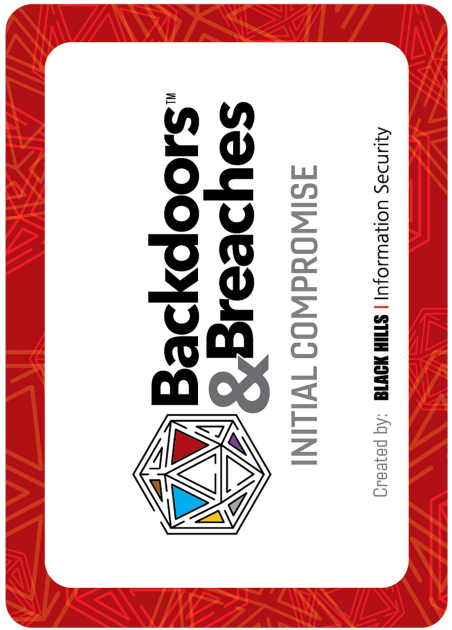
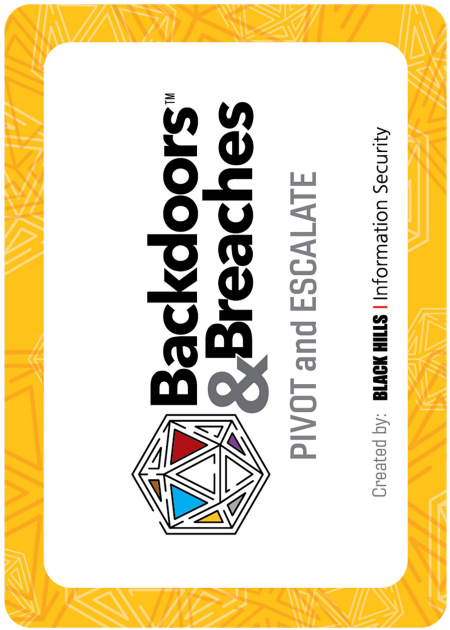
Backdoors & Breaches

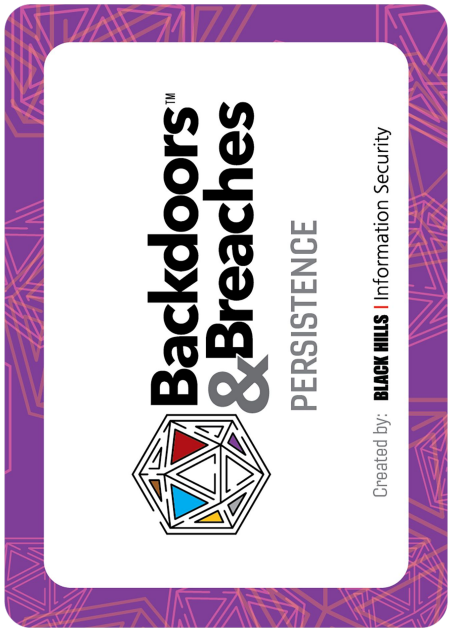
Attack Cards

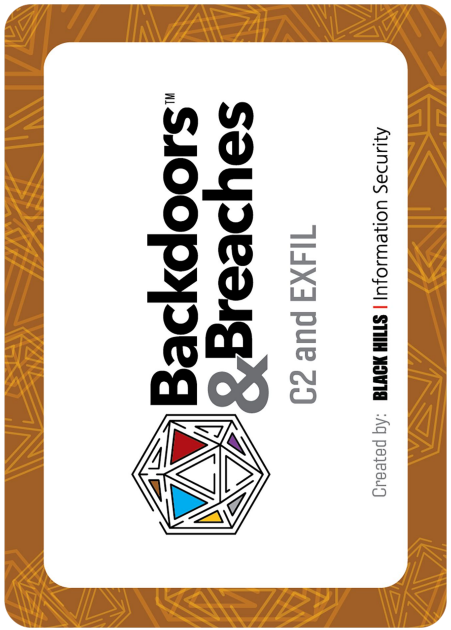
BLACK HILLS
Information Security

Scenario 1









Backdoors & Breaches

BLACK HILLS
Information Security

Scenario 1

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

KERBEROASTING

The attackers use a "feature" of SPNs to extract and crack service passwords.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Honey Services
Internal Segmentation

