PREVENTING DNS INFRASTRUCTURE TAMPERING

Notice

Commercial Endorsement Disclaimer: The United States Government through the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA or DHS.

Simulated Non-Production Data Disclaimer: No production data was used in this demonstration.

Sensitive Information Disclaimer: Be aware that this event is live! Events such as these are attended by people from many different federal agencies. As a student, PLEASE DO NOT DISCLOSE ANY AGENCY SENSITIVE INFORMATION DURING THIS EVENT.

CISA Comment Policy: This course abides by the CISA Comment Policy (www.cisa.gov/cisa-moderation-comment-policy).

DISCLAIMER: This webinar is being recorded and may be made public for the benefit of other students. While you are encouraged to engage with the speaker, you are advised against disclosing personally identifiable information (PII) on the recording. Please contact licensing@cisa.dhs.gov with any questions or comments.

Agenda

Introduction and Overview

- Course Description
- Learning Objectives
- Overview

DNS Tampering Attacks

- Identification
  - Knowledge Checks
- Mitigation
  - Knowledge Checks
- Response/Recovery
  - Knowledge Checks

Case Studies

- Operation Ghost Click
- Brazilian Bank

Resources & Additional Reading

Learning Objectives

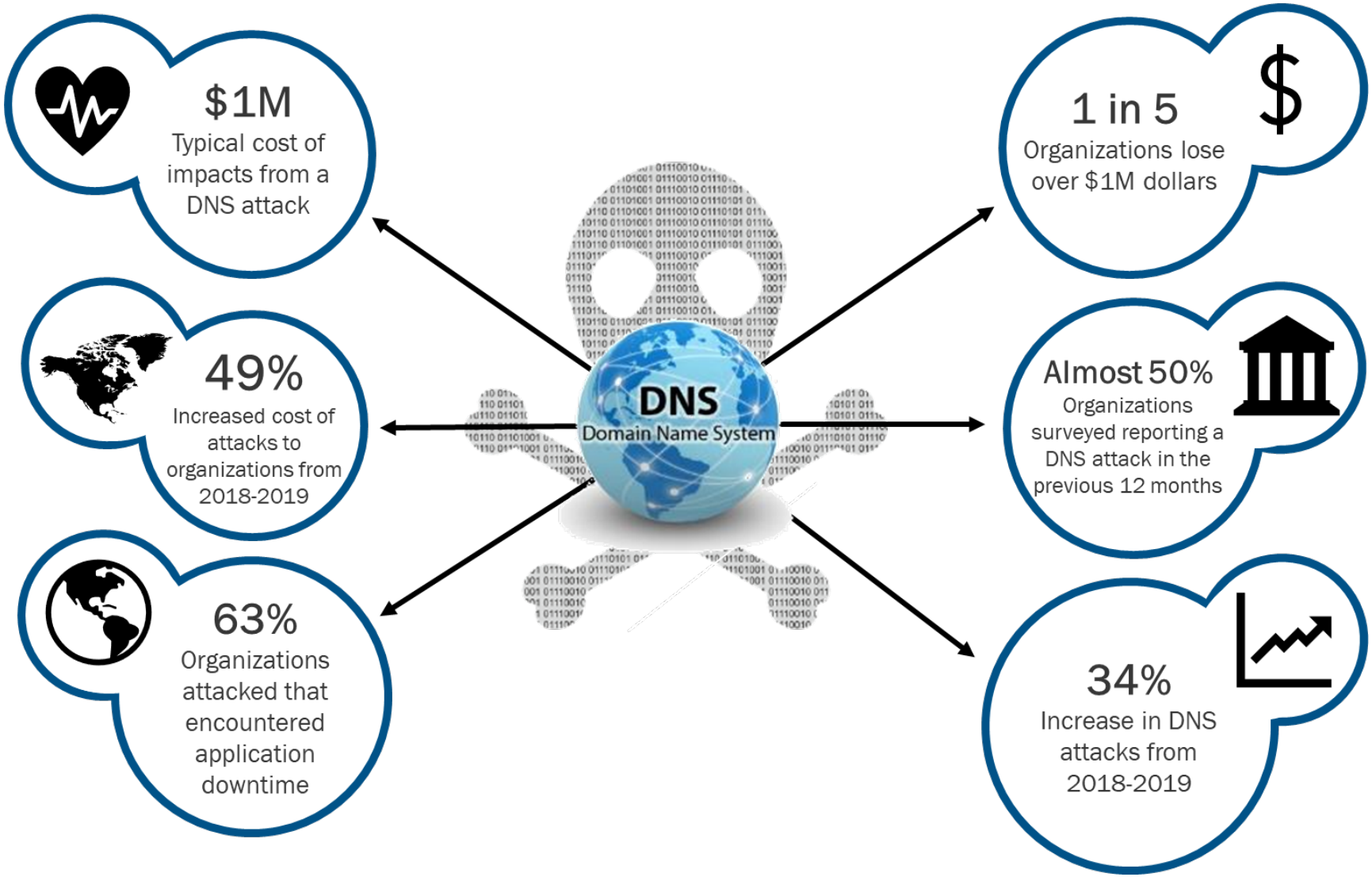
Terminal Objective

Identify the fundamentals of Domain Name System (DNS) Tampering and the impact it can have on your organization.

