Supply chain dangers and disruptions.

ISC2 CHAPTER MEETING

BRANDON BENSON

JULY 16, 2020

#whoami

Brandon Benson

- CISSP since Mar 2008
- SOC Manager
- 15+ years in cyber security
- Curious learner

What I've done over my career…

- Worked with companies to secure sensitive data.
- Help companies implement security procedures and policies
- Investigated breaches from both internal and external sources
- Run a FedRAMP authorization program for a large CSP.

Why this presentation

- Many of our jobs deal with the security of the cyber footprint of our employers.
- In many cases, we do a good job implementing coverage and risk mitigations for the basics. Network segmentation, AV, RBAC, MFA, etc.
- Unfortunately attackers continue to evolve and develop new attack techniques.
- The fight will never end for the defenders.

Supply Chain vulnerabilities

- We've heard about supply chain attacks in the news and at conferences.
- For me, many seemed theoretical or not applicable to my environment.
  - The Western Digital firmware malware in the early 2000's
  - POS device swaps for PCI
  - Shipping industry supply chain disruptions
  - Malware on CD's during a security conference one year

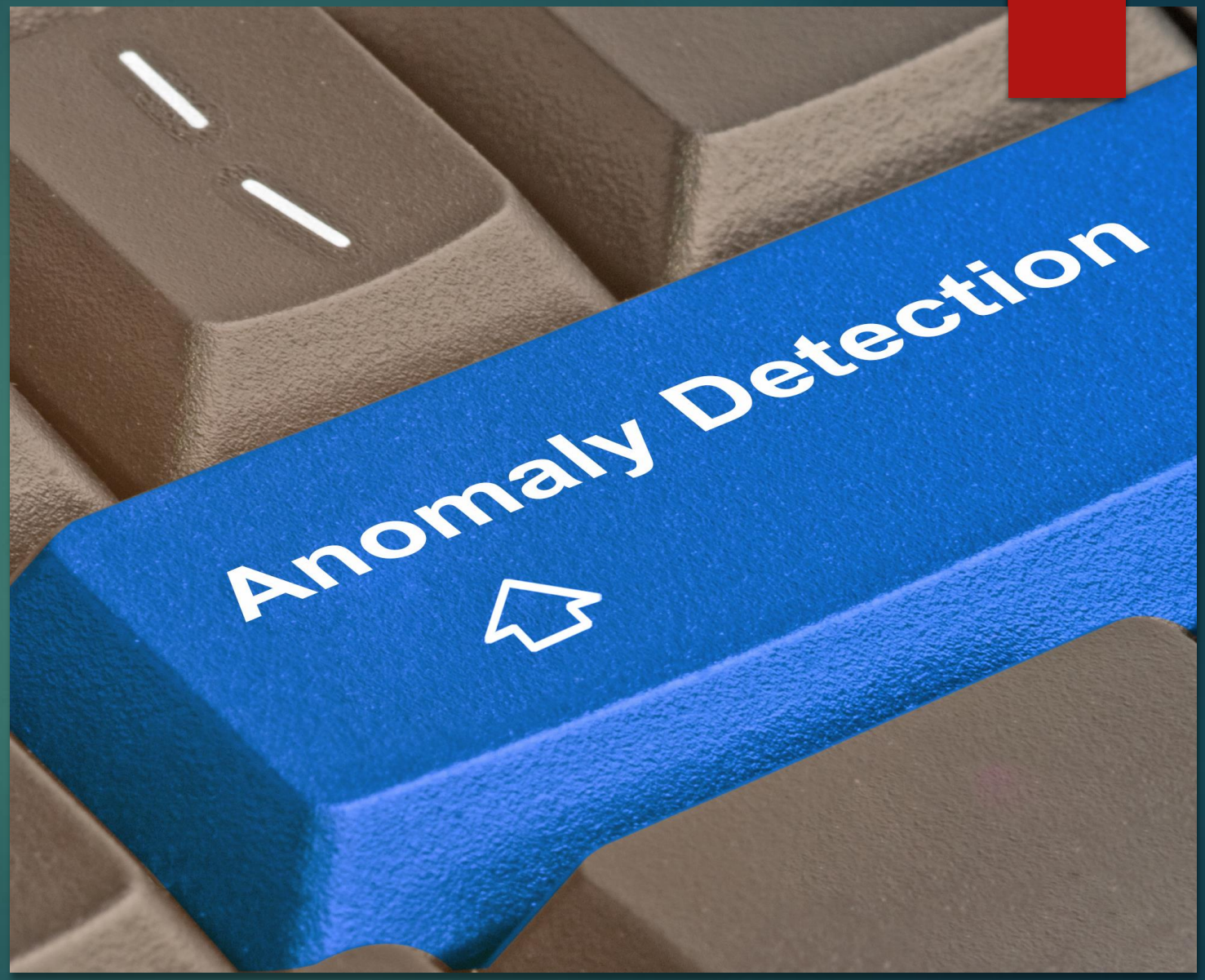
However over the last year I've investigated three that were relevant to my job.