TOOLS

GetUserSPNs.py from Impacket
Hashcat for Cracking

https://www.blackhillsinfosec.com/running-hashcat-on-ubuntu-18-04-server-with-1080ti

https://github.com/SecureAuthCorp/impacket/blob/master/examples/GetUserSPNs.py

DLL ATTACKS

The attackers hijack the order in which DLLs are loaded. This is usually done through insecure directory/file permissions.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

PowerSploit
InvisiMole

https://www.blackhillsinfosec.com/digging-deeper-vulnerable-windows-services

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

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Gcat
Sneaky Creeper

https://github.com/byt3bl33d3r/gcat

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

Backdoors & Breaches

BLACK HILLS Information Security

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

Backdoors & Breaches

BLACK HILLS
Information Security

KERBEROASTING

The attackers use a "feature" of SPNs to extract and crack service passwords.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Honey Services
Internal Segmentation

TOOLS

GetUserSPNs.py from Impacket
Hashcat for Cracking

https://www.blackhillsinfosec.com/running-hashcat-on-ubuntu-18-04-server-with-1080ti

https://github.com/SecureAuthCorp/impacket/blob/master/examples/GetUserSPNs.py

Backdoors & Breaches

BLACK HILLS Information Security

DLL Attacks

The attackers hijack the order in which DLLs are loaded. This is usually done through insecure directory/file permissions.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