Enabling Objectives

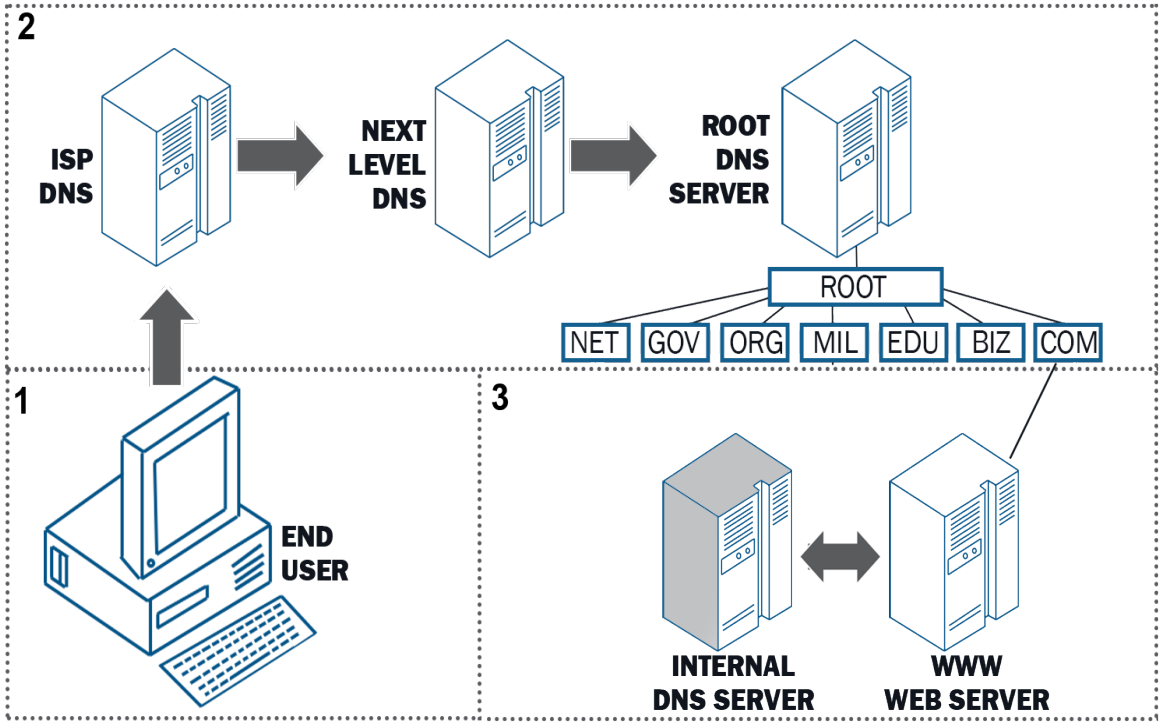
- Define DNS Tampering
- Identify signs of a DNS attack
- Learn mitigation steps of a DNS attack
- Explain the process to recover from a DNS attack
- Explore impacts of DNS attacks through case studies

Domain Name System



What is DNS?

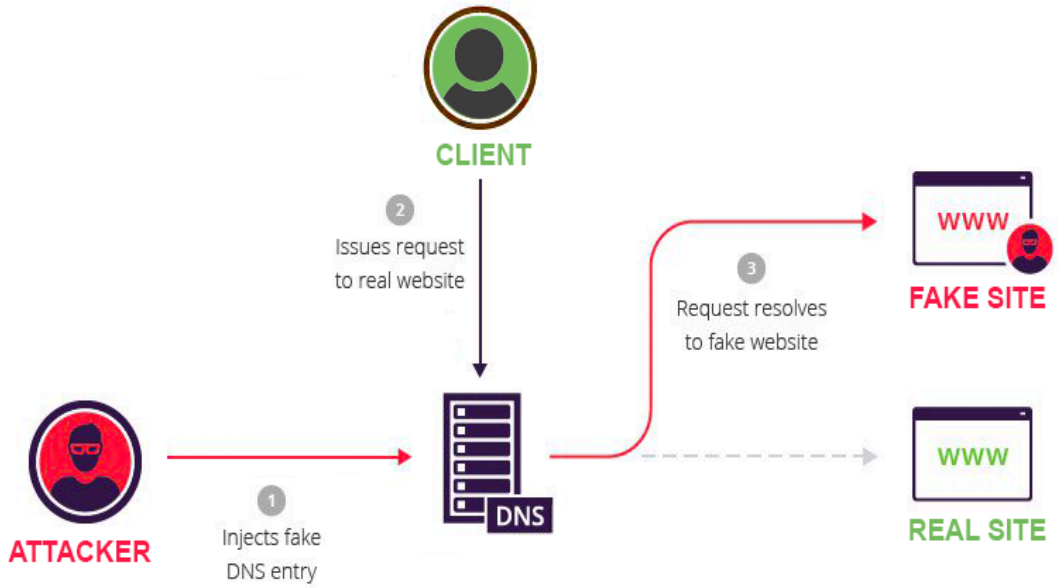
The **Domain Name System (DNS)** is like the phonebook of the internet.



