Destroying the Fog of War

Defenders' Three Tasks and How To Start Improving

Jeff McJunkin

About Me

Hi, I’m Jeff. Check the last slide if I’ve earned your attention by then.

Definitions

Attacker: The person attempting to gain unauthorized access to data (could also be worm, etc). A specific example of a threat.

Penetration tester: Someone who demonstrates the business risk stemming from technical flaws in systems. The in-scope systems could be applications, web servers, entire networks, or even entire companies.

Red teamer: …let's not get into this today, okay?

Breach: More on this momentarily.

Attackers want your data (or money)

Progress | ipswitch

MOVEit®

Therefore, you shouldn't have data be directly accessible online:

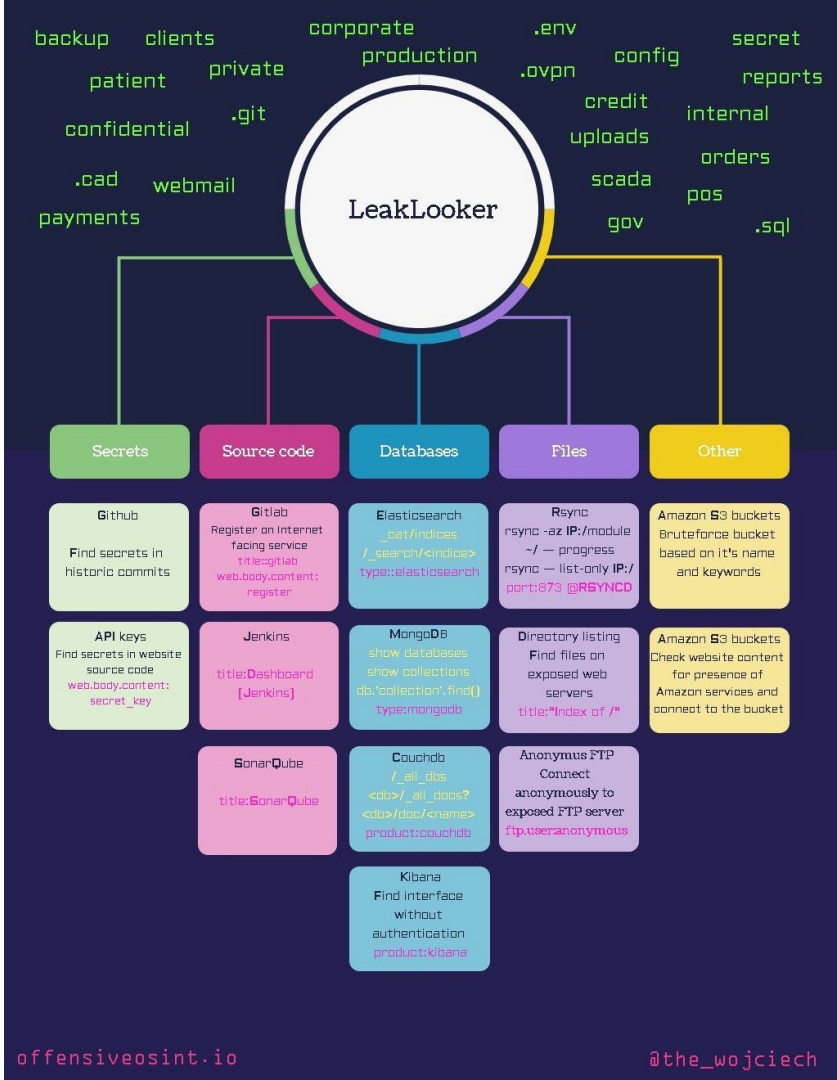
- Public S3 buckets
- MongoDB
- Elasticsearch
- Anonymous FTP servers
- Web servers with directory indexing
- MOVEit Managed File Transfer

Lesson learned: **Know where your data is**

It's probably not *only* inside your network (you share with vendors)

See also: The majority of Amazon S3 breaches

Image credit: https://github.com/woj-ciech/LeakLooker-X



Let's Keep Things Simple

Three things that nearly all attackers want:

1

Internal Access

2

Privileges

3

Goal Data

If the goal data is directly accessible, attackers will access it. Directly.

Only Five Ways In

There's only five ways for an outside attacker to get internal access:

1. Phishing
2. Exploitable Public-Facing Services
3. Authenticating via Public-Facing Services (i.e., VPN/RDP/VDI)
4. Inserting Rogue Devices / "drop boxes" (onto LAN or WiFi)
5. Supply Chain Attacks

This step is usually necessary, because the important data is usually on an internal network. Plus, there's a lot more attack surface internally!

(Hat tip to Tim MalcolmVetter)

Only Five Ways In

This one scales (Initial Access Brokers)

There's only five ways for an outside attacker to get internal access:

1. Phishing
2. **Exploitable Public-Facing Services**
3. Authenticating via Public-Facing Services (i.e., VPN/RDP/VDI)
4. Inserting Rogue Devices / "drop boxes" (onto LAN or WiFi)
5. Supply Chain Attacks

This step is usually necessary, because the important data is usually on an internal network. Plus, there's a lot more attack surface internally!

(Hat tip to Tim MalcolmVetter)

Only Five Ways In

These two are common, but targeted

There's only five ways for an outside attacker to get internal access:

1. **Phishing**
2. Exploitable Public-Facing Services
3. **Authenticating via Public-Facing Services (i.e., VPN/RDP/VDI)**
4. Inserting Rogue Devices / "drop boxes" (onto LAN or WiFi)
5. Supply Chain Attacks

This step is usually necessary, because the important data is usually on an internal network. Plus, there's a lot more attack surface internally!