PowerSploit
InvisiMole

https://www.blackhillsinfosec.com/digging-deeper-vulnerable-windows-services

Backdoors & Breaches

BLACK HILLS
Information Security

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

NetFlow, Zeek/Bro, RITA Analysis

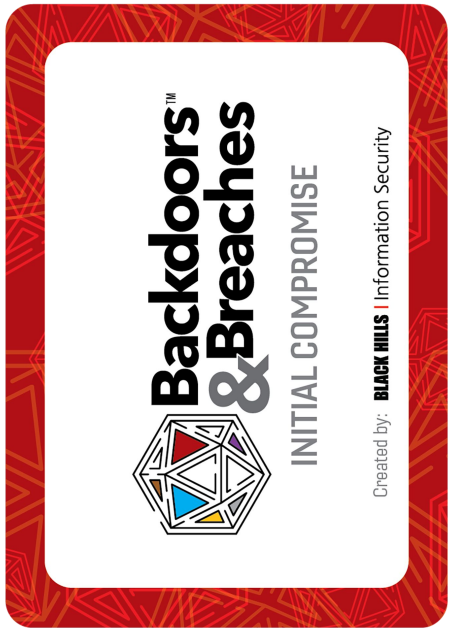
TOOLS

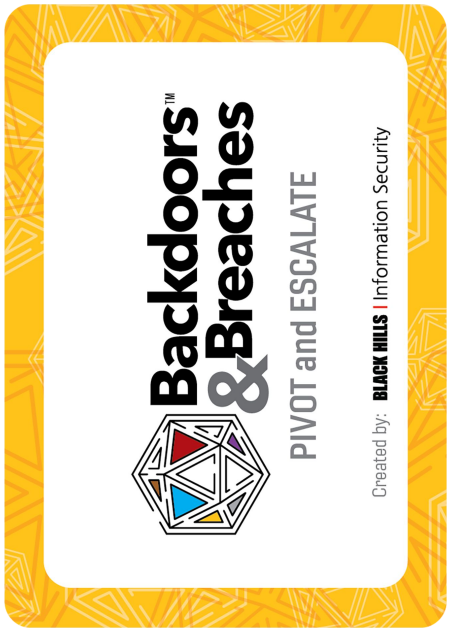
Gcat
Sneaky Creeper

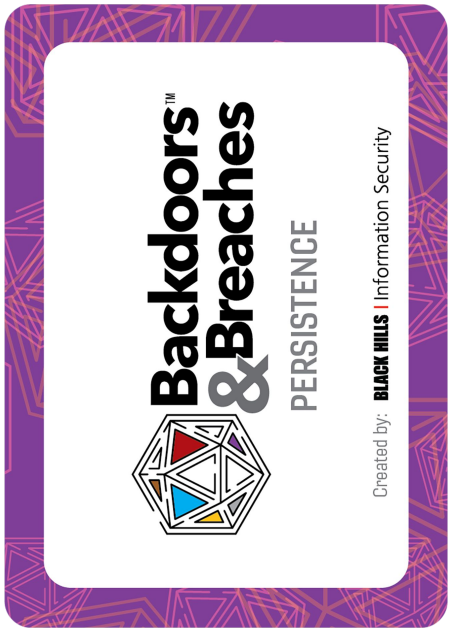
https://github.com/byt3bl33d3r/gcat

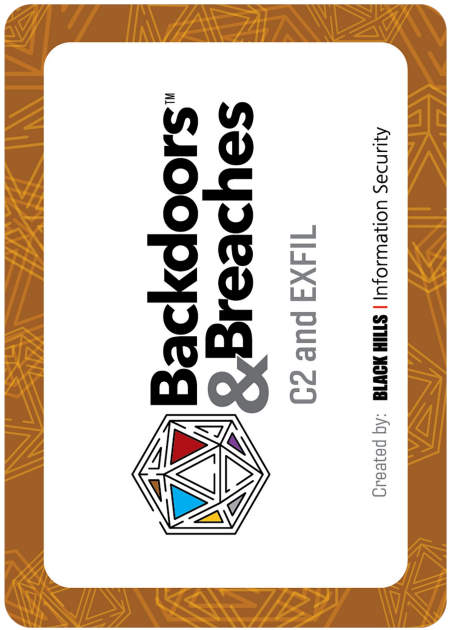
https://github.com/DakotaNelson/sneaky-creeper

Scenario 2









Backdoors & Breaches

BLACK HILLS
Information Security

Scenario 2

Trusted Relationship

A trusted third party who has access to your network is compromised. The attackers use this to pivot to your internal resources.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics

TOOLS

An unfortunate and unfounded trust in humanity and business partners who are complete strangers.

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

Logon Scripts

The attackers install a script that triggers when a user logs on.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Meterpreter Persistence

https://www.metasploit.com

DNS as C2

The attackers use DNS as a C2 channel.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

dnscat2

https://www.blackhillsinfosec.com/bypassing-cylance-part-2-using-dnscat2

Backdoors & Breaches

BLACK HILLS Information Security

Trusted Relationship

A trusted third party who has access to your network is compromised. The attackers use this to pivot to your internal resources.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics

TOOLS

An unfortunate and unfounded trust in humanity and business partners who are complete strangers.

Backdoors & Breaches

BLACK HILLS Information Security

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

Backdoors & Breaches

BLACK HILLS Information Security

Logon Scripts

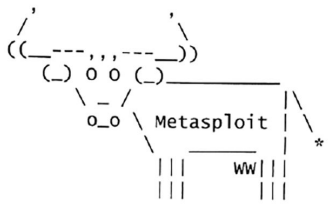
The attackers install a script that triggers when a user logs on.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Meterpreter Persistence



https://www.metasploit.com

Backdoors & Breaches

BLACK HILLS Information Security

DNS AS C2

The attackers use DNS as a C2 channel.