Supply chain vulnerability analysis and case studies.

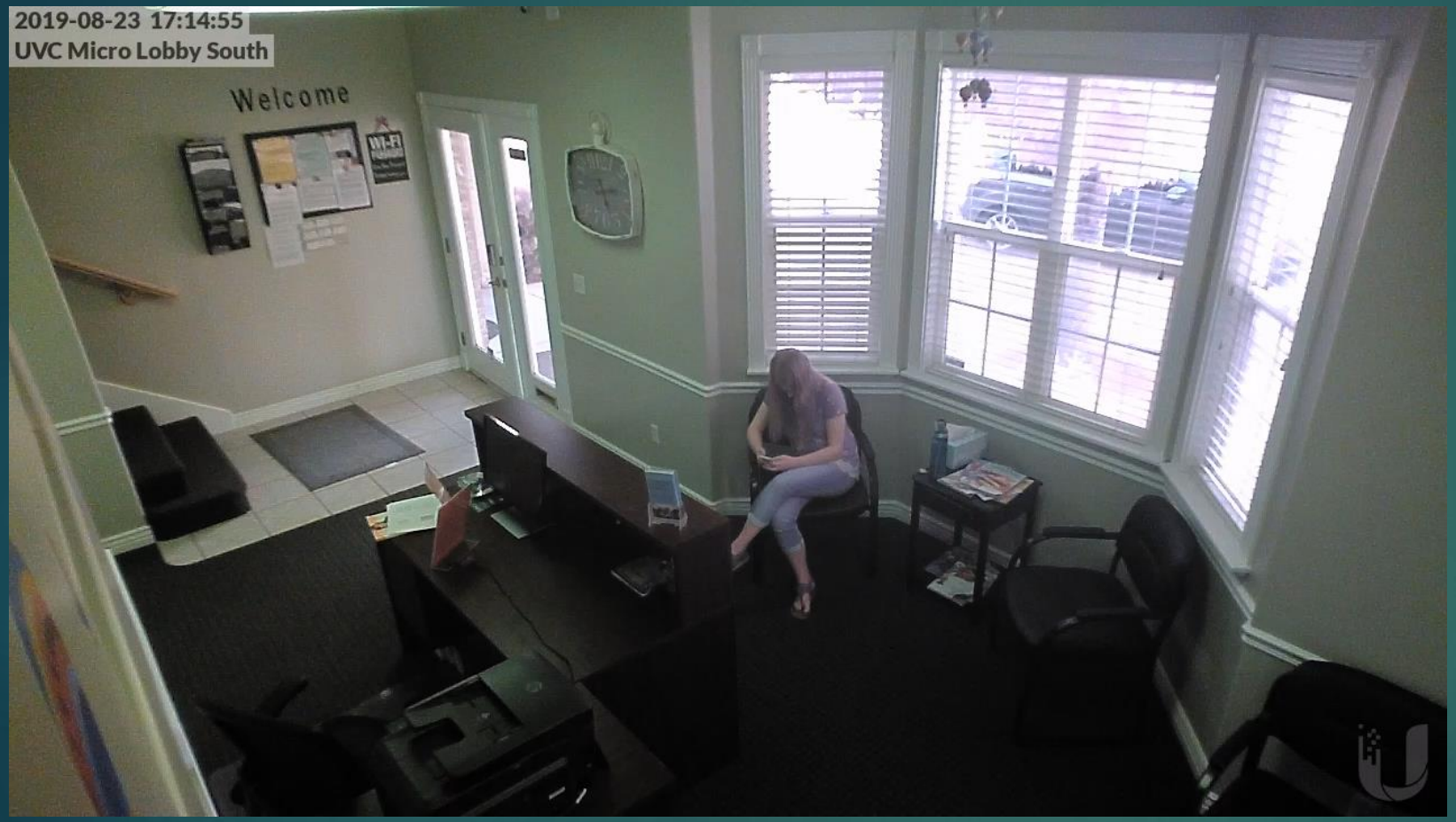
- 1. Third party Software
- 2. Third party access.
- 3. A combination of the two

