AppLocker and Sysmon

Backdoors & Breaches

Malicious Service/Just Malware
Attacker adds a service that starts every time
Detection
Security Protection Analysis
Tools
Persistence
HTTPS as an Exfil
This is pretty basic: just 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/RITA
Tools
Metasploit reverse HTTPS payloads
Credential Stuffing
Attackers take advantage of third-party breaches to identify and use IDs and passwords for your organization.
Detection
Server Analysis
UBEA
Tools
Burp
Hydra
Users registering for services with their work email address
Web Server Compromise
Attackers take over an external web server. They then use this to pivot to your internal network.
Detection
Server Analysis
SIEM Log Analysis
NetFlow
RITA
Bro/Zeek
Tools
Zed Attack Proxy
SQLMap
Burp Proxy
https://www.zaproxy.org
https://portswigger.net/burp
https://www.blackhillsinfosec.com/using-simple-burp-macros-to-automate-testing
Token Passing
weak relationships and auth accounts in Active Directory
Detection
Tools
Firewall Log Review
Can your organization analyze and understand firewall logs? Do you regularly run attack scenarios and verify that your procedures work?
Tools
SOF-ELK
https://github.com/philhagen/sof-elk
Lead Handler Takes Maternity or Paternity Leave
Yea, there is always one person who pretty much runs the whole IR process. That one essential person. Well, now it is time for the IM to silence that person.
Notes
have to be able to work effectively without one or two most advanced people on the team. All of the quite people who are just listening and hoping to not get called need to step up. Now is your time. Shine.
PROTOTYPE

Incident Response Card Game

Launching in
September 2019

Request a Deck!

Type "Backdoors & Breaches" into the Questions Window

We'll randomly select a few requests to get a deck before the official launch.

BLACK HILLS
Information Security
• 2008 •

PENETRATION TESTING

RED TEAMING

THREAT HUNTING

WEBCASTS

OPEN-SOURCE TOOLS

BLOGS

bhis.co

Brought To You By!