(Hat tip to Tim MalcolmVetter)

Only Five Ways In

Rare outside of hospitality, higher ed, and corporate espionage

There's only five ways for an outside attacker to get internal access:

1. Phishing
2. Exploitable Public-Facing Services
3. Authenticating via Public-Facing Services (i.e., VPN/RDP/VDI)
4. **Inserting Rogue Devices / "drop boxes" (onto LAN or WiFi)**
5. Supply Chain Attacks

This step is usually necessary, because the important data is usually on an internal network. Plus, there's a lot more attack surface internally!

(Hat tip to Tim MalcolmVetter)

Only Five Ways In

...mostly for nation states

There's only five ways for an outside attacker to get internal access:

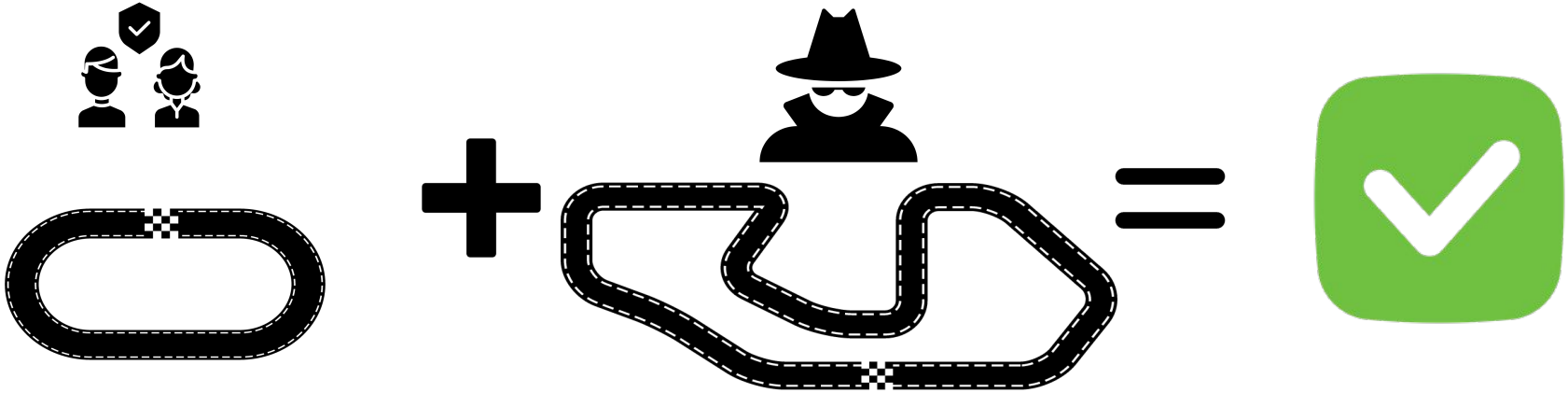
1. Phishing
2. Exploitable Public-Facing Services
3. Authenticating via Public-Facing Services (i.e., VPN/RDP/VDI)
4. Inserting Rogue Devices / "drop boxes" (onto LAN or WiFi)
5. **Supply Chain Attacks**

This step is usually necessary, because the important data is usually on an internal network. Plus, there's a lot more attack surface internally!

(Hat tip to Tim MalcolmVetter)

Defender's Objectives

To prevent successful breaches, defenders need to detect and respond to attackers who gain initial access before they accomplish their goal.



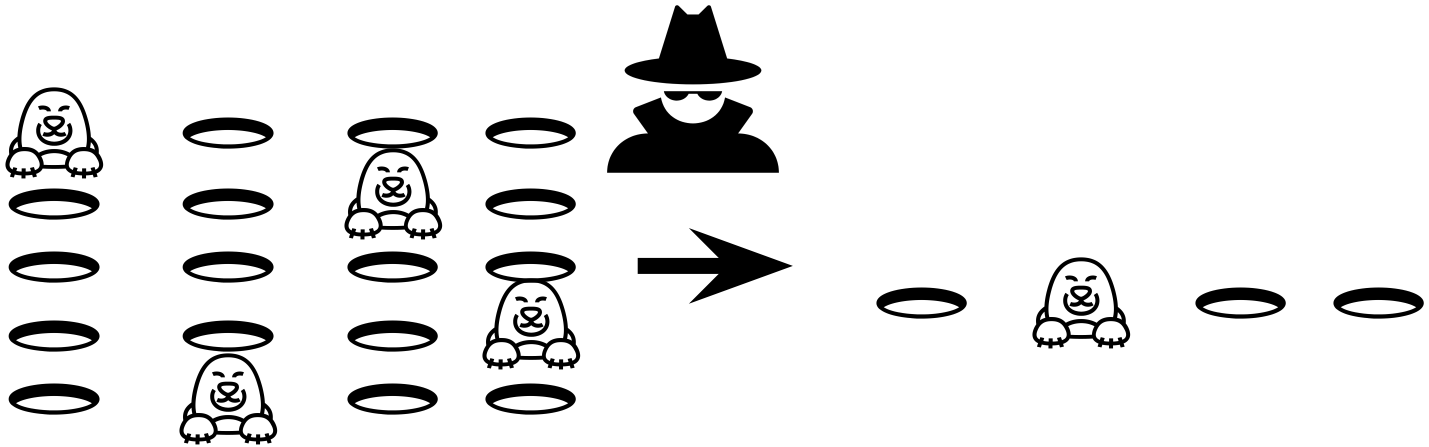
Defender's Objectives

To prevent successful breaches, defenders need to detect and respond to attackers who gain initial access before they accomplish their goal.