Before we start

- It is beneficial to understand a typical attacker methodology.
- Most attacks follow four general steps



Example



The result

Several hours later…

Reconnaissance

- The attacker performs reconnaissance and probing of a system. They identify a target and develop a plan based on opportunities for exploitation.

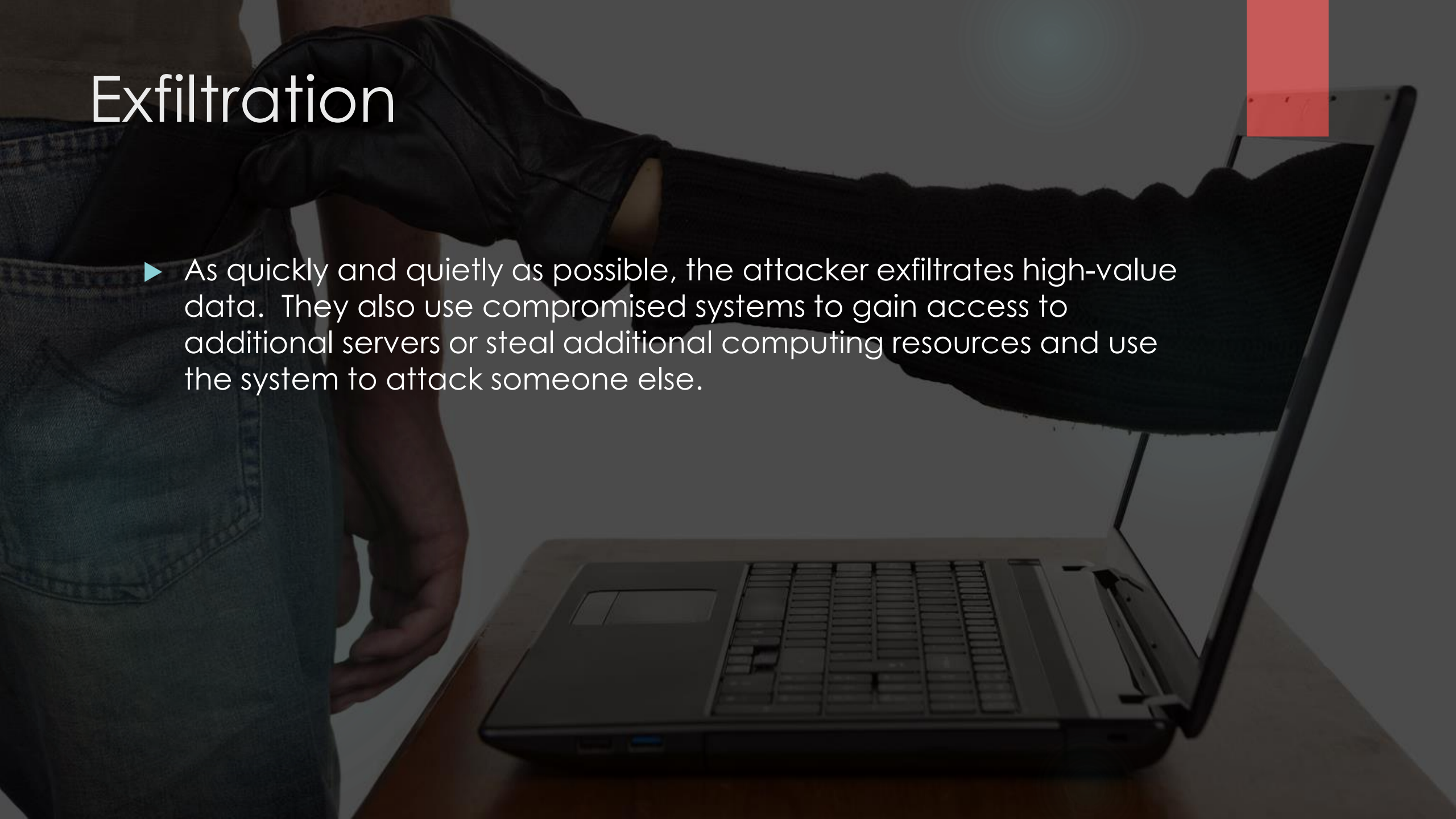
Execution

- The attacker executes the attack and delivers the payload. They place their delivery mechanism online. They use system vulnerabilities or social engineering to gain access to the system.

Exploit

- The attacker exploits the system to place their payload. Where possible, they elevate privileges and install persistence on the system.

Exfiltration



- As quickly and quietly as possible, the attacker exfiltrates high-value data. They also use compromised systems to gain access to additional servers or steal additional computing resources and use the system to attack someone else.

Case Studies:

