GRACE HOPPER CELEBRATION

ANITA B.ORG

Anatomy of a Cyber Attack

#GHC19

Overview

What is a Cyber Attack?

“Any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to a computer system, network, or technology dependent asset.”

Who are the people behind cyber attacks?

Nation States

These are individuals that are well funded spies that can provide political, economic, or military advantage to a home country.

Organized Criminals

These are individuals that try to steal money or data from companies often by exploiting vulnerabilities within their network infrastructure or people.

Criminals

These are individuals that are unskilled, typically use attacks like ransomware, digital fraud or theft.

Hacktivists

Motivated by ideology, attacks groups such as governments or large organizations like the Church of Scientology.

Insider Threats

These are individuals that are unskilled, typically within your organization.

Source: [1] McAfee Labs “Threats Report” March 2018 [2] Verizon 2018 Data Breach Investigations Report, April 2018 [3] Symantec Internet Security Threat Report, Volume 23, March 2018

Where to these attacks come from?

43%

Of attacks target small businesses

91%

Of attacks are launched with phishing emails

38%

Of attacks come from malicious file extensions

54%

Of malware attacks target mobile devices

95%

Data breaches are caused by human error

Source: [1] McAfee Labs “Threats Report” March 2018 [2] Verizon 2018 Data Breach Investigations Report, April 2018 [3] Symantec Internet Security Threat Report, Volume 23, March 2018

Who is at Risk?

Individuals + Businesses + Governments = Everyone

Anatomy of a Cyber Attack:
7 Stages

7 Stages of a Cyber Attack

1. Reconnaissance
2. Weaponize
3. Deliver
4. Exploit
5. Control
6. Execute
7. Maintain

Stage 1: Reconnaissance

Hackers need to identify targets, find weaknesses, and find a way into the networks

It only takes one person to create a hole in the network!

Attack

- Open source reconnaissance
- Social Media
- NMAP, Nikto, Unicornscan

Detection

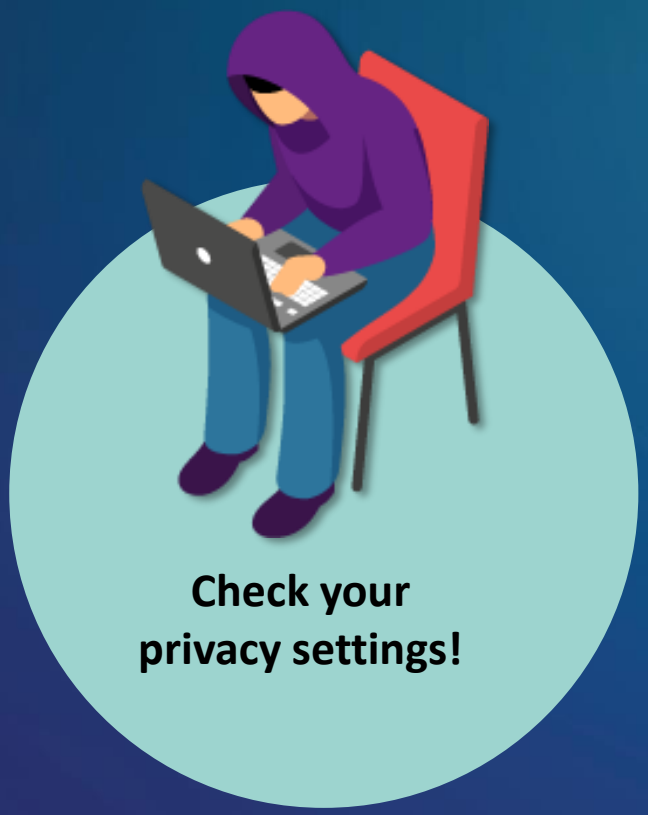
- Logging
- Monitoring
- Response

Defense

- Border Defenses
- Optimized Public Systems
- Robust Patching and Vigilance

Stage 2: Weaponize

At this stage hackers customize their code or attacks to whatever will get you to click



Attack

- Download / Freeware
- Purchase
- Develop

Detection

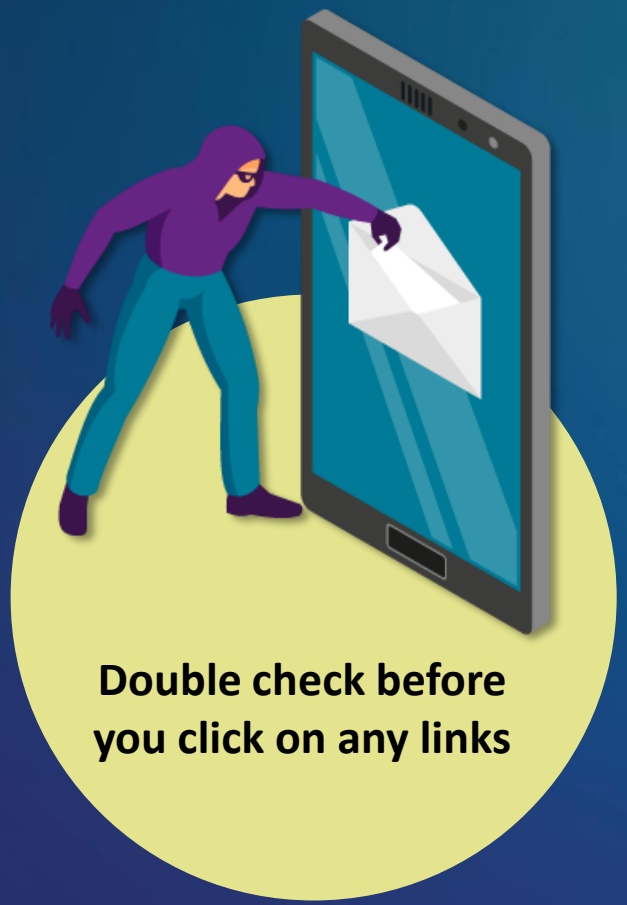
- This is really hard
- Generally not achievable