1. People access information online through domain names, like nytimes.com or nasa.gov.
2. Web browsers interact through Internet Protocol (IP) addresses.
3. DNS translates domain names to IP addresses so browsers can load internet resources.

Examples of DNS Attacks

- DNS Infrastructure Tampering – attackers obtain privileged user credentials and use them to access the DNS to change the DNS registry.
- DNS Poisoning (aka DNS spoofing) – attackers corrupt DNS resolver cache memory, causing the DNS to redirect internet traffic to malicious websites.
- DNSpionage – creation of remote server administrative tools where malware sets up HTTP and DNS communication with the attacker's command and control.



https://www.cisa.gov

https://www.cisa.gov

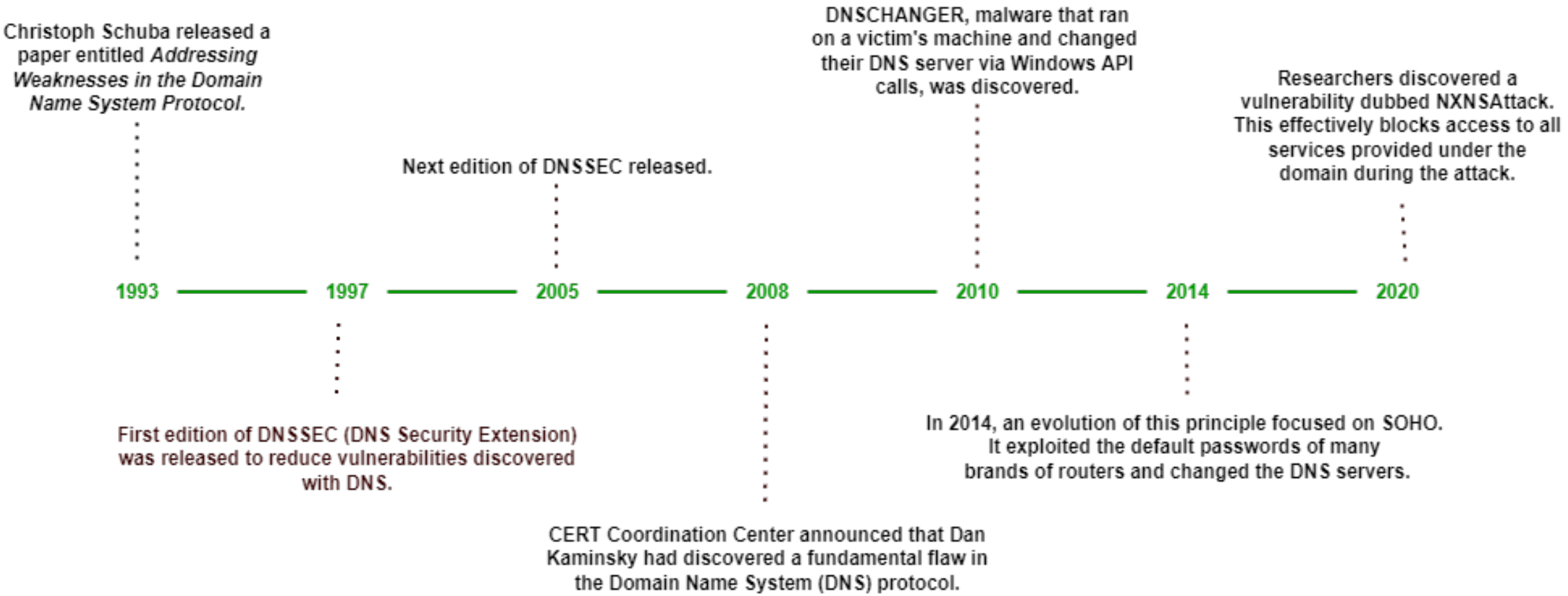
Threat Overview

Decentralization of DNS ecosystems make monitoring difficult

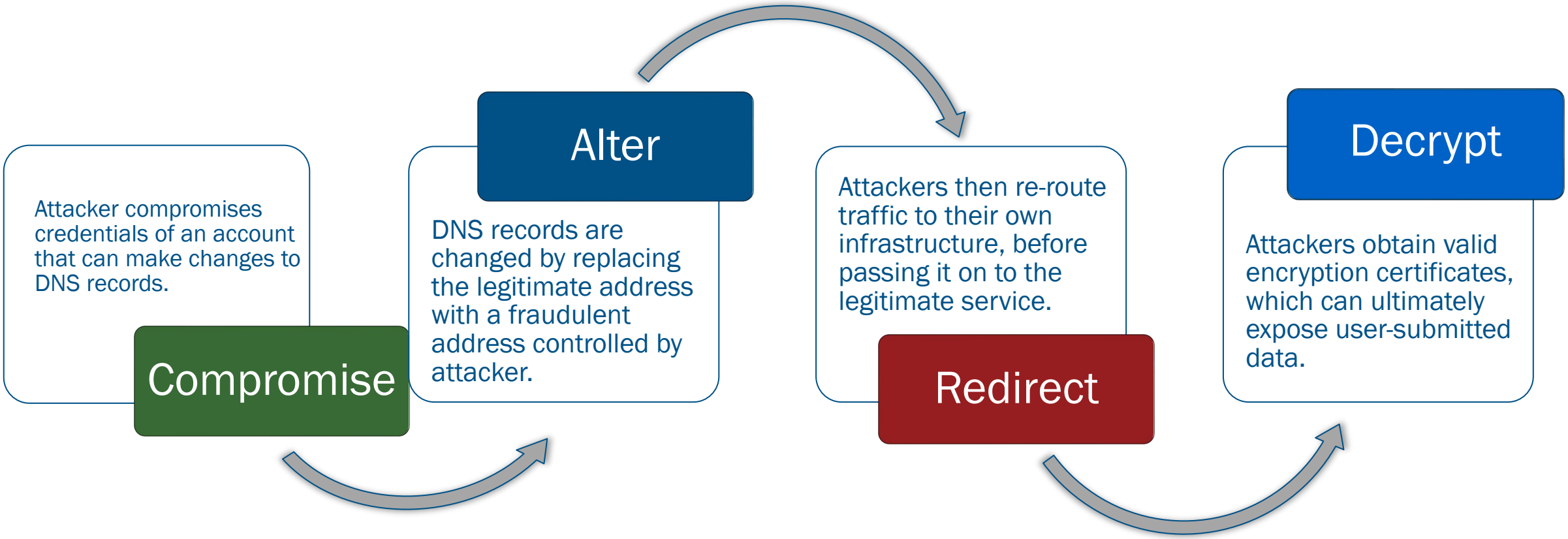
Increase in attackers intercepting & redirecting web and email traffic

Risks persist beyond the period of traffic redirection

History of DNS Security

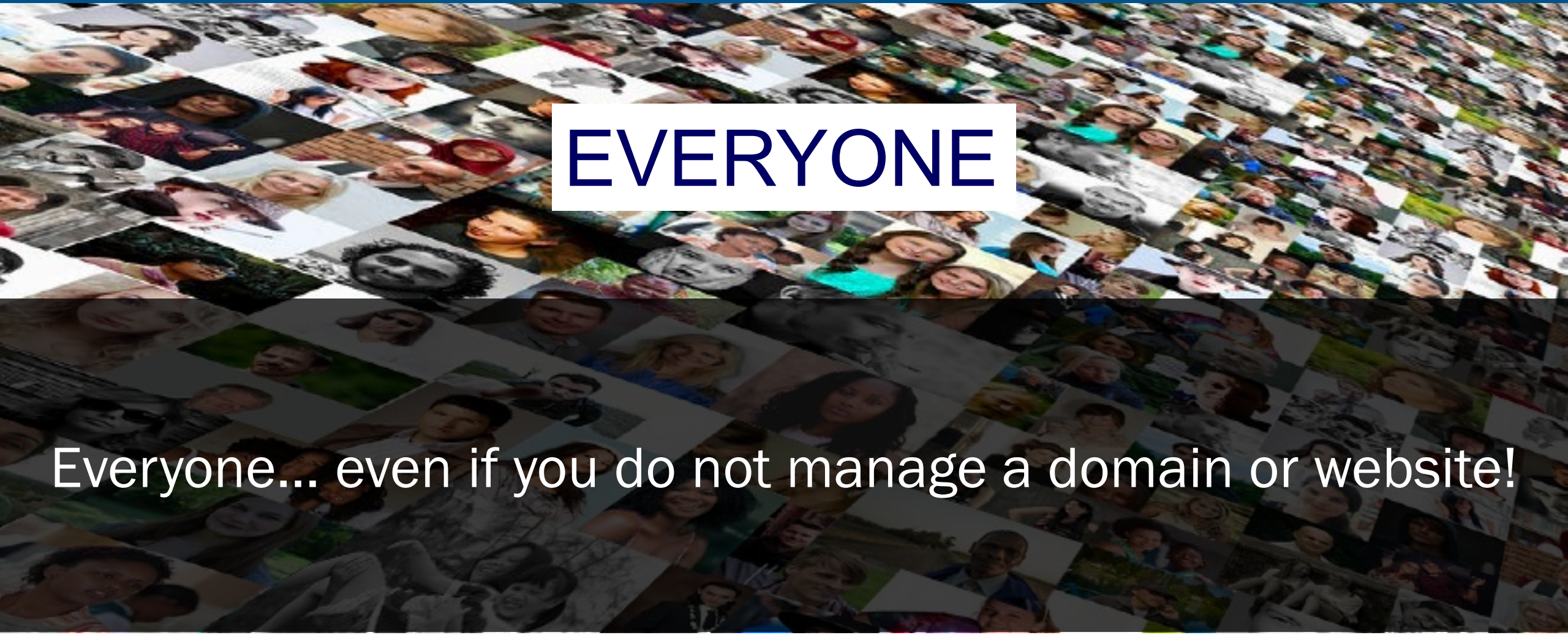


How DNS Tampering is Made Effective



Though various attacks and case studies show DNS ecosystem components being used maliciously, the defense or detection against those attacks varies widely and is usually NOT a DNS-centric security measure.