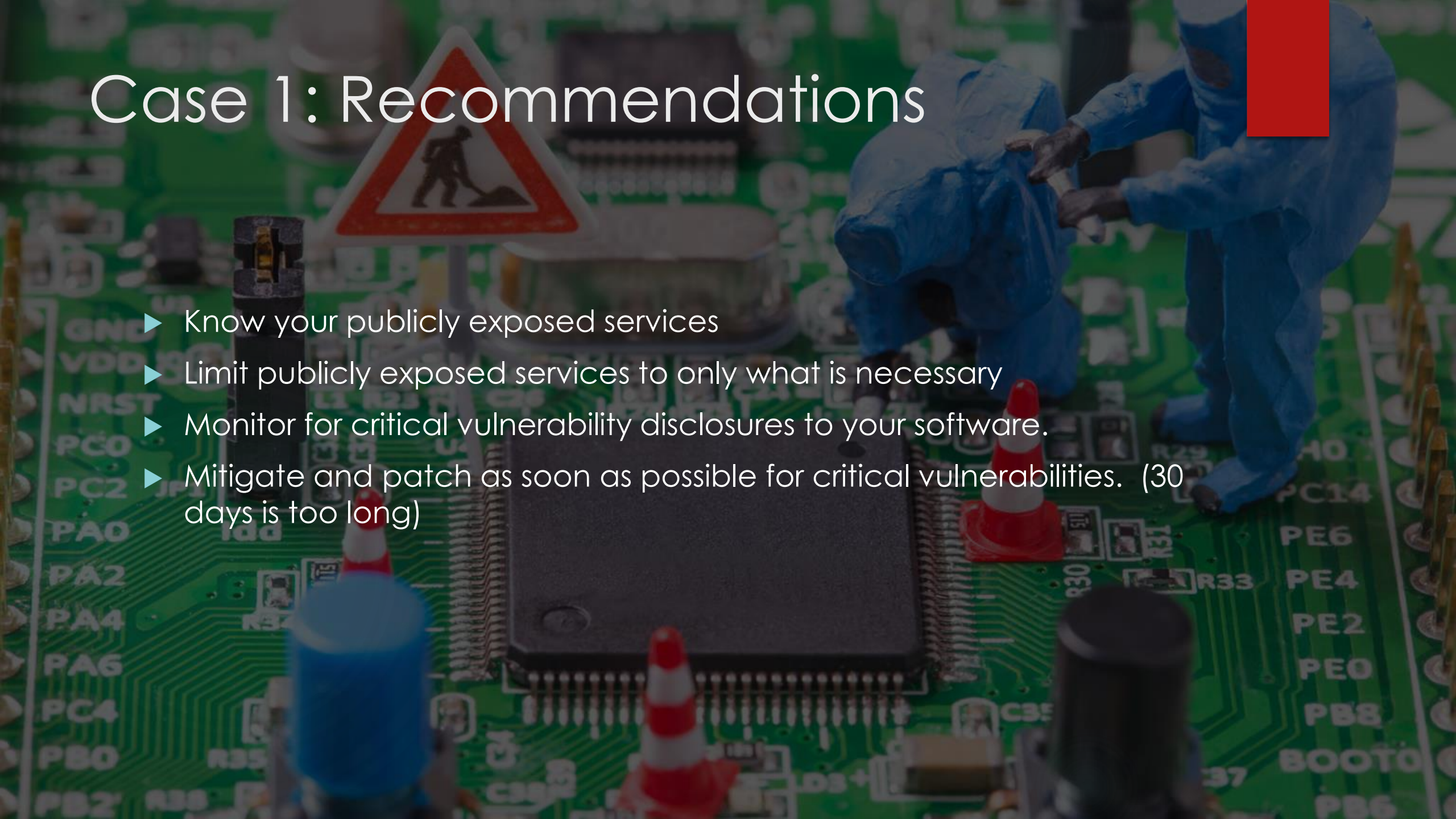
Case 1: Scenario

- A ticketing system released a critical vulnerability which allowed an attacker to bypass system authentication through an arbitrarily code execution vulnerability (RCE - Remote Code Execution).
- A case I worked with had this ticketing system publicly exposed so that their end users can submit problem tickets and requests.
- Within a few days of the vulnerability being exposed attackers had created a payload and compromised several systems in the industry.
- I learned about it when it was mentioned on one of the news feeds I subscribe to.
- I worked with my customers to mitigate the threat while the patch was implemented.

Case 1: Attack

- Vendor disclosed a critical vulnerability that allowed RCE
- The malicious actor reviewed the disclosure and developed an attack payload.
- The attacker scanned internet looking for publicly available hosts.
- When hosts were identified they initiated the attack.
- The attacker injected payload and compromised systems.
- Results: several companies had compromised hosts.

Case 1: Recommendations



- Know your publicly exposed services
- Limit publicly exposed services to only what is necessary
- Monitor for critical vulnerability disclosures to your software.
- Mitigate and patch as soon as possible for critical vulnerabilities. (30 days is too long)

Case 2: Scenario

1. Vendor or contractor had system access for support or other activities.

Vendor was phished or somehow lost their SSH keys.

Case 2: Attack

- A customer had contracted a vendor for support or development activities.
- The vendor was phished or otherwise compromised.
- Through that compromised the attacker obtained SSH keys to our customer's system.
- The attacker then proceeded to access the system and place malware designed to steal sensitive data and send it back to a remote host.
