

TOOLS

modalishka
evilginx
GoPhish

https://github.com/drk1wi/Modlishka
https://www.blackhillsinfosec.com/how-to-phish-for-geniuses
https://www.blackhillsinfosec.com/offensive-spf-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework

CDV2.2_1122



ACCESS TOKEN MANIPULATION

The attackers conduct actions under other user/service account tokens.

DETECTION

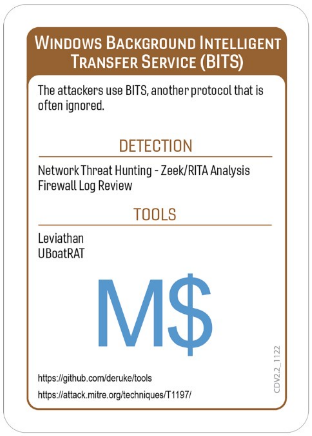
Endpoint Security Protection Analysis
Endpoint Analysis
Cyber Deception

TOOLS

PowerSploit
Empire
PoshC2

https://github.com/Exploit-install/PowerSploit
https://attack.mitre.org/techniques/T1134
https://pentestlab.blog/2017/04/03/token-manipulation

EXPV1.2_1122



WINDOWS BACKGROUND INTELLIGENT TRANSFER SERVICE (BITS)

The attackers use BITS, another protocol that is often ignored.

DETECTION

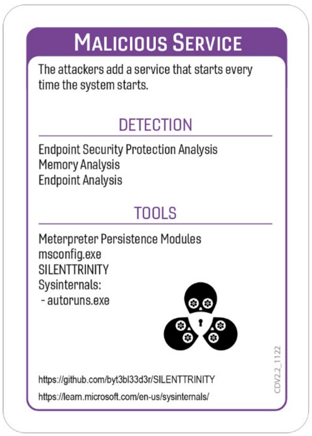
Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

Leviathan
UBoatRAT

https://github.com/deruke/tools
https://attack.mitre.org/techniques/T1197/

CDV2.2_1122



MALICIOUS SERVICE

The attackers add a service that starts every time the system starts.

DETECTION

Endpoint Security Protection Analysis
Memory Analysis
Endpoint Analysis

TOOLS

Meterpreter Persistence Modules
msconfig.exe
SILENTTRINITY
Sysinternals:
- autoruns.exe

https://github.com/byt3bl33d3r/SILENTTRINITY
https://learn.microsoft.com/en-us/sysinternals/

CDV2.2_1122

Initial Scenario: Your organization has recently launched a new internal project, and team members are receiving numerous emails related to project updates and collaboration tools. Amidst these legitimate emails, a spearphishing email mimicking a trusted colleague or partner has been sent to several employees. The email contains a link to a malicious website designed to steal credentials.

Initial Access – Phish: Adversary uses spearphishing emails to obtain initial access.

Pivot & Escalate – Access Token Manipulation: They use credential scraping tools like Mimikatz for privilege escalation, exploiting vulnerabilities such as ZeroLogon and PrintNightmare.

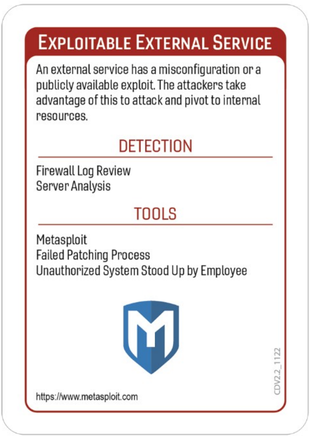
C2 & Exfiltrate – Windows Background Intelligent Transfer Service (BITS): They use BITSAdmin to manage file transfers, facilitating command and control as well as data exfiltration.

Persistence – Malicious Service: They create malicious services for persistence, utilizing tools such as Backstab to disable endpoint detection and response (EDR) tooling.

Scenario – 2 – Akira Ransomware

Incident Report: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

Attack Chain:



EXPLOITABLE EXTERNAL SERVICE

An external service has a misconfiguration or a publicly available exploit. The attackers take advantage of this to attack and pivot to internal resources.

DETECTION

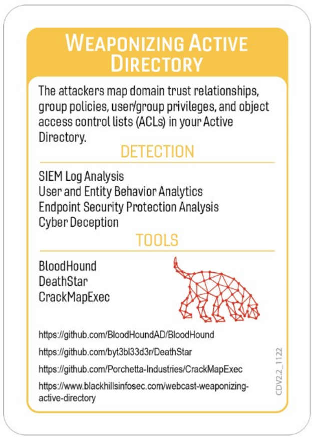
Firewall Log Review
Server Analysis

TOOLS

Metasploit
Failed Patching Process
Unauthorized System Stood Up by Employee

https://www.metasploit.com

CDV2.2_1122



WEAPONIZING ACTIVE DIRECTORY

The attackers map domain trust relationships, group policies, user/group privileges, and object access control lists (ACLs) in your Active Directory.

DETECTION

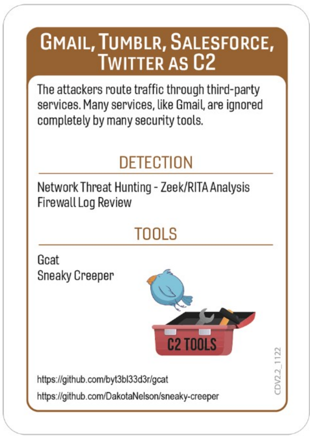
SIEM Log Analysis
User and Entity Behavior Analytics
Endpoint Security Protection Analysis
Cyber Deception

TOOLS

BloodHound
DeathStar
CrackMapExec

https://github.com/BloodHoundAD/BloodHound
https://github.com/byt3bl33d3r/DeathStar
https://github.com/Porchetta-Industries/CrackMapExec
https://www.blackhillsinfosec.com/webcast-weaponizing-active-directory

CDV2.2_1122



GMAIL, TUMBLR, SALESFORCE, TWITTER AS C2

The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.

DETECTION

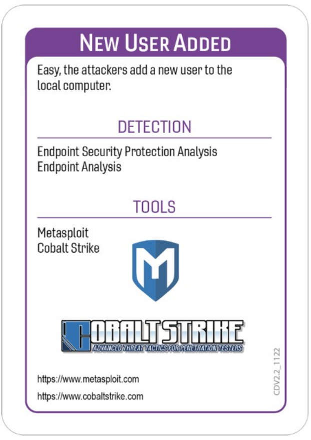
Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

Gcat
Sneaky Creeper

https://github.com/byt3bl33d3r/gcat
https://github.com/DakotaNelson/sneaky-creeper

CDV2.2_1122



NEW USER ADDED

Easy, the attackers add a new user to the local computer.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Metasploit
Cobalt Strike

COBALTSTRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

https://www.metasploit.com
https://www.cobaltstrike.com

CDV2.2_1122

Initial Scenario: Your organisation is a mid-sized financial services company and is recently upgraded its VPN infrastructure to Cisco. The IT Security team is currently working on implementing Multi-Factor Authentication (MFA) across all external services but has not completed the rollout yet. The organization relies heavily on remote access due to its flexible work policy, with many employees working from various locations.

Initial Access – Exploitable External Service: Akira ransomware threat actors gain initial access by exploiting public-facing applications and external remote services such as VPN without MFA configured, using Cisco vulnerabilities.

Pivot & Escalate – Weaponizing Active Directory: They leverage post-exploitation techniques like Kerberoasting and use tools such as Mimikatz and LaZagne to extract and escalate privileges, weaponizing Active Directory using kerberos attacks.

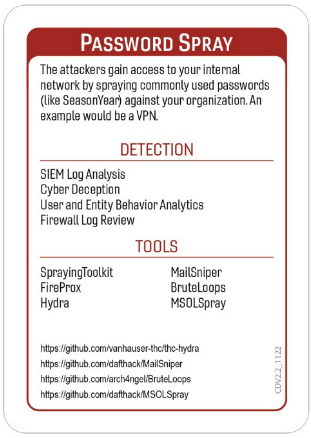
C2 & Exfiltrate – Gmail, Tumblr, Salesforce, Twitter as C2: Akira threat actors use various legitimate tools for command and control, including AnyDesk, MobaXterm, and Ngrok, and leverage cloud storage services like Mega for data exfiltration.

Persistence – New User Added: Persistence is achieved by creating new domain accounts, such as an administrative account named itadm.

Scenario – 3 – Phobos Ransomware

Incident Report: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a

Attack Chain:



PASSWORD SPRAY

The attackers gain access to your internal network by spraying commonly used passwords (like SeasonYear) against your organization. An example would be a VPN.

DETECTION

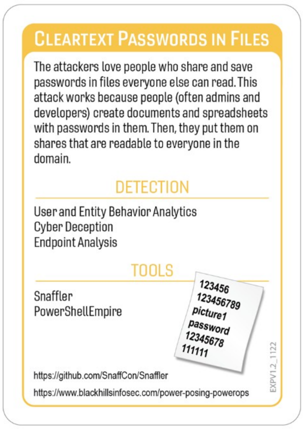
SIEM Log Analysis
Cyber Deception
User and Entity Behavior Analytics
Firewall Log Review

TOOLS

SprayingToolkit
FireProx
Hydra
MailSniper
BruteLoops
MSOLSpray

https://github.com/vanhauser-thc/thc-hydra
https://github.com/dafthack/MailSniper
https://github.com/arch4ngel/BruteLoops
https://github.com/dafthack/MSOLSpray

CDV2.2_1122



123456
123456789
picture1
password
12345678
111111

CLEARTEXT PASSWORDS IN FILES

The attackers love people who share and save passwords in files everyone else can read. This attack works because people (often admins and developers) create documents and spreadsheets with passwords in them. Then, they put them on shares that are readable to everyone in the domain.

DETECTION

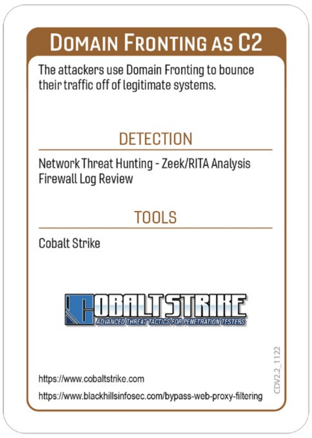
User and Entity Behavior Analytics
Cyber Deception
Endpoint Analysis

TOOLS

Snaffler
PowerShellEmpire

https://github.com/SnaffCon/Snaffler
https://www.blackhillsinfosec.com/power-posing-powerops

EXPV1.2_1122



COBALTSTRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

DOMAIN FRONTING AS C2

The attackers use Domain Fronting to bounce their traffic off of legitimate systems.

DETECTION

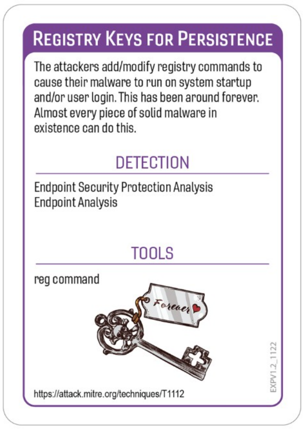
Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

Cobalt Strike

https://www.cobaltstrike.com
https://www.blackhillsinfosec.com/bypass-web-proxy-filtering

CDV2.2_1122



REGISTRY KEYS FOR PERSISTENCE

The attackers add/modify registry commands to cause their malware to run on system startup and/or user login. This has been around forever. Almost every piece of solid malware in existence can do this.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

reg command

https://attack.mitre.org/techniques/T1112

EXPV1.2_1122

Initial Scenario: Over the past week, the IT security team at XYZ Corp has noticed an increase in failed login attempts. These attempts are targeting various user accounts across multiple departments, occurring at irregular intervals. The patterns suggest a potential password spray attack.

Initial Access – Password Spray: Phobos actors often gain initial access through brute force attacks on vulnerable Remote Desktop Protocol (RDP) ports.

Pivot & Escalate – Cleartext Passwords in Files: Phobos actors use tools like Mimikatz to extract credentials, including cleartext passwords, from memory, browser, and password stores on compromised systems.

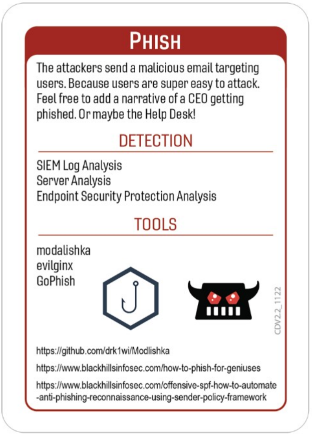
C2 & Exfiltrate – Domain Fronting as C2: Phobos actors have been observed using domain fronting techniques to disguise command-and-control (C2) traffic, making it appear as legitimate network traffic.

Persistence – Registry Keys for Persistence: Phobos actors maintain persistence by creating registry keys using Windows Startup folders.

Scenario – 4 – ALPHV Ransomware

Incident Report: https://thedfirreport.com/2024/06/10/icedid-brings-screenconnect-and-csharp-streamer-to-alphv-ransomware-deployment/

Attack Chain:



PHISH

The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!

DETECTION

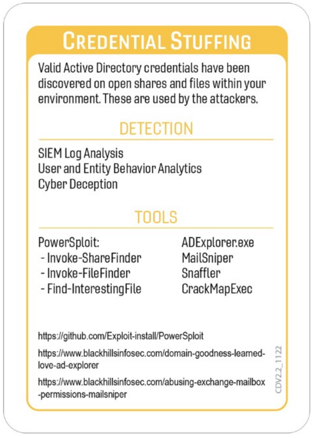
SIEM Log Analysis
Server Analysis
Endpoint Security Protection Analysis

TOOLS

modalishka
evilginx
GoPhish

https://github.com/drk1wi/Modlishka
https://www.blackhillsinfosec.com/how-to-phish-for-geniuses
https://www.blackhillsinfosec.com/offensive-spf-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework

CDV2.2_1122



CREDENTIAL STUFFING

Valid Active Directory credentials have been discovered on open shares and files within your environment. These are used by the attackers.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Cyber Deception

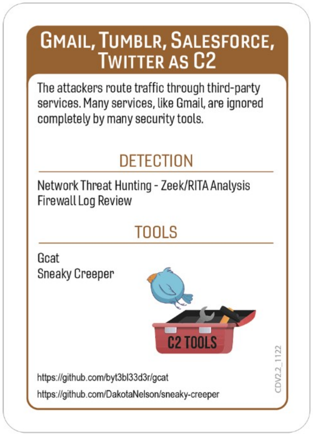
TOOLS

PowerSploit:
- Invoke-ShareFinder
- Invoke-FileFinder
- Find-InterestingFile

ADExplorer.exe
MailSniper
Snaffler
CrackMapExec

https://github.com/Exploit-install/PowerSploit
https://www.blackhillsinfosec.com/domain-goodness-learned-love-ad-explorer
https://www.blackhillsinfosec.com/abusing-exchange-mailbox-permissions-mailsniper

CDV2.2_1122



GMAIL, TUMBLR, SALESFORCE, TWITTER AS C2

The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.

DETECTION

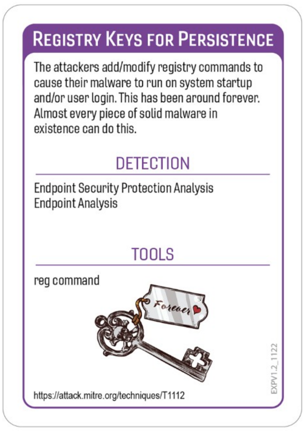
Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

Gcat
Sneaky Creeper

https://github.com/byt3bl33d3r/gcat
https://github.com/DakotaNelson/sneaky-creeper

CDV2.2_1122



REGISTRY KEYS FOR PERSISTENCE

The attackers add/modify registry commands to cause their malware to run on system startup and/or user login. This has been around forever. Almost every piece of solid malware in existence can do this.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

reg command

https://attack.mitre.org/techniques/T1112

EXPV1.2_1122

Initial Scenario: Your organization has been targeted by a sophisticated phishing campaign. Employees receive an email that appears to be from a trusted source, urging them to download an attached ZIP file.

Initial Access – Phish: The intrusion began with a malicious email campaign, enticing recipients to download a ZIP archive containing a Visual Basic Script (VBS) and a benign README file.

Pivot & Escalate – Credential Stuffing: The attacker used Impacket's wmiexec and RDP to install ScreenConnect on multiple systems, allowing execution of commands and deployment of Cobalt Strike beacons.

C2 & Exfiltrate – Gmail, Tumblr, Salesforce, Twitter as C2: The attacker used WebSockets for command and control and exfiltration purposes, leveraging various tools for data staging and exfiltration such as Rclone.

Persistence – Registry Keys for Persistence: Persistence was achieved via scheduled tasks for IcedID and auto-start services for ScreenConnect, which involved modifying registry keys to ensure these services started on reboot.

Reference

1. Antisyphon Training, "Backdoors and Breaches | Jason Blanchard | Offensive Con 2023," YouTube, 28-Feb-2023. [Online]. Available: https://www.youtube.com/watch?v=xFF9yn9s0I8. [Accessed: 25-Jun-2024].
2. Black Hills Information Security, "AASLR: Backdoors & Breaches Live," YouTube, 14-Dec-2020. [Online]. Available: https://www.youtube.com/watch?v=0hAeEQRBVIs. [Accessed: 25-Jun-2024].
3. Black Hills Information Security, "How to Play Backdoors & Breaches, Incident Response Card Game," YouTube, 17-Jun-2022. [Online]. Available: https://www.youtube.com/watch?v=TAiJVr0zWMw. [Accessed: 25-Jun-2024].
4. Black Hills Information Security, "How to Use Backdoors & Breaches to do Tabletop Exercises and Learn Cybersecurity," YouTube, 16-Apr-2020. [Online]. Available: https://www.youtube.com/watch?v=pMY2HXUrKsg. [Accessed: 25-Jun-2024].