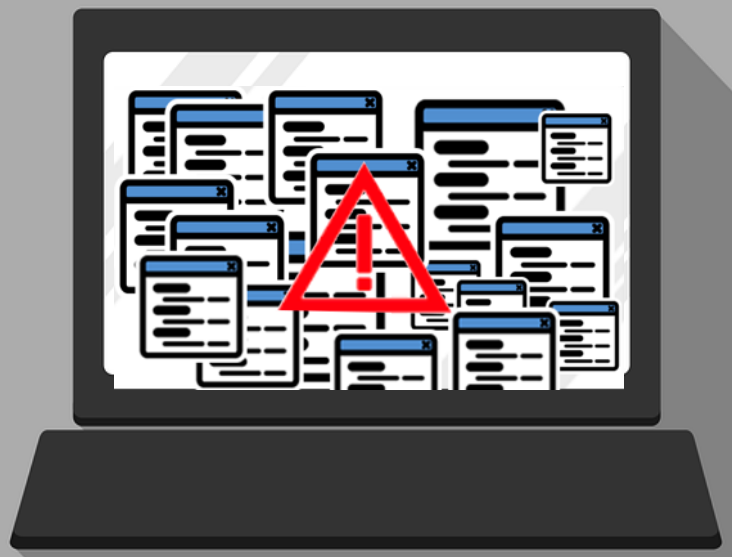
Who is susceptible?



Everyone… even if you do not manage a domain or website!

Identify the Signs of a DNS Attack

- Websites for the given agency, business, or individuals' systems begin loading much slower than usual
- Browser shows incorrect website information as compared against independent information sources
- Irrelevant and unwelcome pop-up ads surface on computers



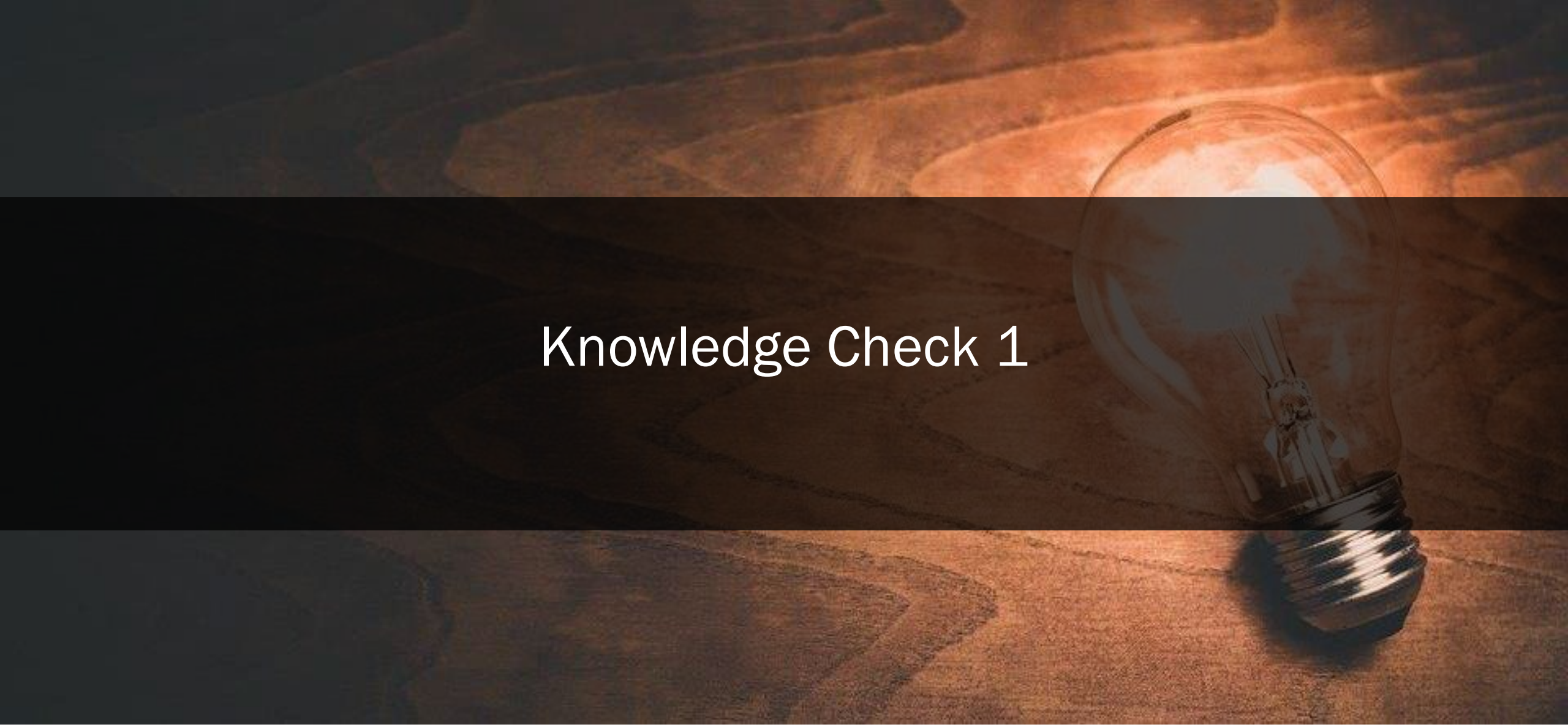
DNS Tampering Mitigation

CISA INSIGHTS CYBER

Mitigate DNS Infrastructure Tampering

Recommended Actions

1. Review DNS Records
2. Change DNS Account Passwords
3. Add Multi-Factor Authentication to DNS Accounts
4. Monitor Certificate Transparency Logs