- The attacker also established persistence on the server to receive and execute commands as well as exfiltrate data.

Case 2: Recommendations

Implement key management requirements for vendors.

Implement key rotation requirements

Implement MFA for SSH access.

Do not allow vendors to use the same key for multiple customers. (e.g. key used to access zyzcorp can't be used to access yourcorp)

Case 3: Scenario

- Vulnerability in server management software.
- Vendor is using the software
- Vendor was compromised through a new exploit.
- The attacker pivoted from the vendor system to compromise their client system.

Case 3: Attack

- Vendor is using a system management tool to manage systems of several customers. (Think how the WSUS server was used to compromise all Target payment devices in 2014)
- The system management software company disclosed a critical vulnerability that allowed RCE.
- The attacker reviewed the disclosure and developed an attack payload
- The attacker scanned internet looking for vulnerable hosts.
- Injected payload and compromised systems.
- Payload also looked for recent connections to other hosts and attempts to compromise them.
- Client's host subsequently infected with malware as the vendor recently connected to it.
- Malware was dropped on or customer's system through the vendor connection.

Case 3: Recommendations

- If possible, understand the tools your vendors use to access your systems.
- Monitor for critical vulnerability disclosures to software that could affect the security of your environment.
- Establish partnership with vendor to address critical vendor critical vulns quickly.
- Mitigate and patch as soon as possible for critical vulnerabilities. (30 days is too long)
- Where possible implement key management and lifecycle requirements.
- Where possible implement MFA for all vendor access.

TAKE AWAY

Every investigation and learned attack technique should be examined to improve our overall security program.