Defender's Objectives

Therefore, defenders have three objectives:

1. **Reduce the number of ways attacker gain initial access**
2. Lower the time to detect and respond to an attacker
3. Increase the time for an attacker to accomplish their goal



Defender's Objectives

Therefore, defenders have three objectives:

1. **Reduce the number of ways attacker gain initial access**
2. Lower the time to detect and respond to an attacker
3. Increase the time for an attacker to accomplish their goal

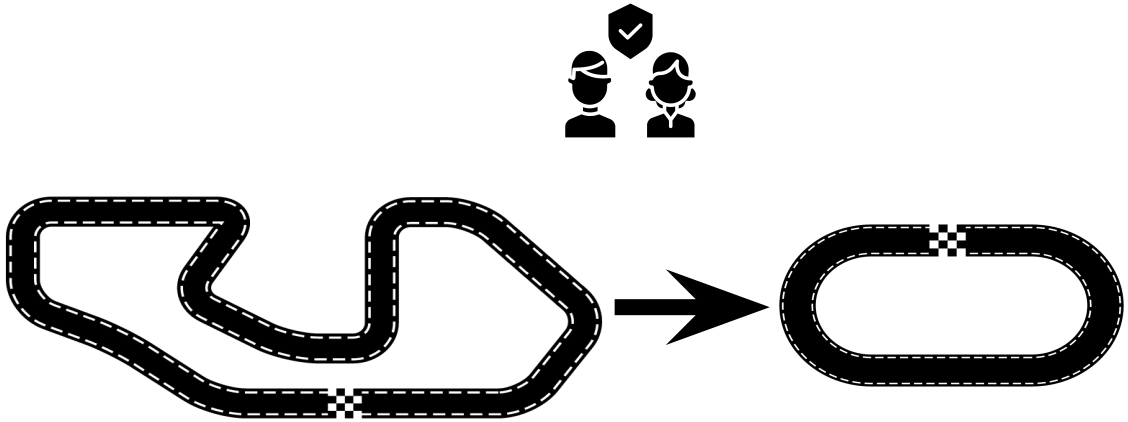
Examples:

1. Consolidate to one method of remote support. Remove and monitor all for all others.
2. Minimize external attack surface (i.e., kill Exchange)
3. Lock down as many methods of code execution as possible from user endpoints (Office macros, AutoDDE, Quick Assist)

Defender's Objectives

Therefore, defenders have three objectives:

1. Reduce the number of ways attacker gain initial access
2. **Lower the time to detect and respond to an attacker**
3. Increase the time for an attacker to accomplish their goal



Defender's Objectives

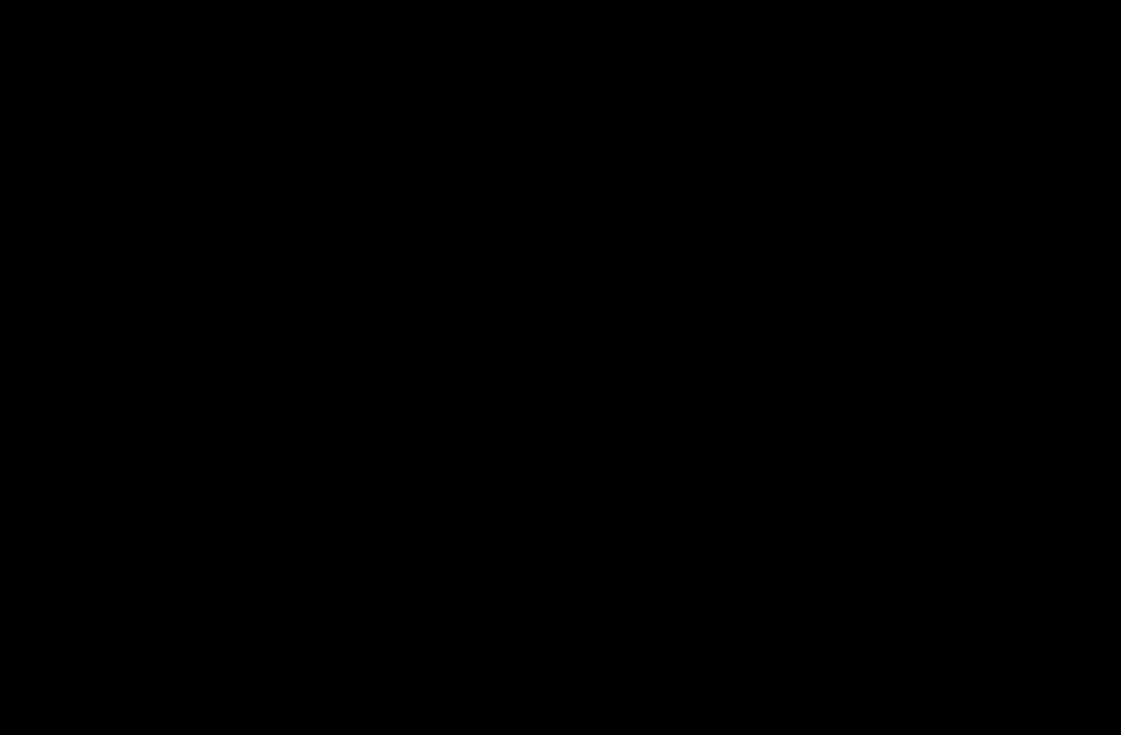
Therefore, defenders have three objectives:

1. Reduce the number of ways attacker gain initial access
2. **Lower the time to detect and respond to an attacker**
3. Increase the time for an attacker to accomplish their goal

Examples:

1. Alert on suspicious activity as soon as possible (more on this later)
2. Train and test your response capabilities – given an infected machine, can you find the compromised user(s) and computer(s) that the attacker <u>also</u> compromised?