AI HUNTER™

Network Threat Hunting Solution

ANALYZE
Network Traffic

IDENTIFY
Compromised Systems

HUNT
Menacing Threats

BEACONS MODULE

LONG CONNECTIONS MODULE

DEEP DIVE MODULE

ALERTING

REQUEST A PERSONAL DEMO

Type “Demo” in Questions Window

Hands On

Chuck Wagon Feast

Adventure

Wild West

Hackin' Fest

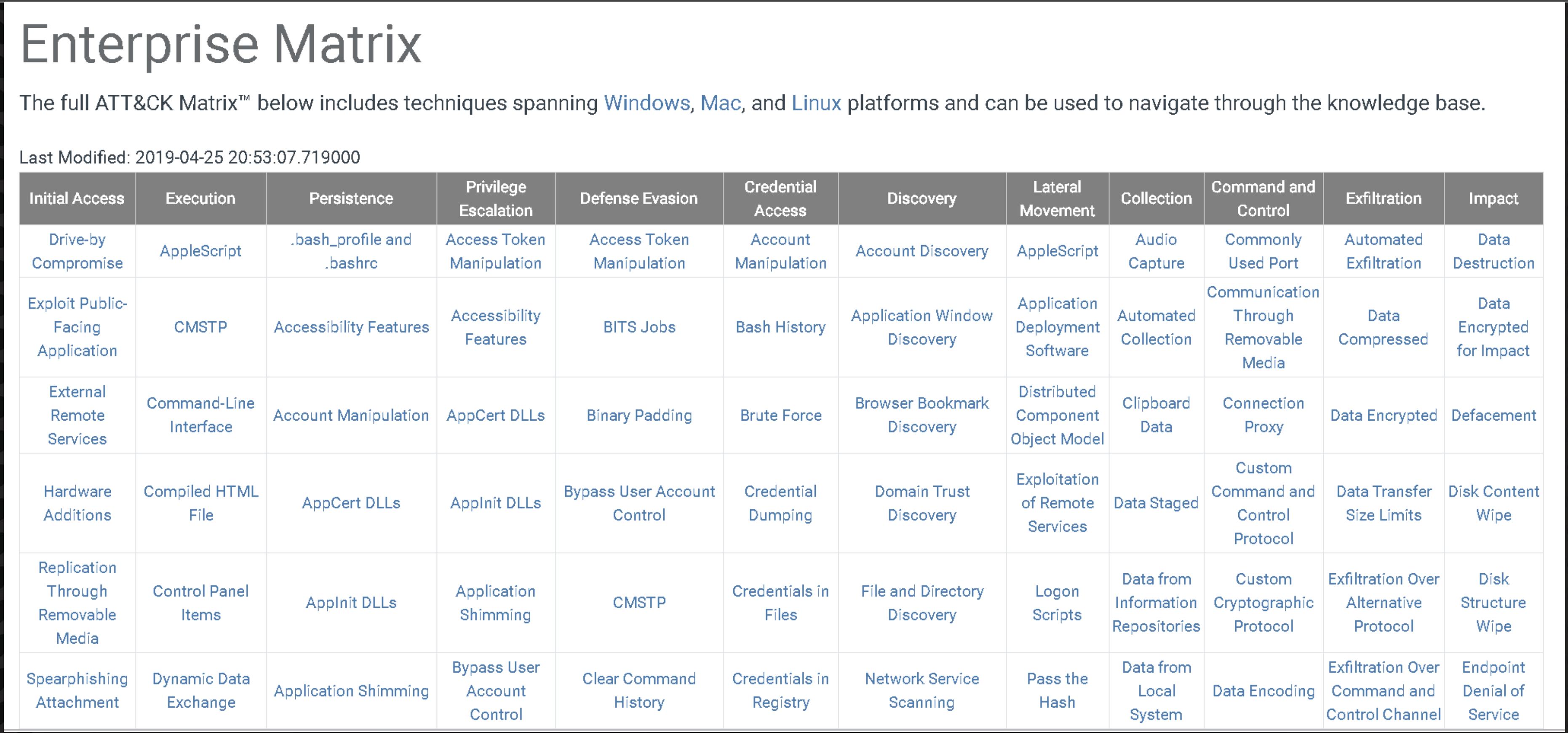
2019

Training 10/22 - 23
Conference 10/23 - 25

Deadwood, SD

wildwesthackinfest.com

Problem Statement



Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2019-04-25 20:53:07.719000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service

Executive Problem Statement

Basic Questions:

- Are our tools working?
- What can we detect?
- What are our gaps?
- Why does M$ logging suck so bad?
- What existing tools can fill them?
- What do we have to buy?
- Do we need to buy something expensive?