Knowledge Check 1

Preventing DNS Spoofing

- Always check for HTTPS in the URL
- Maintain updated antivirus software
- Disable JavaScript and WebRTC
- Choose an encrypted DNS service that validates DNSSEC and a trustworthy open resolver (i.e., Google, Cloudflare, Quad9, Cisco)

DNS Attack Recovery: Near-Term Response

Incident Response and Recovery:

- Verify security vendor service-level agreement (SLA)
- Review DNS records and public domain records
- Identify weak spots and exploits used
- Work with vendors or network administrator(s) to re protocol (BGP) connections
- Check and restart firewalls and other apps
- Get unblocked by your ISP
- Begin application recovery

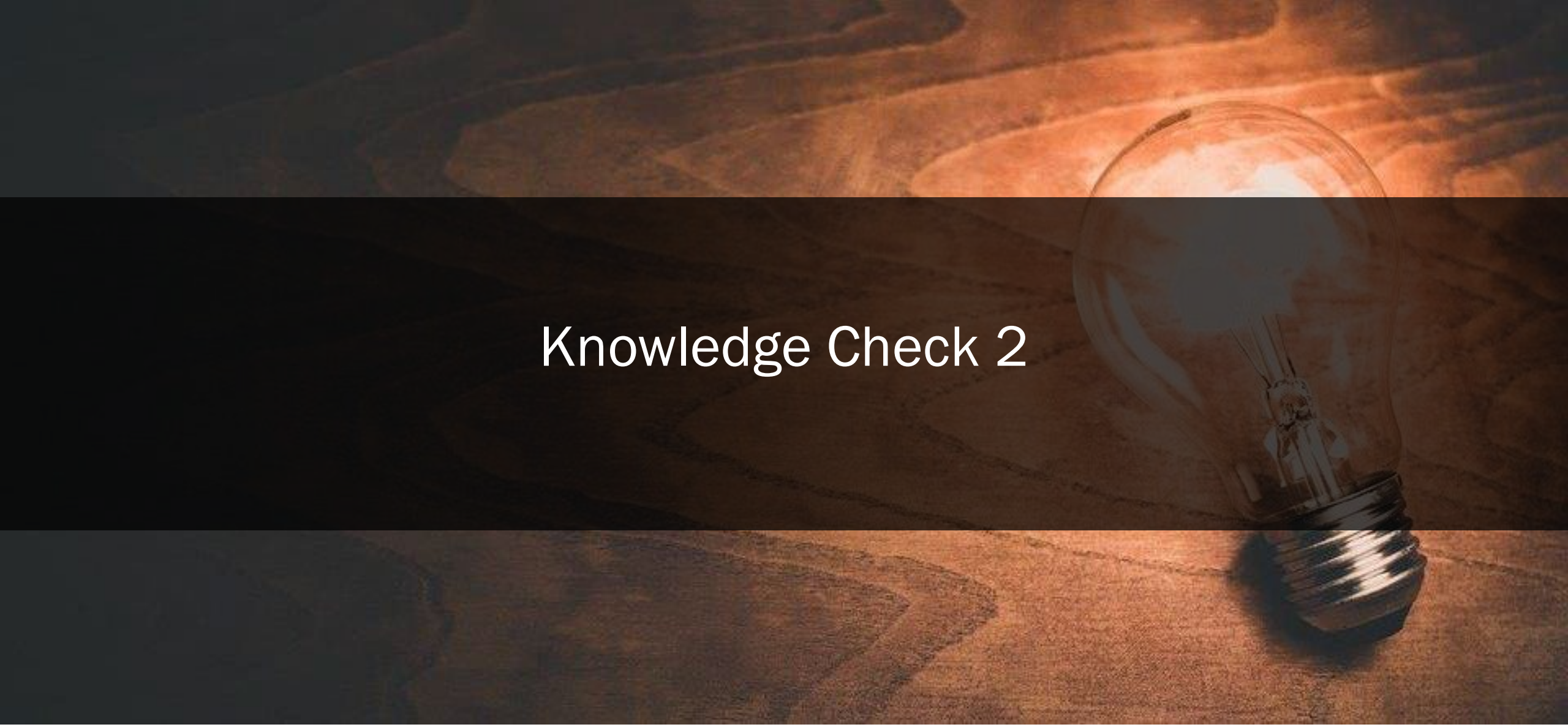
DNS Attack Recovery: Long-Term Preparation

Before an Attack:

- Annually review DNS protection plan, and practice incident response plan
- Analyze investments to upgrade defenses
- Work with other departments to analyze cost of downtime and prioritize business functions