MARIO KART™ Wii



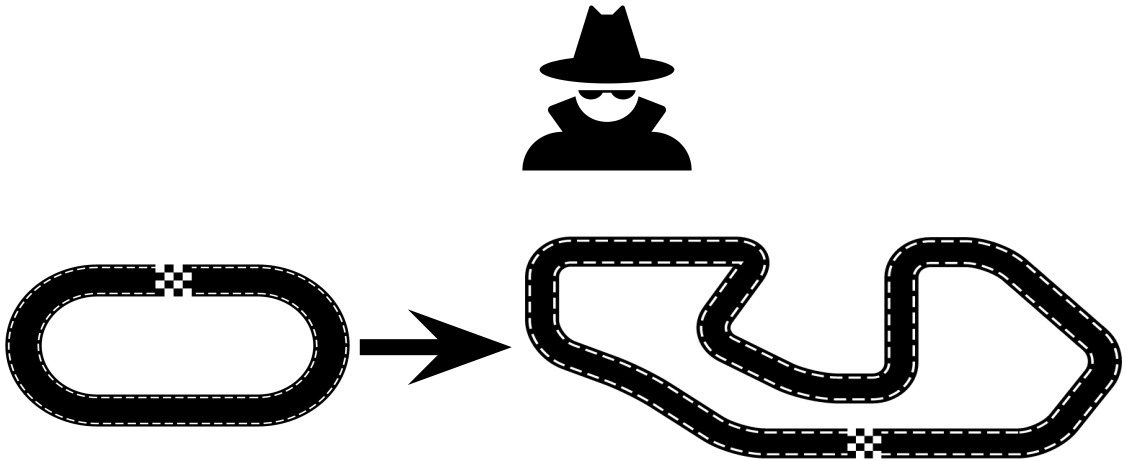
Here are your attackers, zooming ahead

This is your IR team, blissfully unaware

Defender's Objectives

Therefore, defenders have three objectives:

1. Reduce the number of ways attacker gain initial access
2. Lower the time to detect and respond to an attacker
3. **Increase the time for an attacker to accomplish their goal**



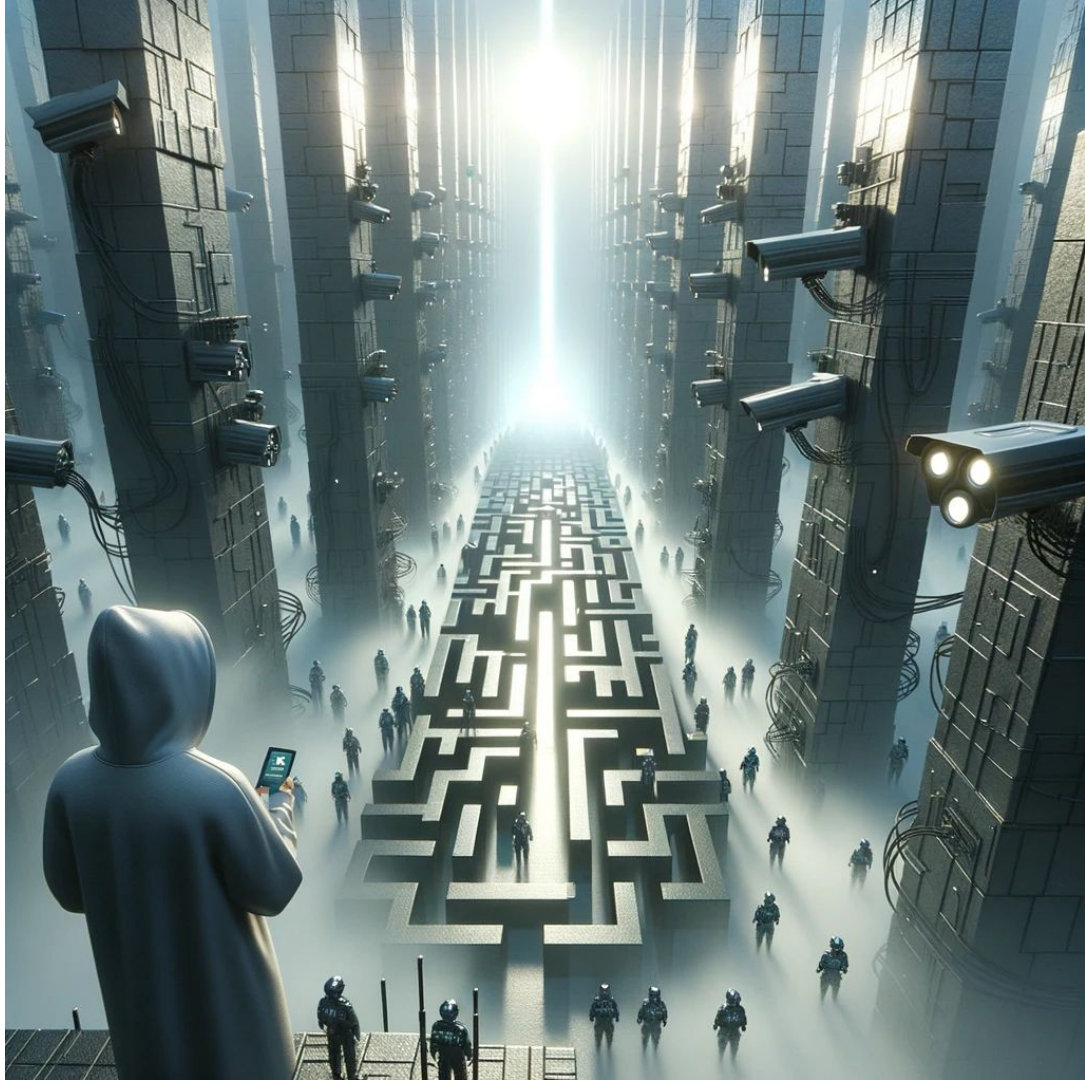
Defender's Objectives

Therefore, defenders have three objectives:

1. Reduce the number of ways attacker gain initial access
2. Lower the time to detect and respond to an attacker
3. **Increase the time for an attacker to accomplish their goal**

If an attacker can get in easily, and gain access to data quickly, no detection and/or response capabilities will stop breaches. Buy yourself some time.

A well-defended environment



Demo Time!


HERE
CONNTACTS
CONTACT
DEADWOOD
DIGITAL DYNAMICS
COUDD SOUTIONS
CIOUD SOOLUTIONS
NETWORK SECURITY
NETWORK SECURTY

A more common environment

Just to be clear…

I’m not crime-ing live

chat.openai.com/c/82701b65-8c8e-4b8e-b023-3d4f0d3c2905

JE

I like those! Let's do some variations for "Deadwood Digital Dynamics", please.

DALL·E 3
Created 4 images

Here are the variations for "Deadwood Digital Dynamics". I've incorporated elements of Deadwood's history with modern tech aesthetics. Please take a look and let me know if these align with your vision or if any further tweaks are required!

Password Guessing

Password guessing needs just three things:

1. Usernames
2. Passwords
3. Some authentication service (ideally 1FA, backed by AD, exposed to the Internet)

Where do you get usernames? Guessing, PowerMeta, enumeration via Teams, LinkedIn, or just https://github.com/insidetrust/statistically-likely-usernames

Crowbar, Legba, Hydra, Metasploit modules, etc can all do the actual guessing - there are plenty of tools

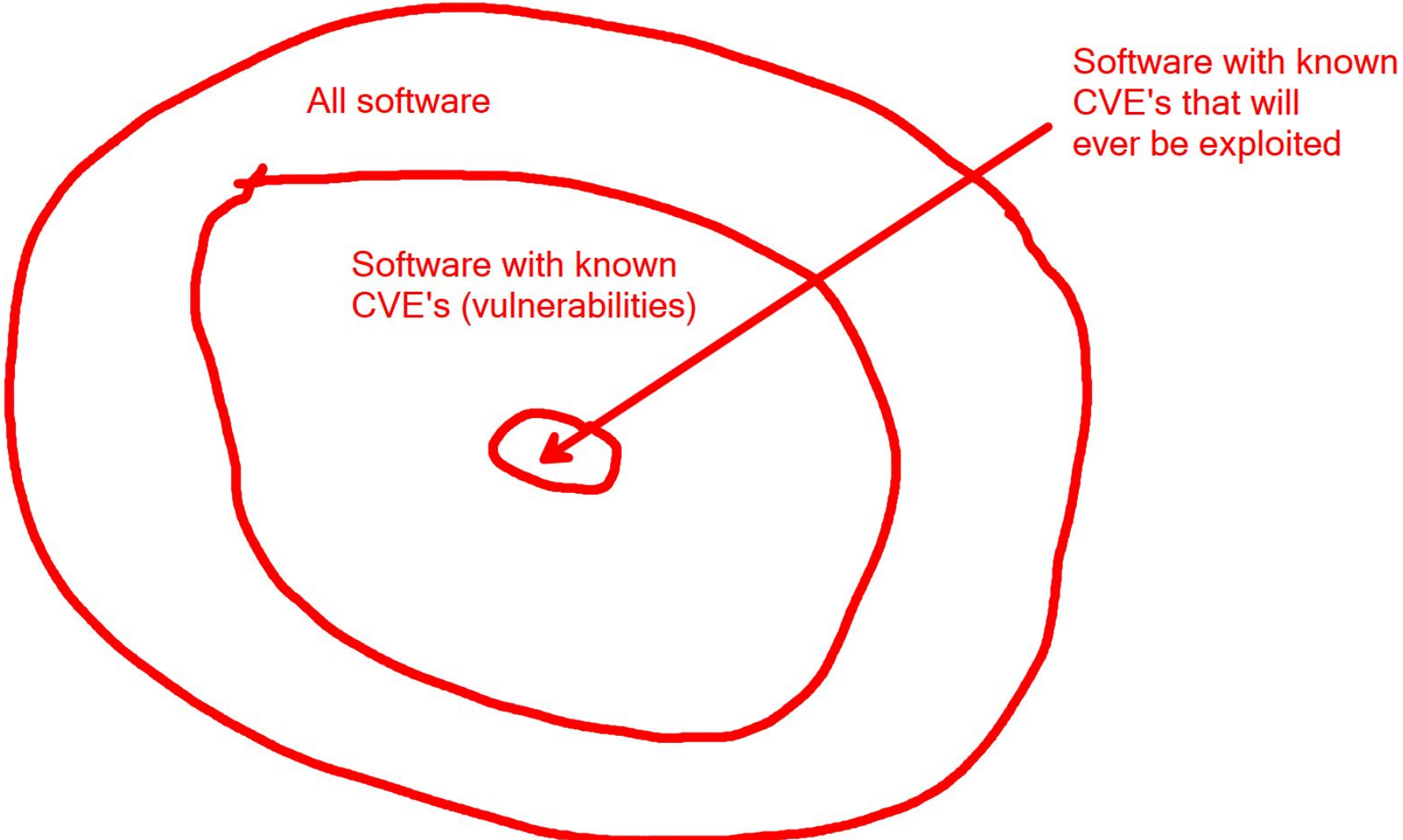
```
Invoke-PowerMeta -Download -Extract -TargetDomain txtsv.com
```

No Exploits Were Used In The Making of this Demo

The significant majority of real-world breaches take advantage of either zero or one patchable flaws

Why one? Initial Access Brokers doing **masscan | nmap | exploit.py**

“Out of our last 100 penetration tests, just two required exploitation to accomplish the goals.” - John Strand, Black Hills Information Security


All software
Software with known CVE's (vulnerabilities)
Software with known CVE's that will ever be exploited

0day "In the Wild"

