



Backdoors and Breaches

John Strand



© Black Hills Information Security | @BHInfoSecurity



Brought To You By!



© Black Hills Information Security | @BHInfoSecurity



Brought To You By!



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



© Black Hills Information Security | @BHInfoSecurity



Why?

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



"Some days you just have to say,
"Screw it. I'm gonna be a unicorn.""



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



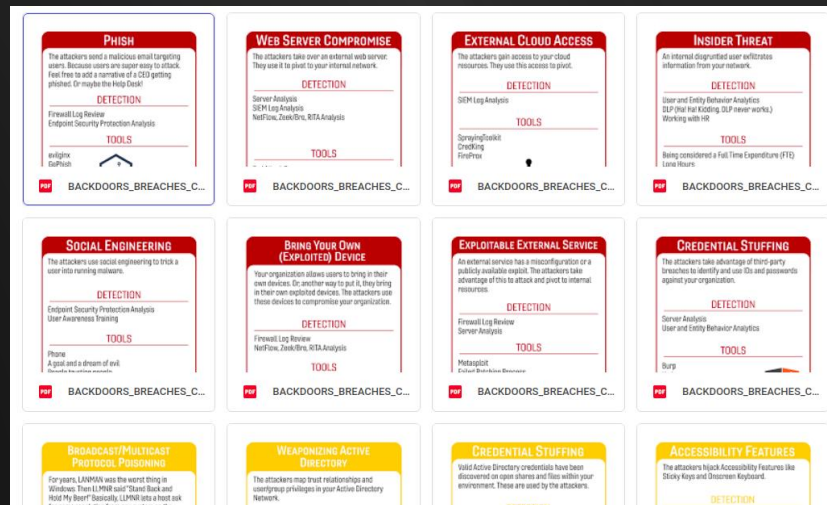
© Black Hills Information Security | @BHInfoSecurity

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



© Black Hills Information Security | @BlackHillsSecurity



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



© Black Hills Information Security | @BHInfoSecurity



Breaking Down a Card



Title

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!

Text

DETECTION

Firewall Log Review
Endpoint Security Protection Analysis

Suggested
Detects

TOOLS

evilginx
GoPhish
CredSniper



Example Tools



CREDSSNIPEr

<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>

Links



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



CRED SNIPER

<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>



© Black Hills Information Security | @BHInfoSec



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>



© Black Hills Information Security | @BHInfoSec

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://github.com/graniet/chromebackdoor)



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

<https://github.com/graniet/chromebackdoor>



© Black Hills Information Security | @BHInfoSec



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
SILENTRINITY

H_eT_vT_iP_s



<https://www.metasploit.com>

<https://attack.mitre.org/techniques/T1032>

<https://github.com/byt3bl33d3r/SILENTRINITY>



© Black Hills Information Security | @BHInfoSec



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>



© Black Hills Information Security | @BHInfoSec



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



© Black Hills Information Security | @BHInfoSecurity



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



JPCERT

<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



SERVER ANALYSIS

The ability to baseline a system and verify that it is operating as normal. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets

Copy of BACKDOORS...

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

Copy of BACKDOORS...

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

Copy of BACKDOORS...

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

Copy of BACKDOORS...

INTERNAL SEGMENTATION

Turn on your host-based firewalls. Segment different organizational units. Trust the internal network as hosts, because it is.

TOOLS

Windows Firewall
Windows Defender Firewall
iptables

Copy of BACKDOORS...

ENDPOINT SECURITY PROTECTION ANALYSIS

Who knew you had AI? Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

TOOLS

Check with your vendor they miss you and always want to chat.

Copy of BACKDOORS...

USER AND ENTITY BEHAVIORAL ANALYTICS (UEBA)

It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays, and more!

TOOLS

LogonTracer

Copy of BACKDOORS...

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

Copy of BACKDOORS...

ISOLATION

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

TOOLS

Switch and Router Commands

Copy of BACKDOORS...

CRISIS MANAGEMENT

Your Legal and Management Teams have procedures for effectively and ethically restoring impacted victims of compromise.

NOTES

This connects the "Data Uploaded to Pastebin" Input Card.

TOOLS

This almost never happens. But, a good crisis management plan will reach into Red with the

Copy of BACKDOORS...



© Black Hills Information Security | @BHInfoSecurity

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/philiagen/sf-elk>

SERVER ANALYSIS

The ability to baseline a system and verify that it is operating as normal is critical. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.

TOOLS

DeepBlueCLI
SANS Analysis Cheat Sheets

Copy of BACKDOORS...

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
iPCart Tools Analysis



Copy of BACKDOORS...

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



Copy of BACKDOORS...

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

Copy of BACKDOORS...

INTERNAL SEGMENTATION

Turn on your host-based firewalls. Segment different organizational units. Trust the internal network as hosts, because it is.

TOOLS

Windows Defender Firewall
iptables

Copy of BACKDOORS...

ENDPOINT SECURITY PROTECTION ANALYSIS

Who knew you have AI? Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

TOOLS

Check with your vendor they miss you and always want to chat.

Copy of BACKDOORS...

USER AND ENTITY BEHAVIORAL ANALYTICS (UEBA)

It's like logging, but it actually works. UEBA looks for multiple concurrent logs, impossible logs based on geography, unusual file access, passwords sprays, and more!

TOOLS

Logenfraser

Copy of BACKDOORS...

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

Copy of BACKDOORS...

ISOLATION

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

TOOLS

Switch and Router Commands

Copy of BACKDOORS...

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.

Copy of BACKDOORS...



© Black Hills Information Security | @BHInfoSecurity

Questions?



© Black Hills Information Security | @BHInfoSecurity