DETECTION

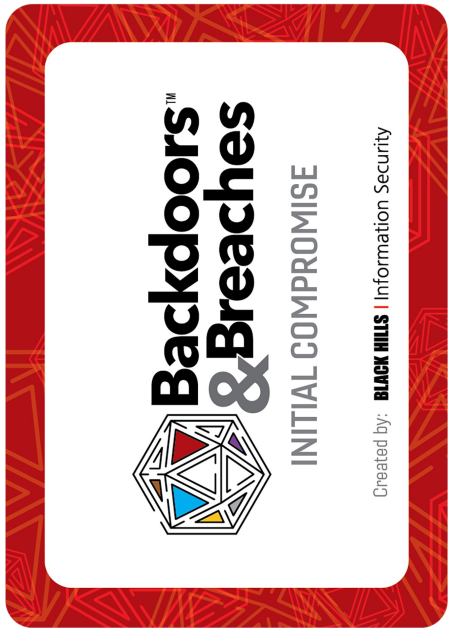
NetFlow, Zeek/Bro, RITA Analysis

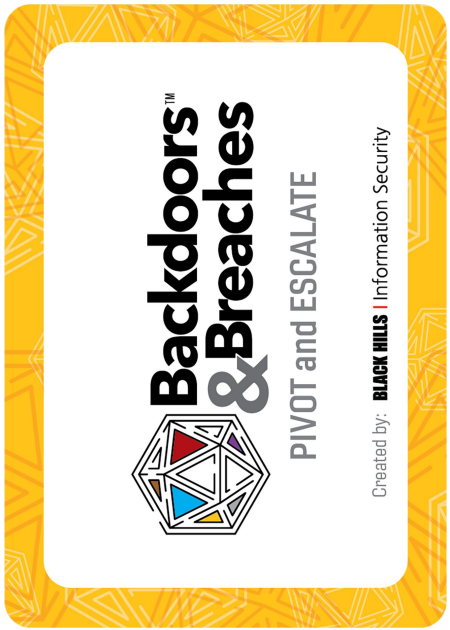
TOOLS

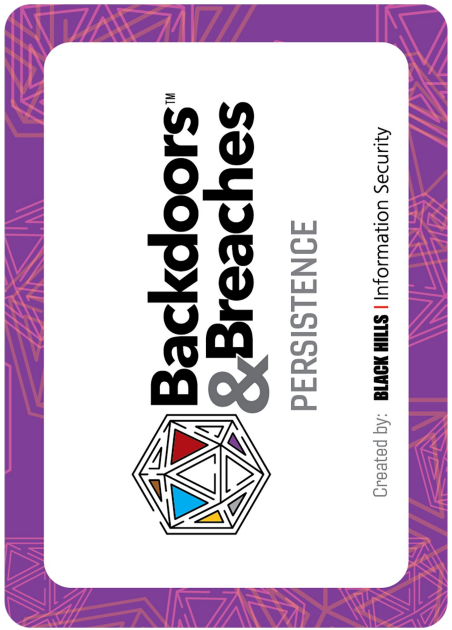
dnscat2

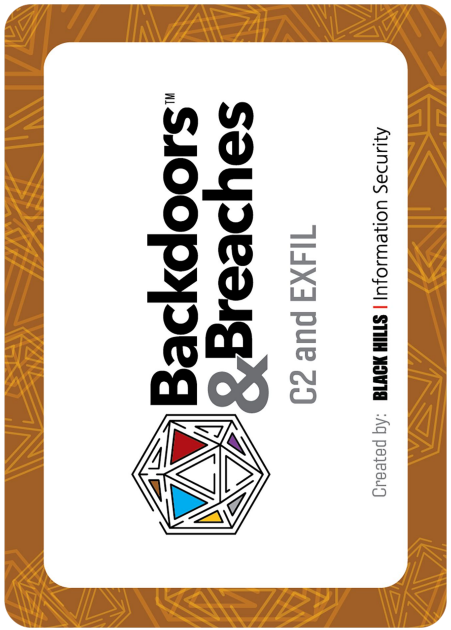
https://www.blackhillsinfosec.com/bypassing-cylance-part-2-using-dnscat2

Scenario 3









Backdoors & Breaches

BLACK HILLS
Information Security

Scenario 3

Insider Threat

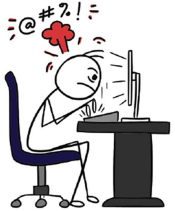
An internal disgruntled user exfiltrates information from your network.

DETECTION

User and Entity Behavior Analytics
DLP (Ha! Ha! Kidding. DLP never works.)
Working with HR

TOOLS

Being considered a Full Time Expenditure (FTE)
Long Hours
Addiction



https://americanaddictioncenters.org

Weaponizing Active Directory

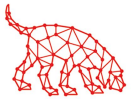
The attackers map trust relationships and user/group privileges in your Active Directory Network.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Internal Segmentation

TOOLS

BloodHound
DeathStar
CrackMapExec



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

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

Domain Fronting as C2

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

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Cobalt Strike

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

Backdoors & Breaches

BLACK HILLS
Information Security

Insider Threat

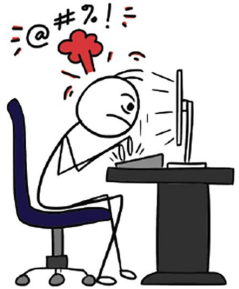
An internal disgruntled user exfiltrates information from your network.