File Edit View Insert Format Data Tools Extensions Help

100% View only

A1 CVE

	A	B	C	D	E	F	G	H	I
11	CVE-2023-28206	Apple	iOS/macOS	Memory Corruption	Out-of-bounds write in IOSurfac	???	2023-04-07	https://support.a	???
12	CVE-2023-28205	Apple	WebKit	Memory Corruption	Use-after-free in WebKit	???	2023-04-07	https://support.a	???
13	CVE-2023-28252	Microsoft	Windows	Memory Corruption	Common Log File System Drive	???	2023-04-11	https://msrc.micr	https://secur
14	CVE-2023-2033	Google	Chrome	Memory Corruption	Type confusion in V8	2023-04-11	2023-04-14	https://chromere	???
15	CVE-2023-2136	Google	Chrome	Memory Corruption	Integer overflow in Skia	2023-04-12	2023-04-18	https://chromere	???
16	CVE-2023-21492	Samsung	Android	Logic/Design Flaw	Kernel pointers exposure in log	2021-01-17	2023-05-01	https://security.s	???
17	CVE-2023-28204	Apple	WebKit	Memory Corruption	Out-of-bounds read	???	2023-05-01	https://support.a	???
18	CVE-2023-32373	Apple	WebKit	Memory Corruption	Use-after-free in WebKit	???	2023-05-01	https://support.a	???
19	CVE-2023-29336	Microsoft	Windows	Memory Corruption	Win32k Elevation of Privilege	???	2023-05-09	https://msrc.micr	???
20	CVE-2023-32409	Apple	WebKit	Memory Corruption	WebContext sandbox escape	???	2023-05-18	https://support.a	???
21	CVE-2023-2868	Barracuda	Email Security G	Logic/Design Flaw	Remote command injection due	2023-05-18	2023-05-30	https://www.barr	???
22	CVE-2023-3079	Google	Chrome	Memory Corruption	Type confusion in V8	2023-06-01	2023-06-05	https://chromere	???
23	CVE-2023-32434	Apple	iOS/macOS	Memory Corruption	Integer overflow in the XNU ker	???	2023-06-21	https://support.a	https://secur
24	CVE-2023-32435	Apple	WebKit	Memory Corruption	Unspecified memory corruption	???	2023-06-21	https://support.a	https://secur
25	CVE-2023-32439	Apple	WebKit	Memory Corruption	Type confusion	???	2023-06-21	https://support.a	???
26	CVE-2023-37450	Apple	WebKit	Memory Corruption	Unspecified memory corruption	???	2023-07-10	https://support.a	???
27	CVE-2023-32046	Microsoft	Windows	Memory Corruption	MSHTML Platform Elevation of	???	2023-07-11	https://msrc.micr	???
28	CVE-2023-36874	Microsoft	Windows	Logic/Design Flaw	Windows Error Reporting Servic	2023-06-30	2023-07-11	https://msrc.micr	???
29	CVE-2023-36884	Microsoft	Windows	Logic/Design Flaw	Office and Windows HTML Rem	2023-07-05	???	https://msrc.micr	???
30	???	Synacor	Zimbra	XSS	Reflected XSS in /m/moveto	2023-06-29	???	https://blog.zimb	???
31	CVE-2023-38606	Apple	iOS/macOS	Memory Corruption	Unspecified kernel vulnerability	???	2023-07-24	https://support.a	???
32	CVE-2023-32409	Apple	iOS/macOS	Memory Corruption	Unspecificed kernel vulnerability	???	2023-07-24	https://support.a	???
33									
34									

Introduction All 2023 2022 2021 2020 2019 2018 2017 2016 2015 2014

THE DFIR REPORT

cobaltstrike Hive ransomware wmiexec

From ScreenConnect to Hive Ransomware in 61 hours

September 25, 2023

The execution of the file resulted in the installation of ScreenConnect. During the investigation, we observed that this initial access method required the end user to be a local Administrator, as less privileged users would cause the installation to fail. Around an hour after execution, the threat actor initiated discovery commands via ScreenConnect using standard Windows utilities like *systeminfo*, *ipconfig*, and *net*. A few minutes later, the threat actor proceeded to run a BITS transfer job to deploy a Cobalt Strike beacon.

THE DFIR REPORT

adfind Attribution cobaltstrike Exfiltrate Data FIN11 FlawedGrace Lace Tempest truebot

A Truly Graceful Wipe Out

June 12, 2023

We also observed some other miscellaneous commands that we tend to see in every intrusion. These discovery commands collected information about the administrator groups and users. Although, there was one notable use of the tasklist command where threat actors used the /S parameter to retrieve the list of currently running processes from remote hosts.

```
quser
net  group "Domain Admins" /domain
net  group "Domain Controllers" /domain
net  group /domain
net  localgroup "Remote Desktop Users"
net  localgroup Administrators
net  user <user> /domain
nltest  /domain_trusts
tasklist /S <IP of remote host>
```