Defense

- Reduced Social Media footprint
- Controlled IT Documentation
- Robust Security Program
- Employee Awareness

Stage 3: Delivery

The hacker delivers the attack via email, website, software, etc., and waits to gain access



Double check before you click on any links

Attack

- Spear Phishing
- Publicly exposed system/application
- Watering hole
- USB Baiting

Detection

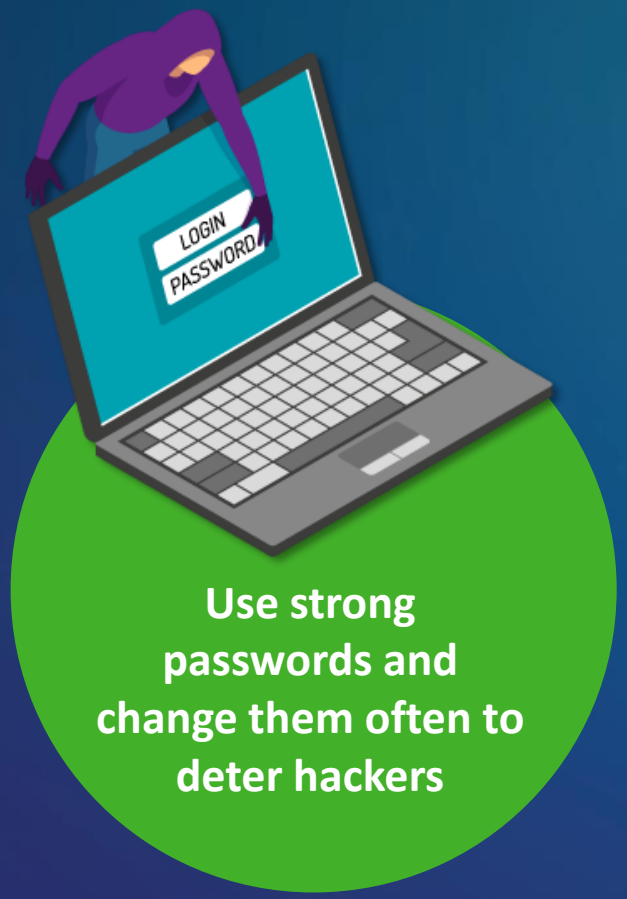
- SPAM filters or Email protections
- IPS
- User Vigilance

Defense

- Security Systems
- Threat Intelligence
- YOU

Stage 4: Exploitation

Now the hacker starts to get information back from the attack to gain access to systems



Use strong passwords and change them often to deter hackers

Attack

- Malware
- Ransomware
- SQLi
- Adware/Spyware

Detection

- Perimeter Defensive Systems
- Host Based Security
- User Awareness

Defense

- Patching
- Up-to-Date AV Signatures
- Secure Configurations
- User Awareness

Stage 5: Control

Once the hacker is in your network, they take steps to make sure they stay there

MFA is one way to maintain a strong perimeter

Attack

- Backdoors/RDP/SSH
- Web, DNS or Mail
- Covert Channels

Detection

- Perimeter Defensive Systems
- Host Based Security
- Log Analysis
- Passive Traffic Analysis

Defense

- Host Based Security
- Malware Analysis
- Threat Intelligence

Stage 6: Execute

Hackers crack the safe and have access to anything on the network

Network segmentation can mean hackers only see part of your data

Attack

- Exfiltration of Data
- Data Modification/Destruction
- Pivot to Another Objective

Detection

- DLP
- Security Systems
- Insider Threat Programs

Defense

- DLP
- Secure Configurations
- User Awareness

Stage 7: Maintain

Hackers do their damage, whether it is stealing money, PII, or crashing systems

Ultimately it is up to us to follow security protocols and try to keep hackers out

Attack

- Establish Persistence
- Lateral Movement
- Credential Harvesting
- Malware Variation

Detection

- Host Based Security
- Passive Traffic Analysis
- Threat Intelligence

Defense

- Segmentation
- Identity Management Program
- Robust Logging
- Threat Intelligence

Key Takeaways

- We are constantly under attack
- If we use precaution, we can protect ourselves
- Patch your systems and network devices
- Do not click any links or emails if you suspect a message may be phishing
- Never leave your devices unattended
- Use strong passwords, and change them often
- Do not give personal information over the phone
- Never Open Attachments from sources your are unsure of

Questions?

Come by Booth #T1836