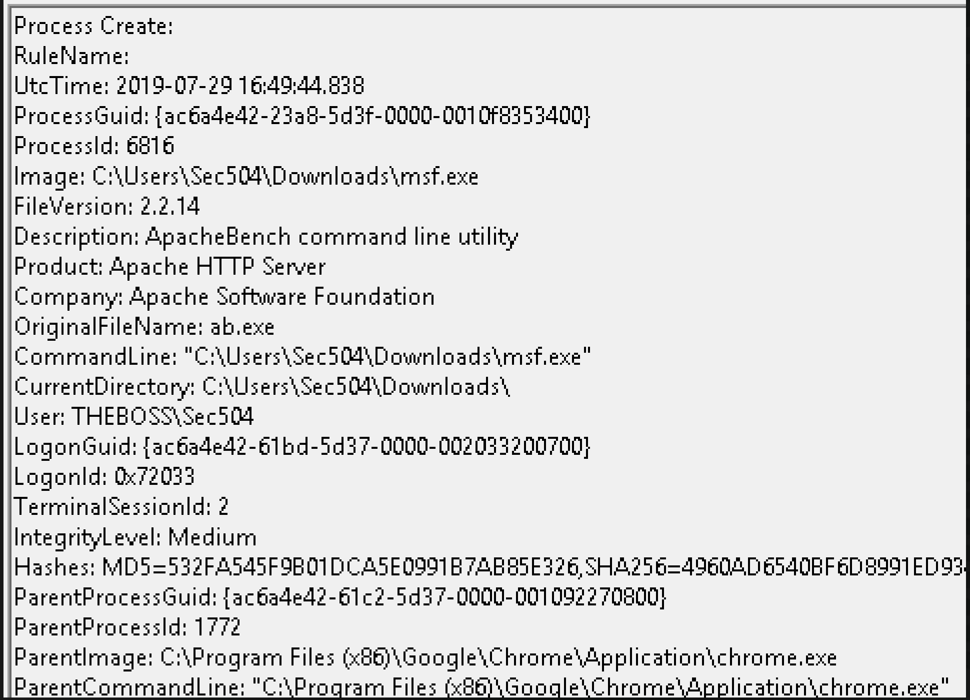
“Maybe, I can take the Sequel Police’s ship to Command headquarters to get a TimePod…”

Sysmon

- Basically…
  - Windows logging is just bad.
  - Finding anything is tough
- Sysmon makes it better
  - In like.. Five minutes
  - Like Heroin!
- Demo!

Sysmon… Is a great drug..

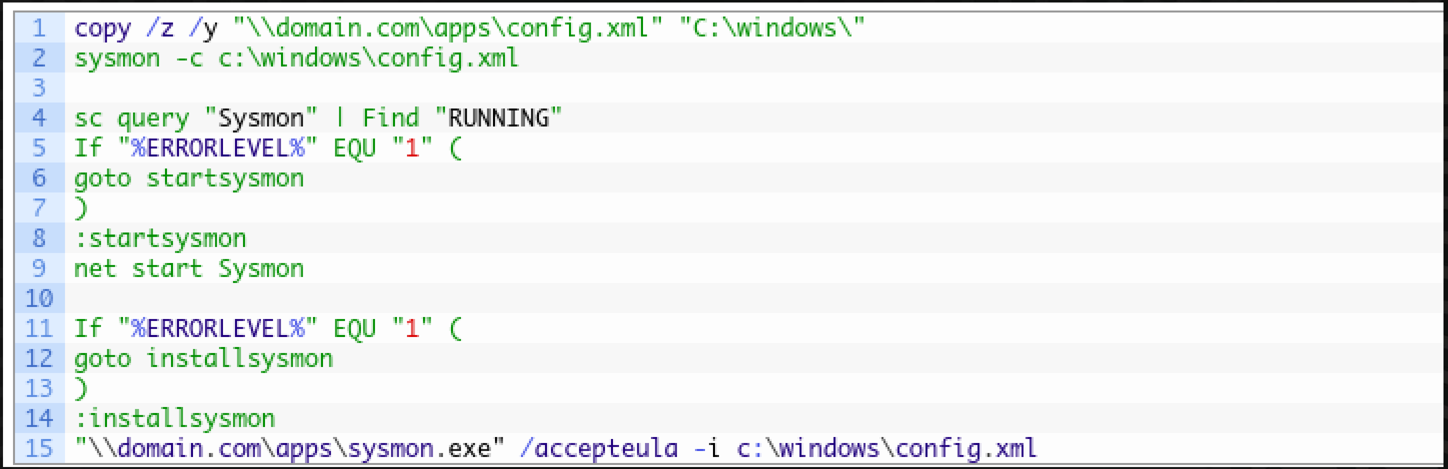
These were the logs you were looking for!



```
Process Create:
RuleName:
UtcTime: 2019-07-29 16:49:44.838
ProcessGuid: {ac6a4e42-23a8-5d3f-0000-0010f8353400}
ProcessId: 6816
Image: C:\Users\Sec504\Downloads\msf.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\Sec504\Downloads\msf.exe"
CurrentDirectory: C:\Users\Sec504\Downloads\
User: THEBOSS\Sec504
LogonGuid: {ac6a4e42-61bd-5d37-0000-002033200700}
LogonId: 0x72033
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=532FA545F9B01DCA5E0991B7AB85E326,SHA256=4960AD6540BF6D8991ED93
ParentProcessGuid: {ac6a4e42-61c2-5d37-0000-001092270800}
ParentProcessId: 1772
ParentImage: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
ParentCommandLine: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
```