THE DFIR REPORT

adfind cobaltstrike icedid quantum ransomware rclone ShareFinder

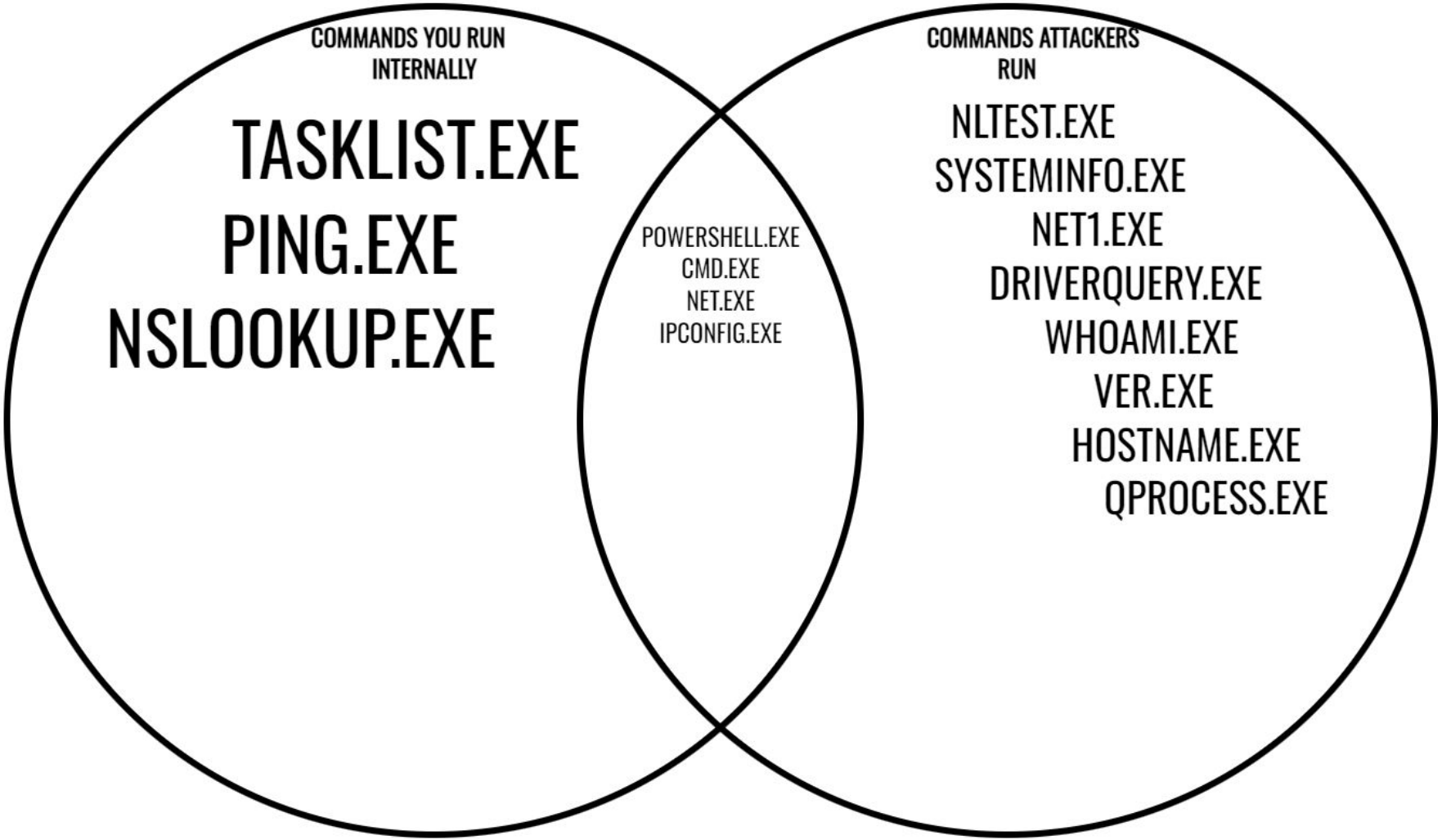
Malicious ISO File Leads to Domain Wide Ransomware

April 3, 2023

From the IcedID malware running via Rundll32, the following LOLBAS commands were observed:

```
rundll32 C:\Users\
[REDACTED]\AppData\Local\Temp\easygoing.
dat,#1
        → nltest /domain_trusts
/all_trusts
        → nltest /domain_trusts
        → net view /all /domain
        → net view /all
        → net group "Domain Admins"
/domain
        → cmd.exe /c chcp >&2
        → ipconfig /all
        → net config workstation
    → systeminfo
```


Why is it, when something happens, it is always you three?
NLTEST
SYSTEMINFO
NET.EXE
imgflip.com


COMMANDS YOU RUN INTERNALLY
TASKLIST.EXE
PING.EXE
NSLOOKUP.EXE
POWERSHELL.EXE
CMD.EXE
NET.EXE
IPCONFIG.EXE
COMMANDS ATTACKERS RUN
NLTEST.EXE
SYSTEMINFO.EXE
NET1.EXE
DRIVERQUERY.EXE
WHOAMI.EXE
VER.EXE
HOSTNAME.EXE
QPROCESS.EXE

CANARY TOKENS

Sensitive command token

alerts@roguevalleyinfosec.com

nltest.exe suspicious command line execution

nltest.exe

Create my Canarytoken

wazuh.roguevalleyinfosec.com/app/wazuh#/overview/?ta...

wazuh. Modules rdp01 Security events

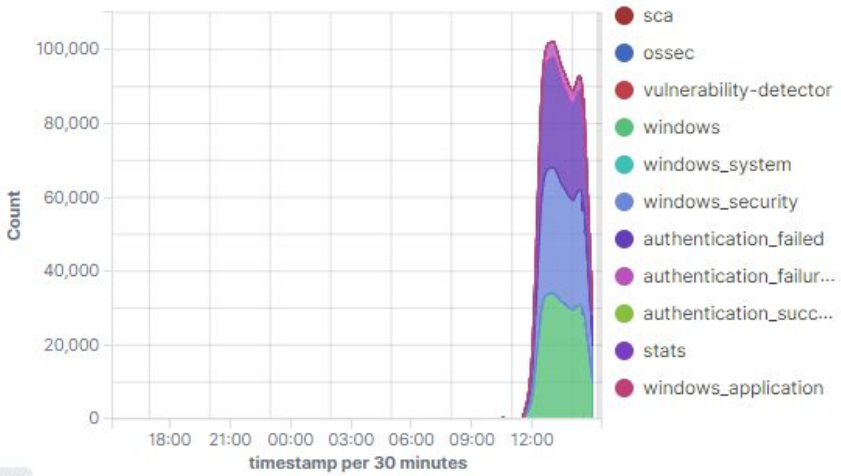
Dashboard Events

Search DQL Last 24 hours

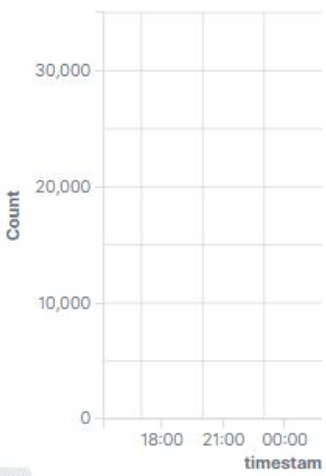
manager.name: ubuntu-16gb-hil-1 agent.id: 003 + Add filter

Total	Level 12 or above alerts	Authentication failure
171634	0	171234

Alert groups evolution



Alerts



If an attacker can get in easily, and gain access to data quickly, no amount of detection and response capabilities will stop breaches

~~If an attacker can get in easily, and gain access to data quickly, no amount of detection and response capabilities will stop breaches~~

If attackers can get in and win in an hour, you're boned.