DETECTION

User and Entity Behavior Analytics
DLP (Ha! Ha! Kidding. DLP never works.)
Working with HR

TOOLS

Being considered a Full Time Expenditure (FTE)
Long Hours
Addiction



https://americanaddictioncenters.org

Backdoors & Breaches

BLACK HILLS Information Security

Weaponizing Active Directory

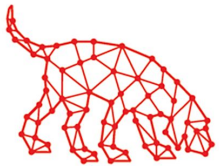
The attackers map trust relationships and user/group privileges in your Active Directory Network.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Internal Segmentation

TOOLS

BloodHound
DeathStar
CrackMapExec



https://github.com/BloodHoundAD/BloodHound

https://github.com/byt3bl33d3r/DeathStar

https://github.com/byt3bl33d3r/CrackMapExec

https://www.blackhillsinfosec.com/webcast-weaponizing-active-directory

Backdoors & Breaches

BLACK HILLS Information Security

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

Domain Fronting as C2

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

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Cobalt Strike

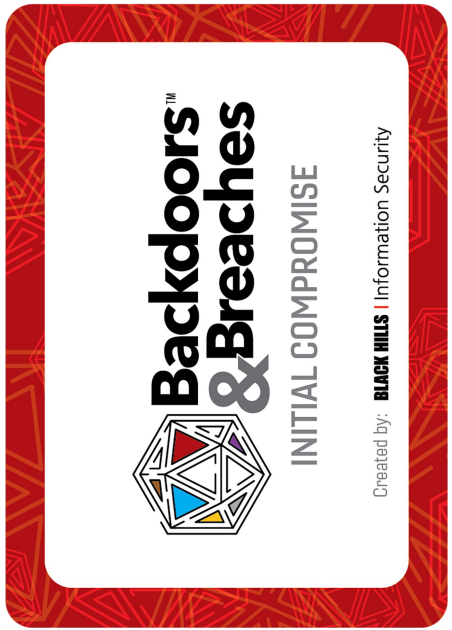
https://www.cobaltstrike.com

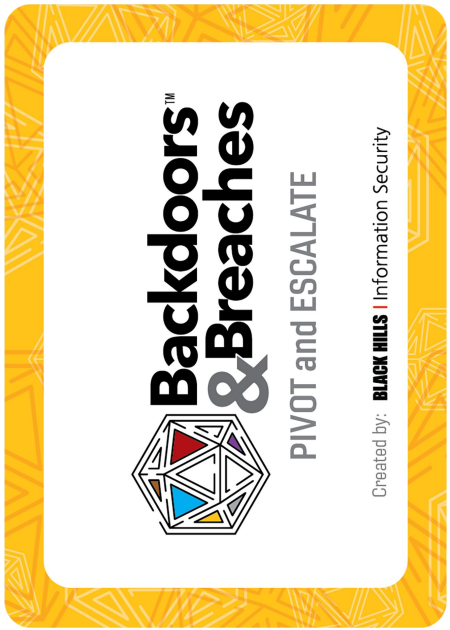
https://www.blackhillsinfosec.com/bypass-web-proxy-filtering

