KILL CHAIN

The 7 Stages of a Cyberattack

By Claudius Thompson
IT Security Consultant (LCCPMA)

Disclaimer

- This is strictly for educational purpose. Usage of any information for attacking targets without prior mutual consent is illegal. I assume no liability and is not responsible for any misuse or damage caused by this course.

WHO AM I?

- Tech Enthusiast
- Programmer
- Web Application Developer
- Network/System Engineer

Contact me

- Email: claudiecool@gmail.com
- Whatsapp: +231(0)778504679

Introduction

- In today's world, reality is, cyberattacks are a daily occurrence and every organization must focus on critical infrastructure surrounding cybersecurity. Businesses have begun to think like the military. How can we defend our enterprise? To that end, it's not surprising that companies have adopted soldierly, combative mindsets and terminology.

What is a Kill Chain

- Term originates from the US Army. Refers to structure – or seven stages – of a cyberattack.
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command & Control
  - Action on Objectives

Thinking like a hacker

Step one - Reconnaissance

The whole point of this phase is getting to know the target.
The questions that hackers are answering at this stage are:

- Identify a vulnerable target.
  - Who are the important people in the company?
    - Check info on website, social media sites (LinkedIn, etc.)
  - Who do they do business with?
    - Use social engineering
    - Dumpster diving
  - What public data is available?
    - IP Address (Scan to determine hardware and software
    - Web registry database (ICAAN)

Step two - Weaponization

In this phase, the hacker uses the information that they gathered in the previous phase to create the things they will need to get into the network

- Spear Phishing e-mails
  - E-mails that they could potentially receive from a known vendor or other business contact
- Watering Holes
  - Fake web pages. These web pages will look identical to a vendor's web page or even a bank's web page.

Step three - Delivery

Now the attack starts

- Phishing e-mails are sent
  - Contains a weaponized attachment
  - Malicious link
- Watering Hole web pages
  - Posted to the Internet and the attacker waits for all the data they need

Step four - Exploitation

Now the ‘fun’ begins for the hacker

- User names and passwords arrive
  - hacker tries them against web-based e-mail systems or VPN connections to the company network
- Malware-laced attachments
  - Attacker remotely accesses the infected computers

Step five - Installation

- Persistent backdoor
- Create Admin accounts on the network
- Disable firewall rules
- Activate remote desktop access on servers and other systems on the network

The intent at this point is to make sure that the attacker can stay in the system as long as they need to

Step six- Command and control

- Can look at anything
- Impersonate any user on the network
- Send e-mails from the CEO to all employees

Now they have access to the network, administrator accounts, all the needed tools are in place

Step seven – Action on objective

- Stealing information on employees, customers, product designs, etc
- Start messing with the operations of the company

Now that they have total control, they can achieve their objectives

Prepare for the attack

- So, what now?
- What can you do to protect your network, your company, even your reputation?

Sooner or later the hackers WILL come for you. Don’t let yourself think that you don’t have anything that they want. Trust me, you do

Conclusion

- Today, all businesses should spend time walking through these stages, identify vulnerabilities, and shoring up their defenses to eliminate them. It’s not an easy task, but the more critically each of us look at these seven stages of the kill chain, the better we can prevent the next hack

Thank You

Questions?