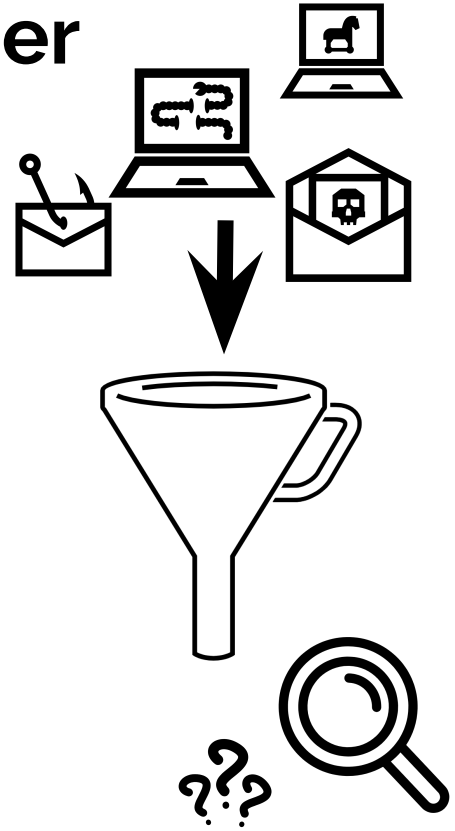
How To Slow Down Attackers?

Read more at https://bit.ly/topattacks

Two Races: Attacker and Defender

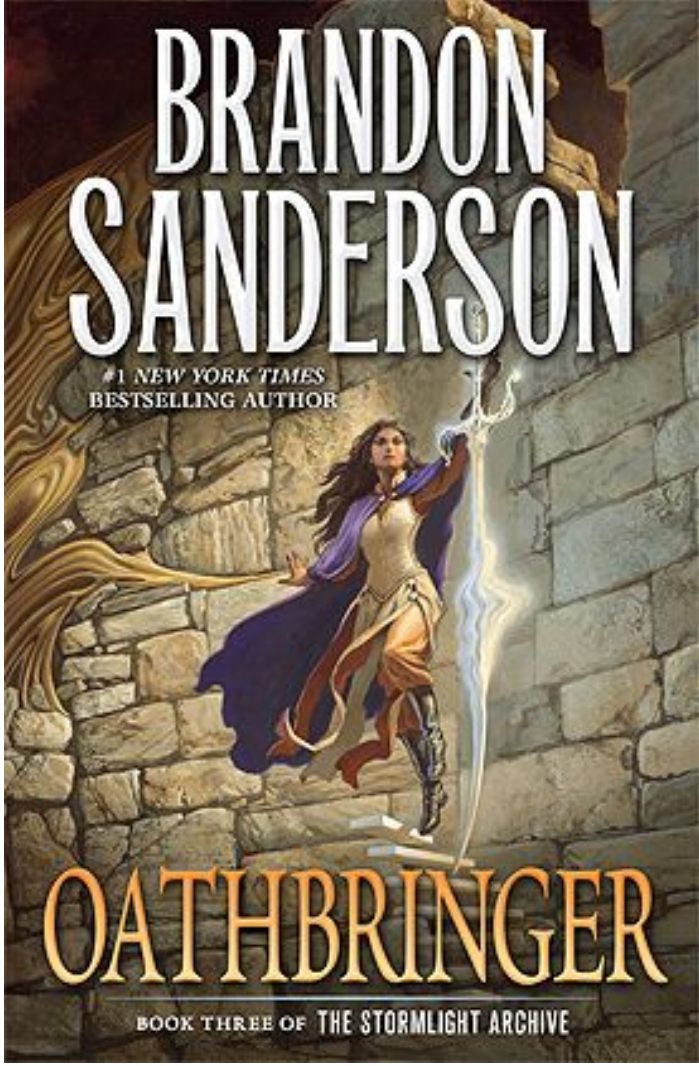
Prevention is ideal, but it's impossible to prevent 100% of incidents.

Therefore, focus on minimizing, detecting, and accelerating response to incidents.



“The most important step a person can take is always the <u>next</u> one.”

- Brandon Sanderson, *Oathbringer*



First Steps

Have something to detect attackers (orgs have one detection by default):

- Test a Canarytoken on a lab or your own machine - it's just a registry key!
- Deploy more of them via Group Policy (or Intune, ConfigMgr, etc)
  - If you get false positives (vendor software running whoami.exe, etc), remove those entries
- More? https://bit.ly/findingattackers

Make sure attackers can't win near-instantly:

- Look through your automatically-mapped file shares. What could hurt you if exfiltrated? (Uber)
- How much data do you have in SharePoint, Teams, Slack, etc? (LAPSUS$)
- More? https://bit.ly/topattacks

Questions?

Slides are online at https://bit.ly/killfog

Recording from WWHF 2023: https://youtu.be/JQ0fbm2XF7w

References:

- Credential stuffing: https://bit.ly/credstuffing
- Slowing down attackers: https://bit.ly/topattacks
- Finding attackers: https://bit.ly/detectingattackers
- AV evasion: https://bit.ly/bypassingav
- Learning from breaches: https://bit.ly/learningfrombreaches
- Home labs: https://bit.ly/kickasslab

Want resume/interview/mentoring help? https://calendly.com/rogueinfosec/mock-interview

My internet auntie (Lesley Carhart) is wonderful, but one person can only scale so far :)

Email: jeff@roguevalleyinfosec.com