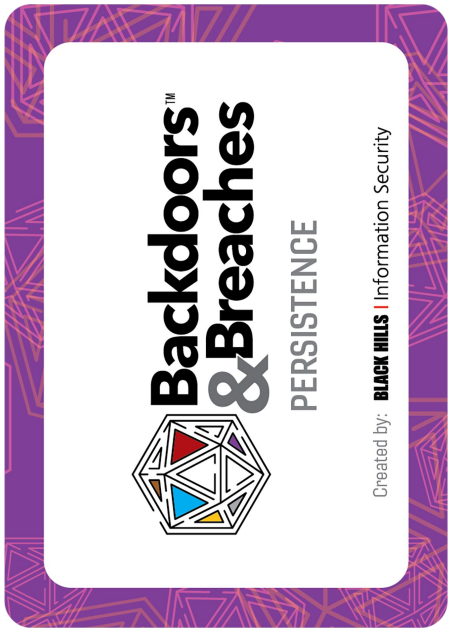
Backdoors & Breaches

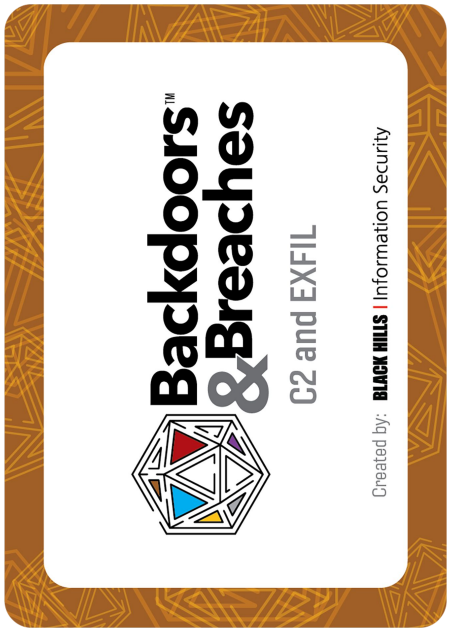
BLACK HILLS Information Security

Scenario 4


Backdoors & Breaches
INITIAL COMPROMISE
Created by: BLACK HILLS | Information Security


Backdoors & Breaches
PIVOT and ESCALATE
Created by: BLACK HILLS | Information Security


Backdoors & Breaches
PERSISTENCE
Created by: BLACK HILLS | Information Security


Backdoors & Breaches
C2 and EXFIL
Created by: BLACK HILLS | Information Security

Scenario 4

External Cloud Access

The attackers gain access to your cloud resources. They use this access to pivot.

DETECTION

SIEM Log Analysis

TOOLS

SprayingToolkit
CredKing
FireProx

https://github.com/byt3bl33d3r/SprayingToolkit
https://github.com/ustayready/CredKing
https://github.com/ustayready/fireprox

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
Internal Segmentation

TOOLS

ADExplorer.exe
Invoke-ShareFinder
Invoke-FileFinder
Find-InterestingFile
MailSniper

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

Accessibility Features

The attackers hijack Accessibility Features like Sticky Keys and Onscreen Keyboard.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

Bash Bunny
USB Rubber Ducky

https://shop.hak5.org

Windows Background Intelligent Transfer Service (BITS)

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

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

CE-

M$

https://github.com/deruke/tools

Backdoors & Breaches

BLACK HILLS Information Security

External Cloud Access

The attackers gain access to your cloud resources. They use this access to pivot.

DETECTION

SIEM Log Analysis

TOOLS

SprayingToolkit
CredKing
FireProx

https://github.com/byt3bl33d3r/SprayingToolkit

https://github.com/ustayready/CredKing

https://github.com/ustayready/fireprox

Backdoors & Breaches

BLACK HILLS Information Security

Credential Stuffing

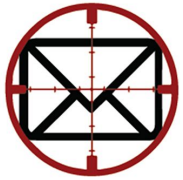
Valid Active Directory credentials have been discovered on open shares and files within your environment. These are used by the attackers.

DETECTION

SIEM Log Analysis
User and Entity Behavior Analytics
Internal Segmentation

TOOLS

ADExplorer.exe
Invoke-ShareFinder
Invoke-FileFinder
Find-InterestingFile
MailSniper



https://www.blackhillsinfosec.com/domain-goodness-learned-love-ad-explorer

https://www.blackhillsinfosec.com/abusing-exchange-mailbox-permissions-mailsniper

Backdoors & Breaches

BLACK HILLS Information Security

Accessibility Features

The attackers hijack Accessibility Features like Sticky Keys and Onscreen Keyboard.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

Bash Bunny
USB Rubber Ducky

https://shop.hak5.org

Windows Background Intelligent Transfer Service (BITS)

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

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

CE-

https://github.com/deruke/tools