Implementing Sysmon Via GPO

- Great Article via Syspanda
  - https://www.syspanda.com/index.php/2017/02/28/deploying-sysmon-through-gpo/



```
copy /z /y "\\domain.com\apps\config.xml" "C:\windows\"
sysmon -c c:\windows\config.xml

sc query "Sysmon" | Find "RUNNING"
If "%ERRORLEVEL%" EQU "1" (
goto startsysmon
)
:startsysmon
net start Sysmon

If "%ERRORLEVEL%" EQU "1" (
goto installsysmon
)
:installsysmon
"\\domain.com\apps\sysmon.exe" /accepteula -i c:\windows\config.xml
```

AppLocker

- Let’s create a very basic AppLocker profile
  - Just the Defaults
- And let’s push it out via GPO
- Need the OU, the Policy and the Service configured
- Demo

AppLocker Bypass

- Pretty much any bypass technique will work
  - Rundll32, EvilGrade-ISR, Service exploits, .sct files, etc.
- But 95%+ of the drive-by download attacks will fail
  - (That’s most attacks BTW)

Bypasses never seem to end.
They just go on and on my friends!
SubTee, started hacking and not knowing what it was..
Now we will just keep on hacking it forever
Just because..

Implementation Principles

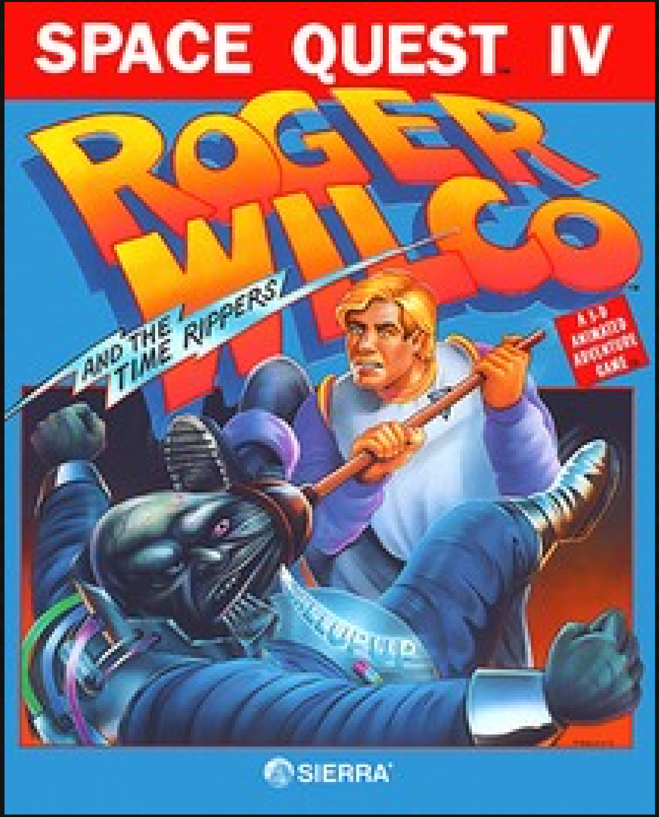
- Start small. With your own team
- Start in Audit mode!
- Roll out in stages to other “techy” teams
- No need to go super detailed to start

Roll it out to these people first.
They know things..

BLACK HILLS
Information Security
• 2008 •

Questions?

Answer!!



@BHInfoSecurity