Responding to Advanced Adversaries

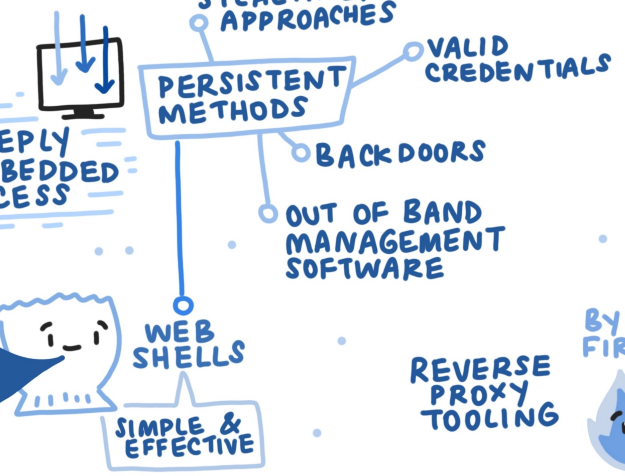
Anurag Khanna

RESPONDING TO ADVANCED ADVERSARIES

ANURAG KHANNA

1 GAIN ACCESS
2 MAINTAIN ACCESS
3 PERFORM ACTION-ON-OBJECTIVES

INITIAL VECTOR
- SUPPLY CHAIN ATTACKS
- SPEAR PHISHING
- VALID CRED.
- PASSWORD SPRAYING
- COMPROMISE VULNERABLE INTERNET FACING SYSTEMS



@SANSINSTITUTE #BLUETEAMSUMMIT

SANS BLUE TEAM SUMMIT & TRAINING

What will we talk about today?

- Advanced Adversaries/APTs/Nation State/State-nexus Targeted Attacks
- Phases of a state-nexus targeted attack
- Tactics, Techniques, and Procedures (TTPs) of Advanced Adversaries
- Responding to such intrusions

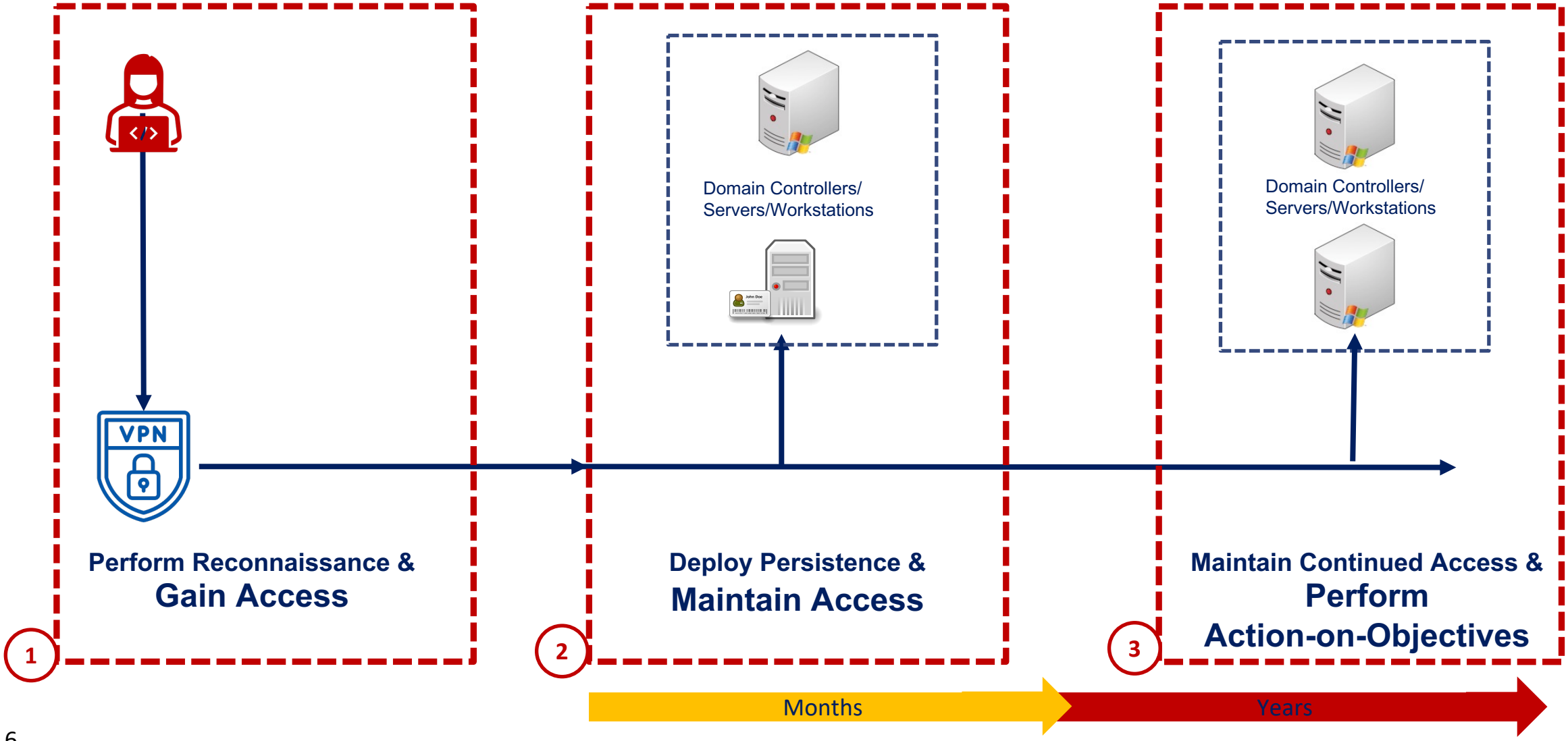
Takeaway: Understand a targeted attack and response to such attacks.

Who are these adversaries?

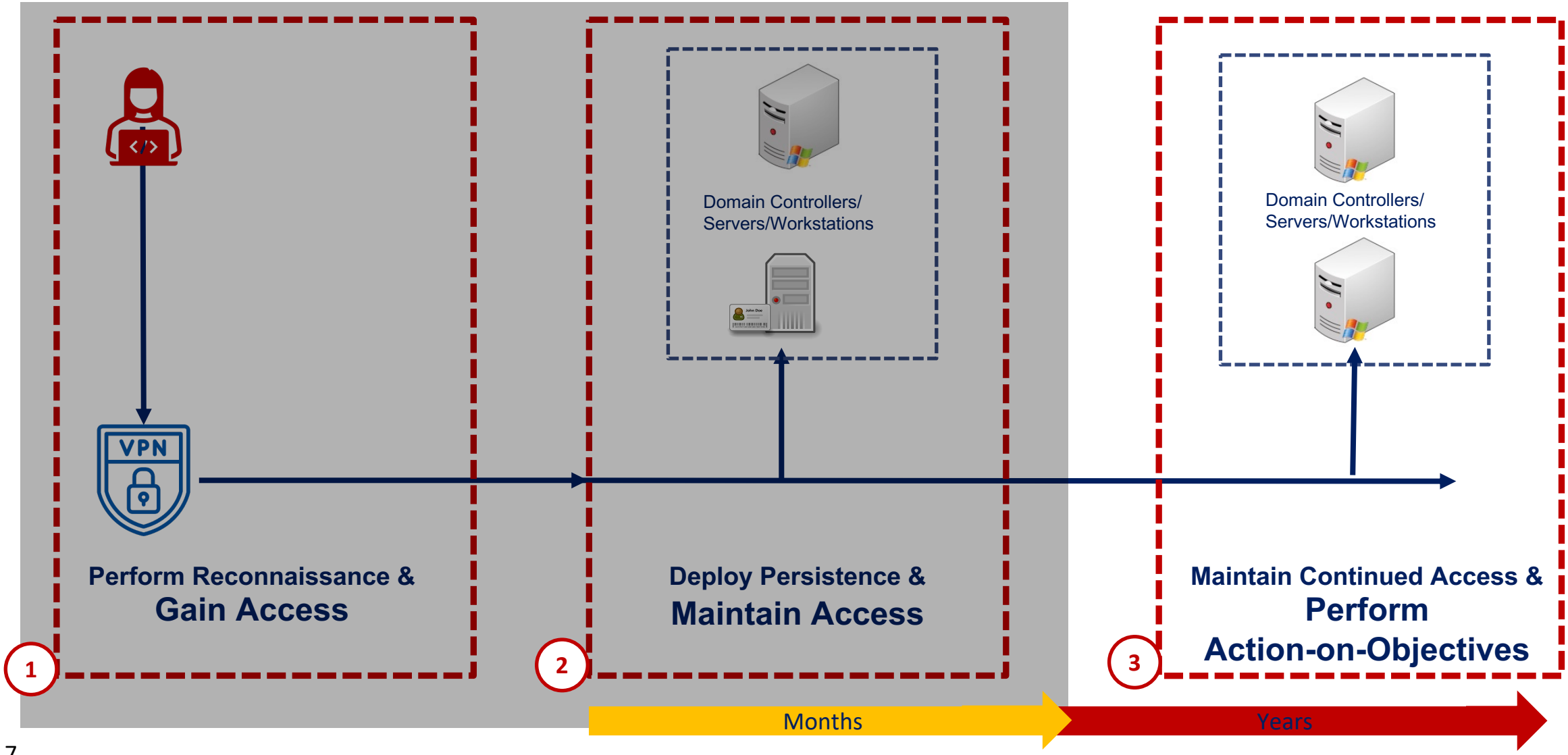
State-nexus intrusions are malicious cyberattacks that

- Originate from a particular country
- Adversaries working in interest of a State
- Well funded & resourced – attacker with a purpose
- Often includes
  - cyber espionage,
  - destructive and disruptive attacks
  - currency generation to support regime

Anatomy of Advanced Adversary



Anatomy of Advanced Adversary



Cyber espionage

Cyber espionage remains the primary motivation of state-nexus adversaries

LightBasin: A Roaming Threat to Telecommunications Companies

October 19, 2021 Jamie Harries and Dan Mayer From The Front Lines

networks via SSH and through previously established implants. CrowdStrike identified evidence of at least 13 telecommunication companies across the world compromised by LightBasin dating back to at least 201

November 10, 2021 • 5 min read

> The hunt for NOBELIUM, the most sophisticated nation-state attack in history

Disruptive/Destructive Attacks

- Destructive attacks from state-nexus adversaries have happened and continue
- Sony Pictures Attack, WannaCry, Ukraine power grid hack, NotPetya, DOS attacks

Alert (AA22-187A)

More

North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector

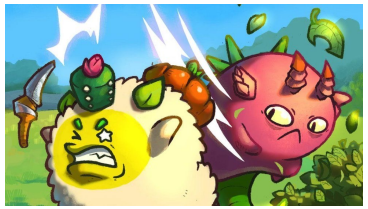
Original release date: July 06, 2022 | Last revised: July 07, 2022

Print Tweet Send Share

3 Action on Objectives

Crypto Heist

- Traditionally targeting of Banks to steal funds "2016 - Bangladesh Bank cyber heist"
- Now Transformed into Crypto Heist

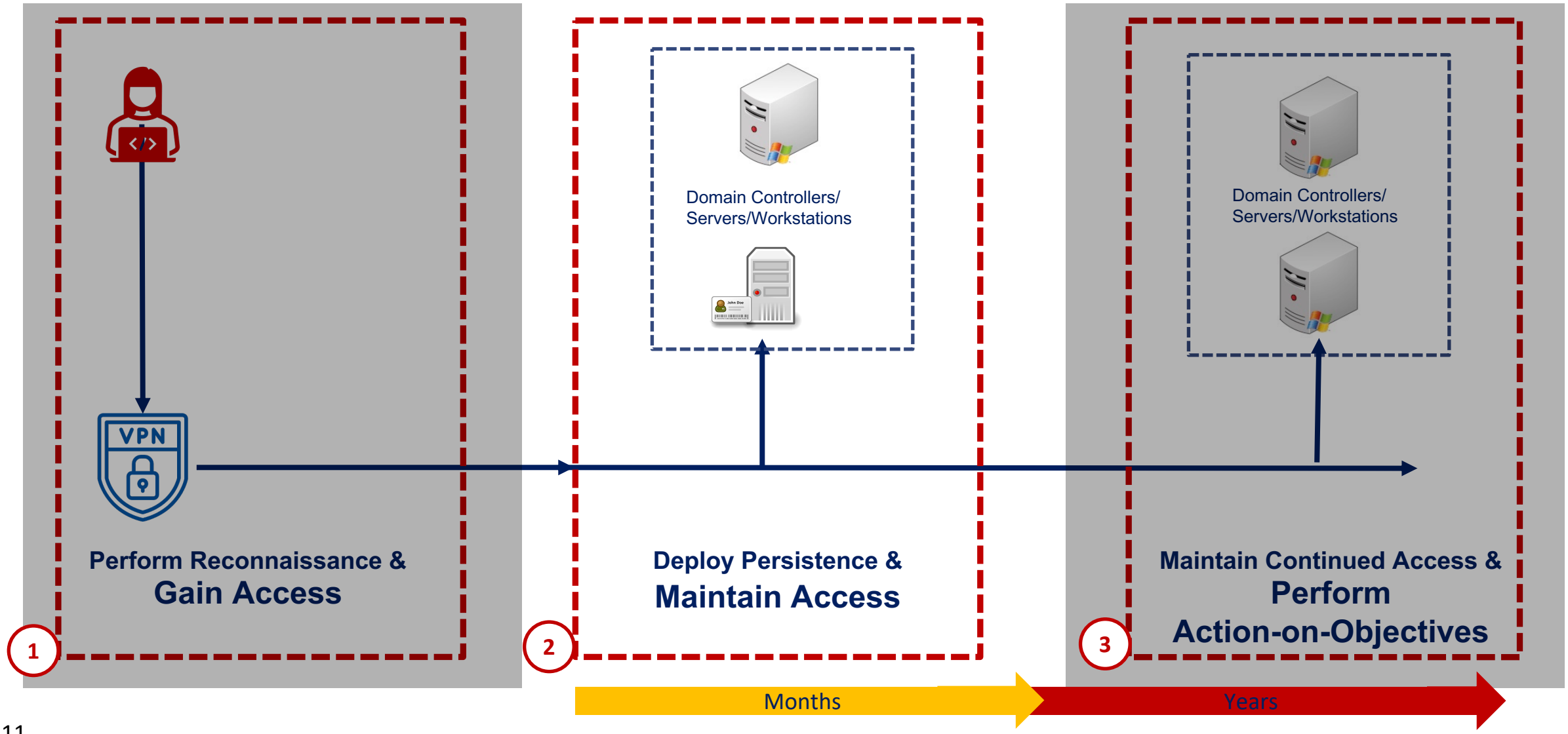


Alert (AA22-108A)

TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies

Original release date: April 18, 2022 | Last revised: April 20, 2022

Anatomy of Advanced Adversary



Covert Persistence - You do not see me!

- Deeply embedded access focused on Operational Security
- Persistent methods to maintain long term covert access
  - Backdoors and Implants
  - Valid Credentials connecting over VPN
  - Out of Band management software
    - AnyDesk, TeamViewer, ConnectWise
  - Stealthier approaches, GoldenSAML, Golden Ticket, ESXI based persistence

BLOG

Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors

ALEXANDER MARVI, JEREMY KOPPEN, TUFAIL AHMED, JONATHAN LEPORE

SEP 29, 2022 | 16 MINS READ

#MALWARE #BACKDOOR

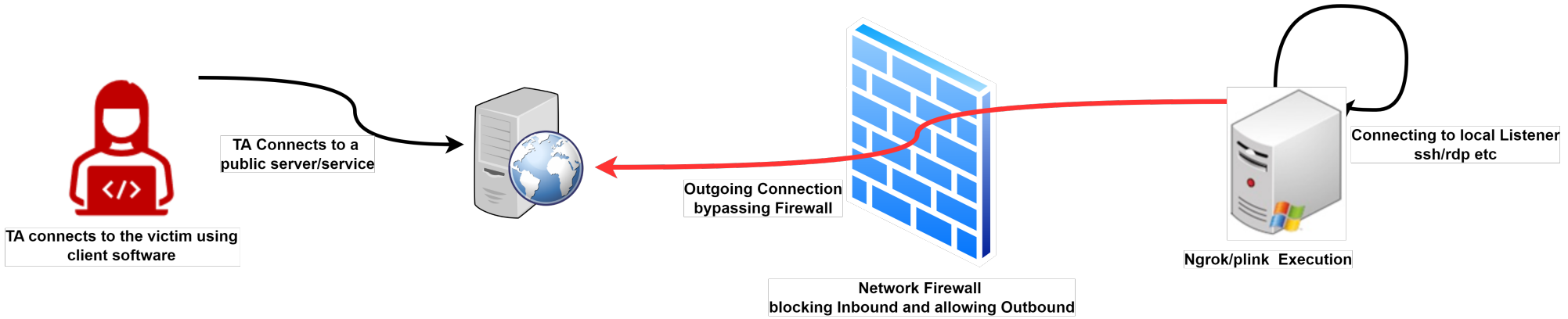
2 Maintain Access

Web Shells

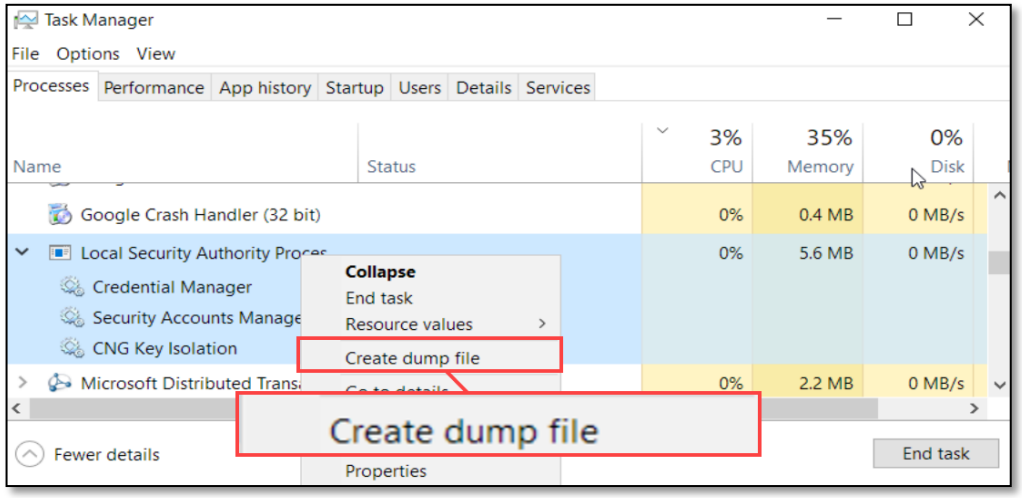
- Simple and effective
- Used as Initial vectors, deployed using vulnerabilities
  - ProxyShell, RCEs, Application Vulnerabilities
- Used as covert persistence mechanisms
  - Very difficult to detect
  - Require understanding the context

I come from No-Where- Reverse Proxy Tooling

- Used by Threat Actors to maintain covert access, by bypassing Firewalls
- Tools like Ngrok, SSH Clients (plink), fatedier can be used to perform tunneling



Credential Theft – dumping LSASS



Task Manager

```
C:\Tools>procdump -ma lsass.exe C:\tools\lsass.dmp
….
[04:02:26] Dump 1 initiated: C:\tools\lsass1.dmp
[04:02:26] Dump 1 writing: Estimated dump file size is 43 MB.
[04:02:26] Dump 1 complete: 43 MB written in 0.1 seconds
[04:02:26] Dump count reached.
```

SysInternals Procdump

Microsoft .NET

```
C:\Tools>createdump -u -f lsass.dmp -d 640
Writing full dump to file lsass.dmp
Dump successfully written
```

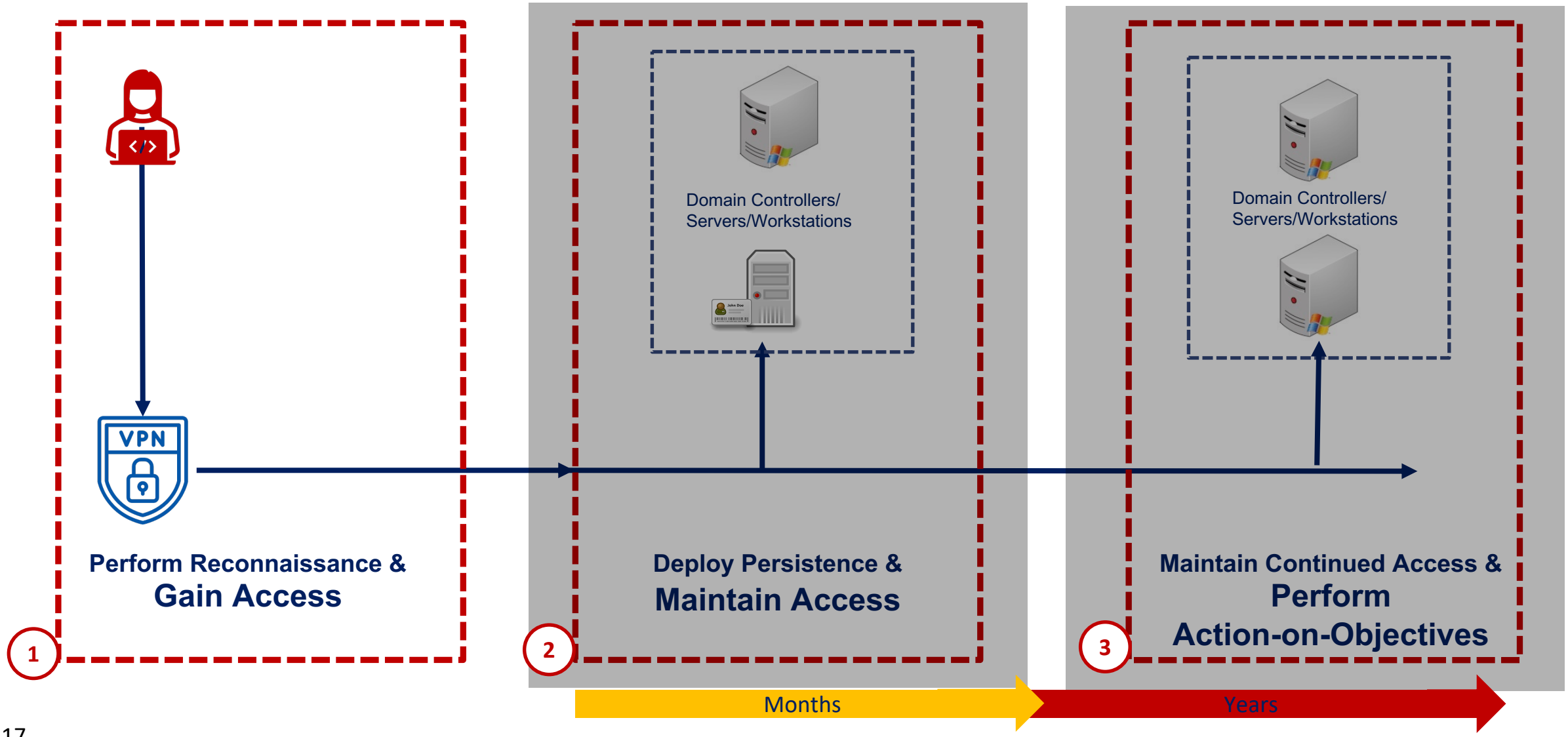
Dotnet Createdump

Credential Theft - Keys to the Kingdom – Dumping NTDS.DIT

```
C:\temp>powershell ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp\ntd' q q
Copying registry files...
Copying c:\temp\ntd\registry\SYSTEM
Copying c:\temp\ntd\registry\SECURITY
Snapshot {ddb1f6fa-a650-4f5b-b49e-074db672985e} unmounted.
IFM media created successfully in c:\temp\ntd
```

Stealing NTDS.DIT

Anatomy of Advanced Adversary



Reconnaissance and Information Gathering

- Nation State often spend considerable time gathering intelligence for their target – "*Patience is a Virtue!*"
- Willing to target victims over Social Networks to gain trust
- Identify vulnerabilities and novel techniques to exploit
- Exploit vulnerabilities and add persistence

Knock- Knock - Initial Vector

- Valid Credentials, Password Spraying (RDP, VPN…)
- Compromise Vulnerable internet facing systems
- Spear Phishing
- Supply Chains, Partners, Global offices

CrowdStrike Falcon Platform Identifies Supply Chain Attack via a Trojanized Comm100 Chat Installer

September 30, 2022 CrowdStrike Intelligence Team From The Front Lines Research & Threat Intel

Microsoft Releases Guidance on Zero-Day Vulnerabilities in Microsoft Exchange Server

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Original release date: September 30, 2022

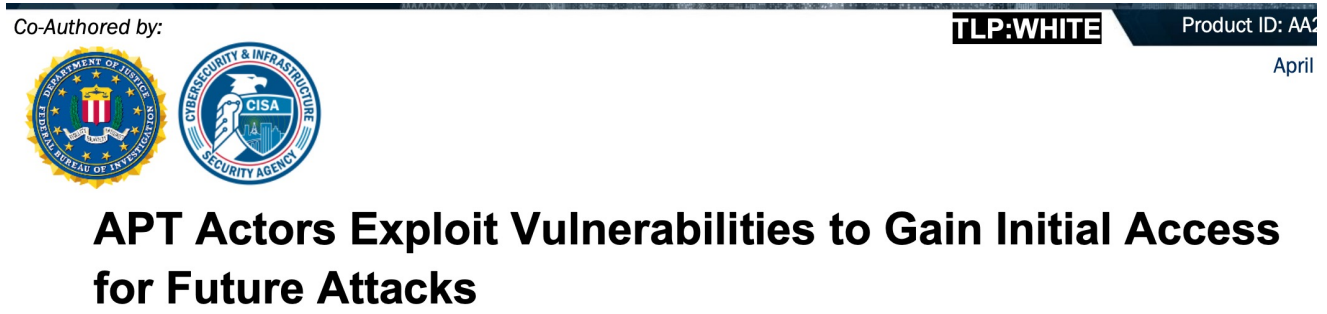
Print Tweet Send Share

Microsoft has released Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server. According to the blog post "Microsoft is aware of limited targeted attacks using the two vulnerabilities to get into users' systems." The two vulnerabilities are CVE-2022-41040 and CVE-2022-41082, affecting on-premises Microsoft Exchange Server 2013, 2016, and 2019

"Microsoft is aware of limited targeted attacks using the two vulnerabilities to get into users' systems."

1 Gain Access

I know you were Vulnerable last summer!



Zoho ManageEngine Password Manager Zero-Day Gets a Fix, Amid Attacks

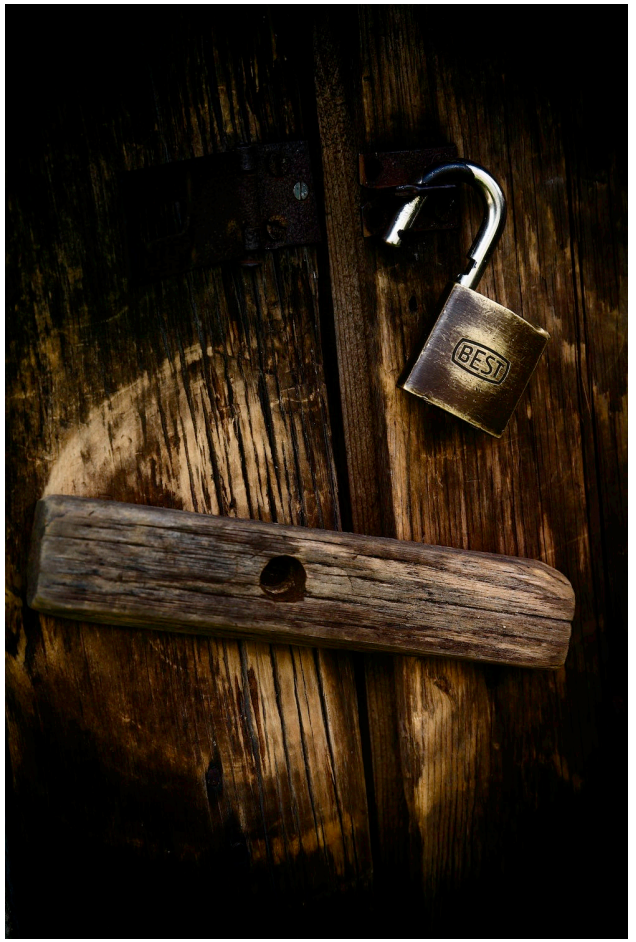
March 2, 2021 • 9 min read

HAFNIUM targeting Exchange Servers with 0-day exploits

1 Gain Access

Multi Factor Authentication

- MFA is the cost of doing business on the Internet.
- But MFA is not a a silver bullet
  - MFA Fatigue attacks
  - Accounts/Groups without MFA
  - Dormant account usage
  - Self-Enrollment process



Gain the Control back

Coordinated Remediation Event?

Whac-A-Mole

Game-of-Chess

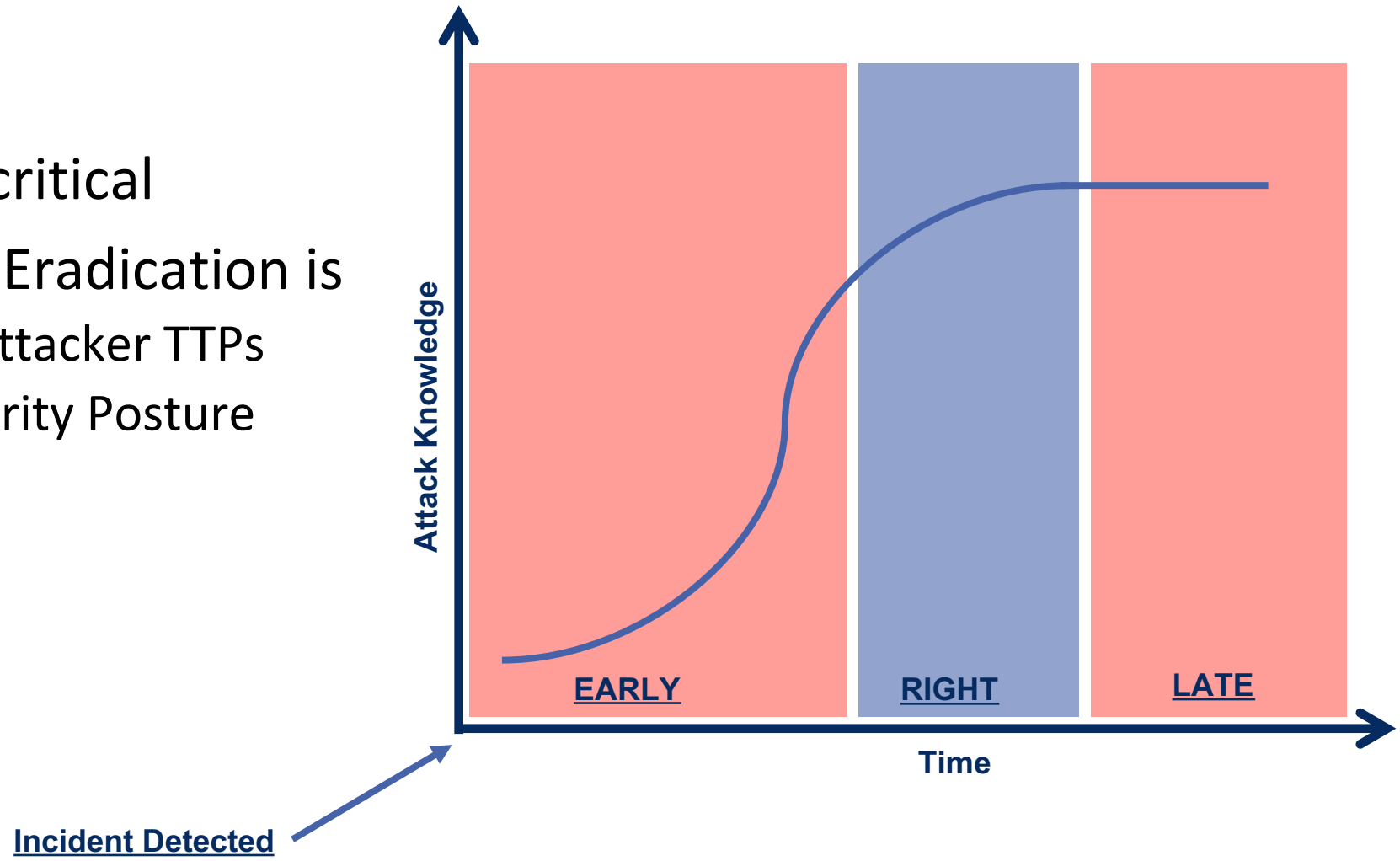
1,2,3 and poof!

1. Gain Host based Visibility
2. Understand the Intrusion
3. Perform a Removal Event

But When to Eradicate?

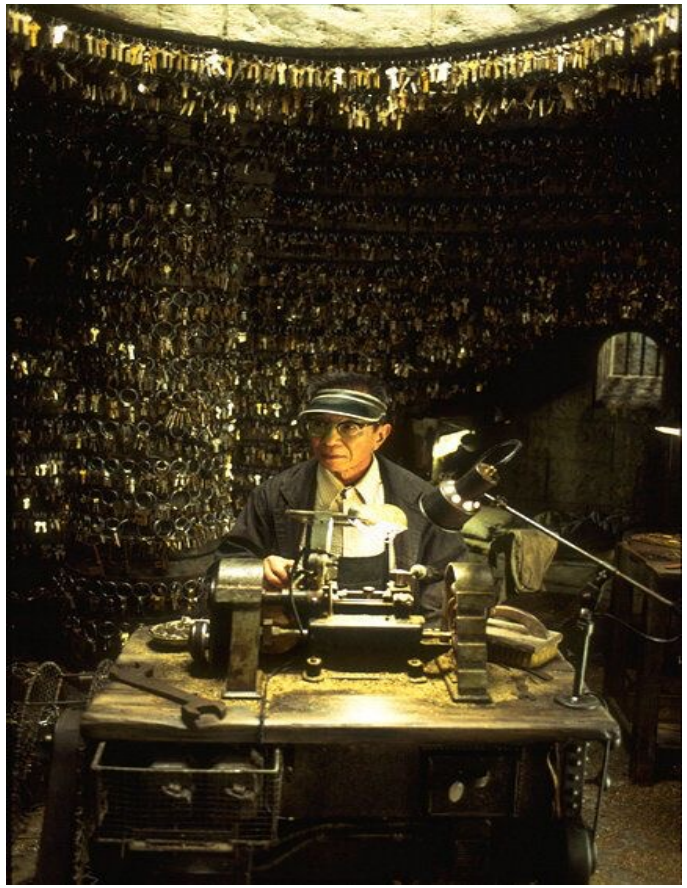
Timing is the key!

- Eradication timing is critical
- Best time to perform Eradication is
  - Post understanding attacker TTPs
  - Improvement of security Posture
  - Incident scoped



Change All the Keys! – Enterprise-Wide Password Reset

1. Perform KRBTGT (Kerberos account) Password reset
2. Execute Password reset for ALL accounts
   - Service Accounts
   - Privileged Accounts
   - User Accounts
3. Reset Directory Service Restore Mode Password Reset (DSRM) – All DCs
4. Reset Domain Trust keys, Certificates for IDPs



Change All the Keys! – Enterprise-Wide Password Reset

5. Ensure MFA coverage
6. Network Devices
7. Reduce Computer account password rotation period
8. Reset Local Administrator Passwords for ALL endpoints
9. Reset Application Passwords

What to do if you have an intruder ?

- Slow Down
  - Fast is not Fast – Smooth is Fast!
- Stay Calm
- Create a Plan
  - External support
  - Improve visibility
  - Create eradication plan
- Execute it

Take-Aways

- Slow Down - Stay Calm
  - Fast is not Fast – Smooth is Fast!
- Make a plan and execute
- Visibility is the difference between a successful eradication and failed one
- Prepare for long haul

Thanks for listening!

Anurag Khanna

@khannaanurag

www.linkedin.com/in/khannaanurag