After an Attack:

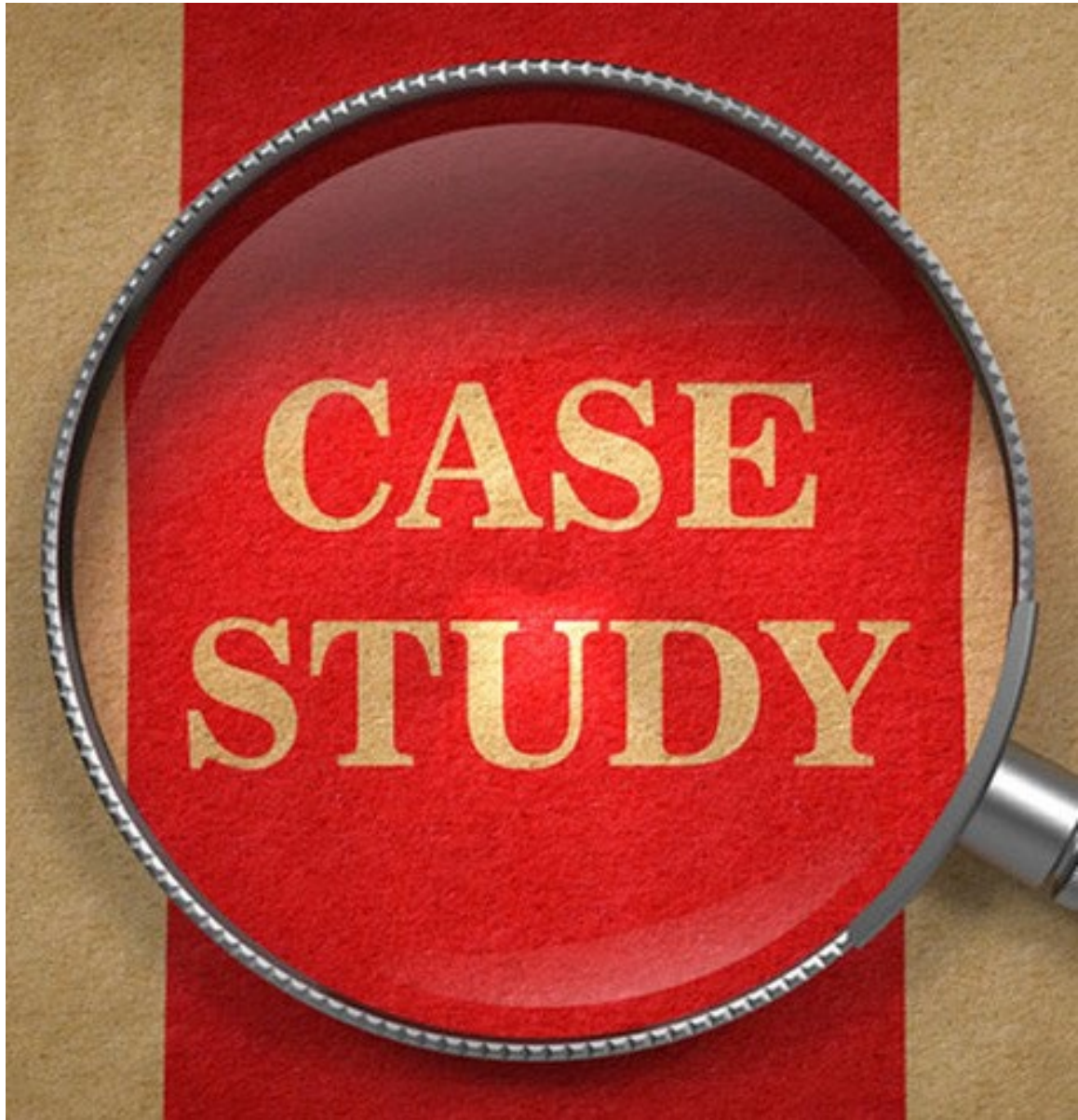
- After Action Review:
  - What was the target?
  - How long was the network affected?
  - How was the attack carried out?
  - Did third-party vendors perform as expected?



Knowledge Check 2

DNS Tampering Case Studies

- Operation Ghost Click/DNSChanger
- Brazilian Bank Website Hijacked



Operation Ghost Click – Overview

Scenario Overview

- Six Estonian nationals and one Russian national were responsible for infecting more than **4 million computers in over 100 countries** with malware that altered DNS server settings on infected computers.
- The scheme lasted for four years.

Attack Vector

- Victims' computers became infected with malware when they visited certain websites or downloaded certain software to view videos online.
- The malware altered the DNS server settings on victims' computers, **routing infected computers to rogue DNS servers** operated by the attackers.

Operation Ghost Click – Exploits

Exploits

- Malware known as DNSChanger replaced legitimate advertisements on victims' web browsers with ads that rewarded the hackers and hijacked referral commissions from other advertisers.
- The malware also prevented infected systems from downloading software updates and visiting many security web sites to scan for and remove the malware.

