Backdoors and Breaches

John Strand

Brought To You By!

Backdoors & Breaches

Brought To You By!

Just type “TRAINING,`<script>alert(document.cookie);</script>` `or ' 1=1;--`” into the Questions box

Why?

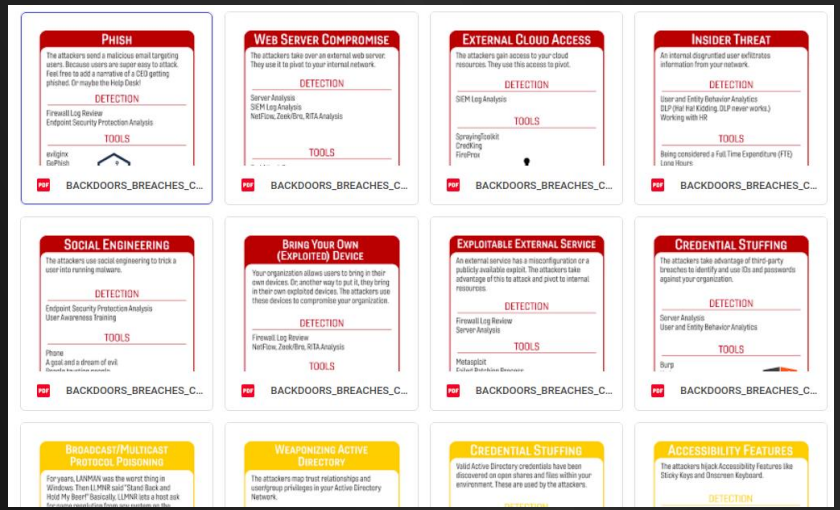
- Tabletops are not fun
- Arguments over what and what does not work
- Incomplete attack scenarios
- Magic unicorn hacks
- What matters?

"Well, we learned a lot about our IR processes and coworker weaknesses today."

State of Play

Roles

1. Incident Master
   a. Drives the game, what they say goes
   b. Draws 4 cards to “build” the incident
   c. Keeps the game going
2. Players
   a. Draw 4 PROCEDURE cards
   b. Discuss and take actions
   c. Roll dice on actions
3. Dice - They get rolled
   a. 11 and over == Success
   b. 10 and lower == fail
   c. +3 PROCEDURES



D&D Roots

- The goal is to build conversations
- Track missing procedures
- Talk through how your org would handle these issues
- It is not a monopoly-style game
  - Every action is ***not*** scripted
  - The IM decides
- It helps to get into roles

Breaking Down a Card

Title

Suggested Detects

Text

Example Tools

Links

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

Firewall Log Review
Endpoint Security Protection Analysis

TOOLS

evilginx
GoPhish
CredSniper

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

INITIAL COMPROMISE

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

Firewall Log Review
Endpoint Security Protection Analysis

TOOLS

evilginx
GoPhish
CredSniper

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

PIVOT and ESCALATE

INTERNAL PASSWORD SPRAY

The attackers start a password spray against the rest of the organization from a compromised system.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis

TOOLS

Domain Password Spray

https://github.com/dafthack/DomainPasswordSpray

https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack

PERSISTENCE

Malicious Browser Plugins

The attackers install plugins in the browser. This can be used as part of C2 and persistence. The browser is the new endpoint.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Web Proxy (Firewall Log Review)
NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Grammarly is a keylogger
graniet/chromebackdoor

https://www.kaspersky.com/blog/browser-extensions-security/20886

https://github.com/graniet/chromebackdoor

C2 and EXFIL

HTTPS as Exfil

This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Metasploit Reverse HTTPS Payloads
SILENTTRINITY

https://www.metasploit.com
https://attack.mitre.org/techniques/T1032
https://github.com/byt3bl33d3r/SILENTTRINITY

PROCEDURES

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter

https://www.activecountermeasures.com/free-tools/rita

https://securityonion.net

https://www.activecountermeasures.com

INJECTS

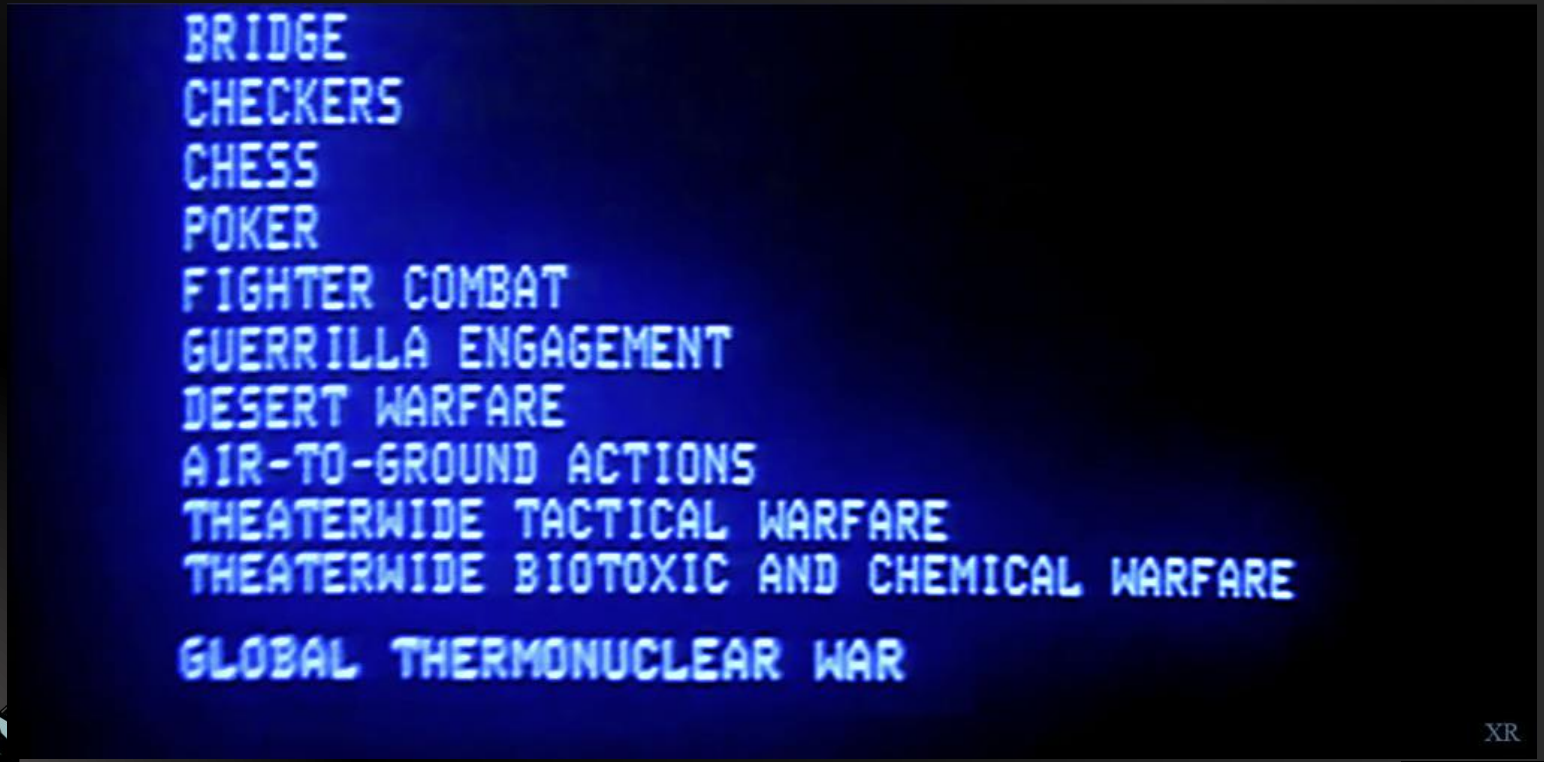
DATA UPLOADED TO PASTEBIN

Bummer, the attacker has posted internal sensitive data on Pastebin. Your customers are now informed of the attack by the media.

NOTES

It happens... a lot, but it's just pure evil. Time to bring in Upper Management and the Legal Team.

Let's Play


BRIDGE
CHECKERS
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE
GLOBAL THERMONUCLEAR WAR
XR

Game One: Procedures

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter

https://www.activecountermeasures.com/free-tools/rita
https://securityonion.net
https://www.activecountermeasures.com

Security Information and Event Management (SIEM) Log Analysis

Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tools Analysis

https://github.com/philhagen/sof-elk
https://jpcertcc.github.io/ToolAnalysisResultSheet

Endpoint Analysis

This is where the defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets

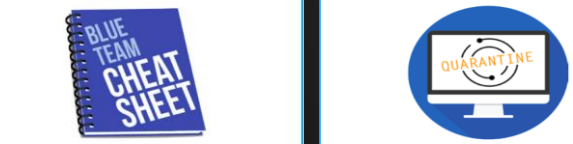
https://github.com/sans-blue-team/DeepBlueCLI

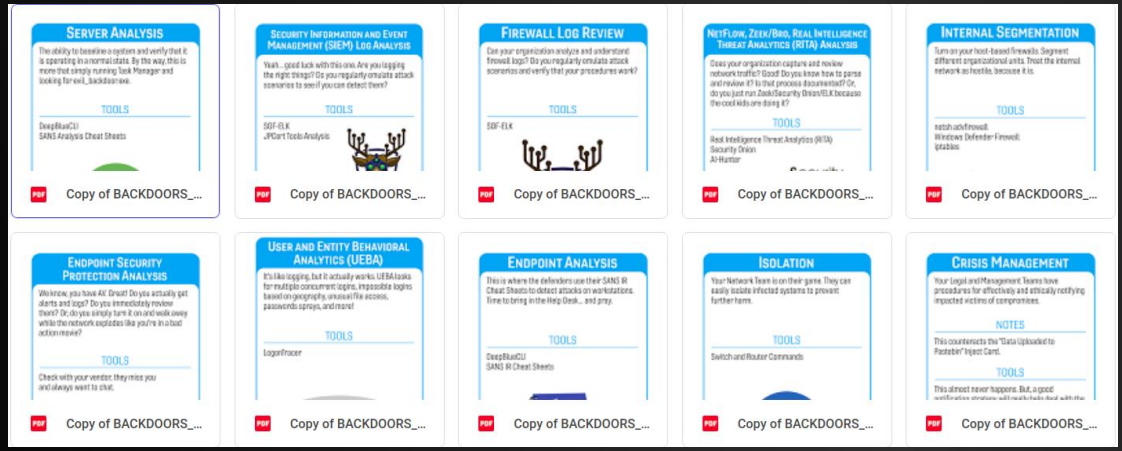
Isolation

Your Network Team is on their game. They can easily isolate infected systems to prevent further harm.

TOOLS

Switch and Router Commands





Game Two: Procedures

NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter

https://www.activecountermeasures.com/free-tools/rita
https://securityonion.net
https://www.activecountermeasures.com

Crisis Management

Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.

NOTES

This counteracts the "Data Uploaded to Pastebin" Inject Card.

TOOLS

This almost never happens. But, a good notification strategy will really help deal with the political fallout.

Endpoint Analysis

This is where the defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets

https://github.com/sans-blue-team/DeepBlueCLI

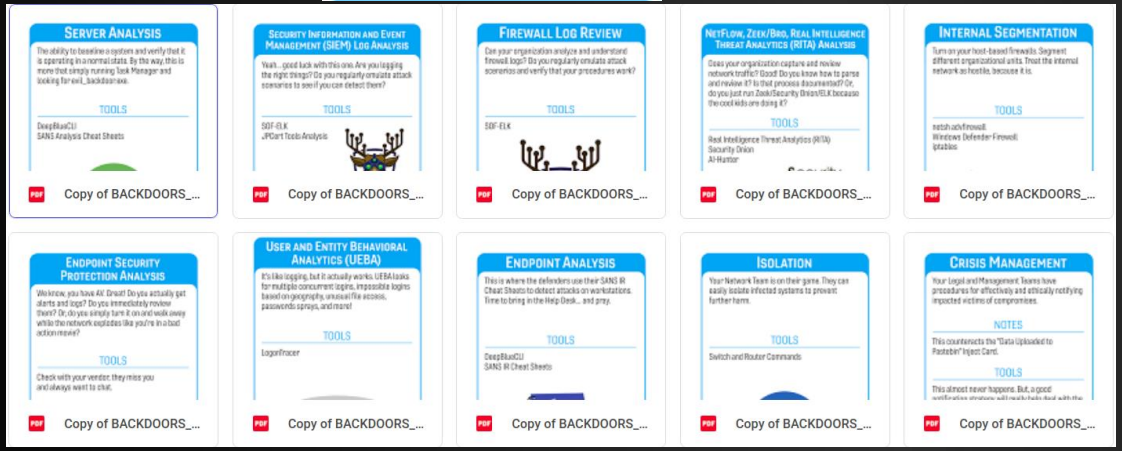
Firewall Log Review

Can your organization analyze and understand firewall logs? Do you regularly emulate attack scenarios and verify that your procedures work?

TOOLS

SOF-ELK

https://github.com/philhagen/sof-elk



Questions?

Backdoors & Breaches