Operation Ghost Click – Impacts

Impacts

- The hackers generated upwards of $14 million in illegitimate income through click hijacking and advertisement replacement fraud.
- Even two months after the Internet hijacking scheme was shut down, the malware was still running on computers at nearly half of Fortune 500 companies and federal government agencies.

Operation Ghost Click – Identification

How was the attack Identified?

- Threat researchers investigated and catalogued the malicious DNS servers.

Operation Ghost Click – Mitigation

How was this Mitigated?

- United States authorities froze the hackers' financial accounts, seized computers at numerous locations, and disabled their network of U.S. based computers, including rogue DNS servers located in New York and Chicago.
- The hackers' rogue DNS servers were replaced with legitimate ones so that the victims would still be able to access websites.

Operation Ghost Click – Recovery

How did victims Recover?

- Individuals who believed that they were victims of the DNSChanger malware could check their DNS at the below site:

  https://forms.fbi.gov/check-to-see-if-your-computer-is-using-rogue-DNS

- Potential victims could find additional information regarding how to check DNS settings, along with other technical details about DNSChanger at:

  https://www.fbi.gov/file-repository/dns-changer-malware.pdf/view

Brazilian Bank Hijacked – Overview

Scenario Overview

In October 2016, hackers targeted a major Brazilian financial company with hundreds of branches, operations in the U.S. and Cayman Islands, 5 million customers, and more than $27 billion in assets with a DNS redirect attack.

Attack Vector

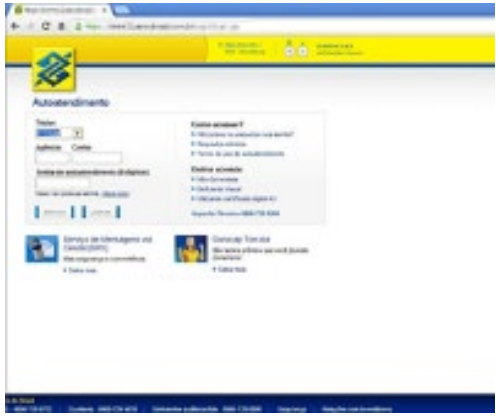
- Security researchers believe that the hackers compromised the bank's account with their domain registration service through a vulnerability in its website that could allow for changes to clients' settings.
- The Brazilian DNS service has attributed the attack to social engineering.

https://www.wired.com

Brazilian Bank Hijacked – Exploits

Exploits

- After the hackers compromised the bank's domain registration service account, they redirected the bank's website to lookalike sites with valid SSL certificates.



Brazilian Bank Hijacked – Impacts

Impacts

- For approximately five hours, bank users were redirected to lookalike sites that also infected the victims with a malware download disguised as a browser security plug-in that the Brazilian bank offered customers.
- According to researcher analysis, the malware could harvest bank login credentials, email credentials, and contact lists from Outlook and Exchange.
- The bank has not publicly disclosed how many customers were affected.

Brazilian Bank Hijacked – Response

From an incident response standpoint…

How was this attack identified?

The burst of malware set off alarms for security vendors and was eventually traced back to the bank.

How was the attack mitigated?

- Since the bank was also unable to access its email systems, they were **unable to alert customers**.
- The bank coordinated with the DNS service to correct the DNS registration for its domains.

How did the bank recover?

Though the bank regained control of its DNS infrastructure, the **malware could remain on the victims' machines and cause persistent damage.**

Key Takeaways

IDENTIFY

- Websites begin loading much slower than usual
- Browser shows incorrect website information
- Irrelevant and unwelcome pop-up ads

MITIGATE

- Review DNS Records
- Change DNS Account Passwords
- Add Multi-Factor Authentication to DNS Accounts
- Monitor Certificate Transparency Logs

RECOVER

- Verify security vendor service-level agreement (SLA)
- Review
- DNS records and public domain records
- Identify weak spots and exploits used
- Work with vendors or network administrator(s) to reestablish border gateway protocol (BGP) connections
- Check and restart firewalls and other apps
- Get unblocked by your ISP
- Begin application recovery

Resources

Emergency Directive 19-01: Mitigate DNS Infrastructure Tampering

https://www.cisa.gov/emergency-directive-19-01

Binding Operation Directive 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems

https://www.cisa.gov/binding-operational-directive-19-02

Informational Memorandum: Addressing Domain Name System Resolution on Federal Networks

https://www.cisa.gov/sites/default/files/publications/Addressing_DNS_Resolution_on_Federal_Networks_Memo.pdf

CISA Insights: Mitigate DNS Infrastructure Tampering

https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-MitigateDNSInfrastructureTampering_S508C.pdf

Additional Resources

CISA Website

https://www.cisa.gov

IR Training Website

https://www.cisa.gov/resources-tools/programs/Incident-Response-Training

CISA GitHub

https://github.com/cisagov

CISA YouTube Channel

https://www.youtube.com/channel/UCxyq9roe-npgzrVwbpoAy0A

FedVTE

https://fedvte.usalearning.gov

CISA Commenting Policy

https://www.cisa.gov/cisa-moderation-comment-policy

Additional Reading

Greenberg, Andy. “How an Unprecedented Heist Hijacked a Bank’s Entire Online Operation”. April 2017, wired.com

https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA