BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Stages of a Cyber Attack

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Threat Landscape and Common Cyber Attacks

innovate achieve lead

Agenda

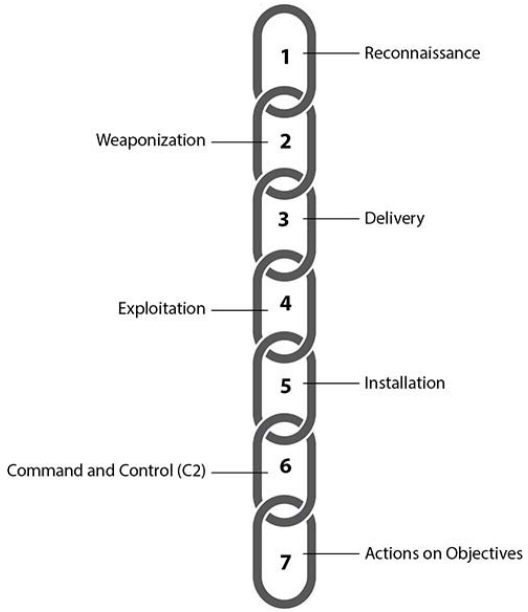
- The Threat Landscape
- Understanding Vulnerabilities
- Common Cyber Attacks
  - Stages and Patterns
  - Targeted and Non-targeted Attacks
  - Reducing exposure to Cyber Attacks
- Essential Cyber Security Controls
  - Boundary firewalls and Internet gateways
  - Secure configuration
  - Whitelisting and execution control
  - User access control
  - Password policy
  - Content checking

Stages of a Cyber Attack

Stages of a Cyber Attack

Kill Chain in Cyber Security

- Defines the steps used by adversaries in conducting their attacks
- According to this model, cyber attacks may occur in phases and can be disrupted through controls established at each phase
- The idea is that by breaking down an attack process into stages, defenders can pinpoint where along the lifecycle of an attack an activity is and deploy appropriate countermeasures
- In 2011, computer scientists at Lockheed-Martin adapted this concept and described a new "intrusion kill chain" model to defend computer networks
- The kill chain can also be used as a management tool to help continuously improve network defense



Source: https://en.wikipedia.org/wiki/Kill_chain

Stages of a Cyber Attack

Step 1: Reconnaissance

- In this stage, attackers gain understanding about the topology of the network and key individuals with system or specific data access.
- Reconnaissance actions (referred to as recon) can be passive or active in nature
  - Passive Recon
    - To acquire information about a target network or individual without direct interaction
    - For example
      - The attacker may monitor for new domain registration information about a target company to get technical points of contact information
      - E.g., Dumpster diving
  - Active Recon
    - Involves more direct methods of interacting with the organization to get a lay of the land
    - For example
      - The attacker may scan and probe a network to determine technologies used, open ports, and other technical details about the organization's infrastructure
      - The downside (for the actor) is that this type of activity may trigger detection rules designed to alert defenders on probing behaviors

Stages of a Cyber Attack

innovate achieve lead

Step 1: Reconnaissance

- The questions that hackers are answering at this stage are:
  - Who are the important people in the company?
    - This can be answered by looking at the company web site or LinkedIn.
  - Who do they do business with?
    - For this they may be able to use social engineering, by making a few "sales calls" to the company.
    - The other way is good old-fashioned dumpster diving
  - What public data is available about the company?
    - Hackers collect IP address information and run scans to determine what hardware and software they are using
    - They check the ICANN web registry database
      - The Internet Corporation for Assigned Names and Numbers (ICANN) is an American multi-stakeholder group and nonprofit organization responsible for coordinating the maintenance of IP numbers and Domain Name System root

Source: https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270

Stages of a Cyber Attack

innovate achieve lead

Step 1: Reconnaissance

- What do hackers look for?
  - Email addresses
  - Phone numbers to carry out Vishing
    - Voice Phishing
  - Passwords and other information that we might have written on sticky notes for our convenience
  - Bank statements/financial statements
  - Medical records

- What do hackers look for?
  - Account login credentials
  - Business secrets
  - Marketing secrets
  - Information of the employee base
  - Information about the software/tools/technologies that is being used at the company

Stages of a Cyber Attack

Step 2: Weaponization

- The hacker uses the information gathered in the previous phase to create things they need to get into the network
- This involves creating:
  - documents with naming schemes similar to those used by the company
    - These may be used in a social engineering effort at a later point
  - specific malware to affect a device identified during the recon
  - believable Spear Phishing e-mails
    - Sending emails to specific and well-researched targets while purporting to be a trusted sender
  - Watering Holes
    - A watering hole attack is a targeted attack designed to compromise users within a specific industry or group of users by infecting websites they typically visit and luring them to a malicious site
  - Fake Web Pages
    - These web pages will look identical to a vendor's web page or even a bank's web page

Source: https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270

Stages of a Cyber Attack

Step 3: Delivery

- This is the point at which the adversary goes fully offensive and transmits the attack
- For example:
  - Phishing and Spar Phishing e-mails are sent
  - Short Message Service (SMS)
  - Watering Hole web pages are deployed on the Internet
  - Social Engineering Schemes
  - Delivering a tainted USB drive
  - Convincing a target to switch to an attacker-controlled infrastructure
    - in the case of a rogue access point or physical man-in-the-middle attack

Stages of a Cyber Attack

innovate achieve lead

Step 4: Exploitation

- The Exploitation phase includes the actual execution of the exploit against a flaw in the system
- Now the 'fun' begins for the hacker
- As user names and passwords arrive, the hacker tries them against
  - web-based e-mail systems or
  - VPN connections to the company network
- If malware-laced attachments were sent, then the attacker remotely accesses the infected computers
- The attacker explores the network to gain a better idea of
  - the traffic flow on the network
  - what systems are connected to the network and
  - how they can be exploited

Source: https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270

Stages of a Cyber Attack

innovate achieve lead

Step 4: Exploitation

- This is the point where
  - the adversary triggers the exploit against a server vulnerability, or when the user clicks a malicious link or executes a tainted attachment
- Here, an attack can take one of two courses of action:
  - the attacker can install a dropper to enable him to execute commands, or
  - he can install a downloader to enable additional software to be installed at a later point
- The key objective here is often to get as much access as possible to begin establishing some permanence on the system
- Knowing what assets are present on the network and patching any identified vulnerabilities improves resiliency against such attacks
- This, combined with more advanced methods of determining previously unseen exploits, puts defenders in a better position to prevent escalation of the attack

Stages of a Cyber Attack

Step 5: Installation

- Here, the adversary aims to achieve persistence, or extended access to the target system for future activities
- The attacker has taken a lot of steps to get to this point, and would likely want to avoid going through them every time he wants access to the target
- At this point, the threat actor attempts to:
  - install a persistent backdoor
  - create Admin accounts on the network
  - disable firewall rules
  - perhaps even activate remote desktop access on servers and other systems on the network
- Endpoint detection is frequently effective against activities in the stage
- Security analysts may sometimes need to use more advanced logging interpretation techniques to identify clever or obfuscated installation techniques

Source: https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270

Stages of a Cyber Attack

innovate achieve lead

Step 6: Command & Control (C2)

- In this phase, the attacker creates a channel in order to facilitate continued access to internal systems remotely
- C2 is often accomplished through periodic beaconing via a previously identified path outside of the network
  - Beacon - A signaling or guiding device that emits light, such as a lighthouse, or repeating sound, like a beep
- At this stage, the attackers
  - are in complete control
  - have access to the network, administrator accounts, all the needed tools are in place
  - have unfettered access to the entire network
  - can look at anything, impersonate any user on the network, and even send e-mails from the CEO to all employees
  - can lock you out of your entire network if they want to

Source: https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270

Stages of a Cyber Attack

innovate achieve lead

Step 6: Command & Control

- Defenders can monitor for this kind of communication to detect potential C2 activity
- Problem is that many legitimate software packages perform similar activity for licensing and update functionality
- The most common malicious C2 channels are over the Web, Domain Name System (DNS), and e-mail, sometimes with falsified headers
- For encrypted communications, beacons tend to use self-signed certificates or custom encryption to avoid traffic inspection
- When the network is monitored correctly, it can reveal all kinds of beaconing activity to defenders hunting for this behavior
- To complicate things more, beaconing can occur at any time or frequency, from a few times a minute to once or twice weekly

Stages of a Cyber Attack

innovate achieve lead

Step 7: Action on objective

- Now that the hackers have total control, they can achieve their objectives. Example:
  - Exfiltrate sensitive intellectual property
  - Encrypt critical files for extortion
  - Sabotage via data destruction or modification
  - Stealing information on employees, customers, product designs, etc.,
  - Start messing with the operations of the company
- Not all hackers want to steal the money, sell information or post incriminating e-mails on WikiLeaks
- Some hackers just want to mess things up and cause pain. For example:
  - In online retailing
    - The attacker could shut down the order-taking system or delete orders from the system
    - They could even create orders and have them shipped to the organization's customers
  - Industrial Control System
    - They could shut down equipment, enter new set points, and disable alarms

Source: https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270

Stages of a Cyber Attack

innovate achieve lead

Step 7: Action on objective

- Defenders can use several tools at this stage to prevent or at least detect these actions
- Data loss prevention software, for example, can be useful in preventing data exfiltration
- In any case, it's critical that defenders have a reliable backup solution that they can restore from in the worst-case scenario
- Much like the Reconnaissance stage, detecting activity during this phase can give insight into attack motivations, albeit much later than is desirable

Stages of a Cyber Attack

Summary

- Cyber Kill Chain can enable organizations to build defense-in-depth strategies that target specific parts of the kill chain
- However, it may fail to capture attacks that aren't dependent on all of the phases to achieve end goals
- For example:
  - In modern phishing attacks, attackers rely on victims to execute an attached script
- Additionally, the kill chain is very malware-focused and doesn't capture the full scope of other common threat vectors such as:
  - insider threats, social engineering, or any intrusion in which malware wasn't the primary vehicle for access

States of a Cyber Attack

innovate achieve lead

Summary

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Action on Objectives
Identify the target and its weaknesses	Create/select attack vectors to penetrate the target	Deliver the malicious payload	The malware begins executing on the target system	The malware installs a backdoor or other ingress accessible to the attacker	The intruder gains persistent access to the victim's systems/network	Intruder initiates end goal actions, such as data theft, data corruption, or data destruction
Research, Identification and selection of targets Often represented as crawling the Internet websites and mailing lists for email addresses, social relationships, or information on specific technologies	Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer) Increasingly, client applications data files such as Adobe PDF or Microsoft Documents serve as weaponized deliverable	Transmission of the weapon to the targeted environment using vectors like email attachments, websites, and USB removal media.	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability	Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel	Only now, after progressing through the first six stages, can intruders take actions to achieve their original objective. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim's environment.

Source: https://countuponsecurity.com/2014/08/29/intelligence-driven-incident-response/

Stages of a Cyber Attack

References

- Common Attack Pattern Enumeration and Classification
  - CAPEC is a tool that security professionals can use to understand attacks
  - CAPEC Web site hosted by MITRE
  - This online repository can be searched for characteristics of a particular attack or simply browsed for additional knowledge of how attacks occur procedurally
  - http://capec.mitre.org
- Other References
  - https://www.ibm.com/services/business-continuity/cyber-attack
  - https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270
  - https://tax.thomsonreuters.com/blog/kill-chain-the-7-stages-of-a-cyberattack/
  - CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002), 2nd Edition by Brent Chapman; Fernando Maymi

Targeted and Untargeted Attacks

Targeted and Untargeted Attacks

Untargeted Attack

- What is the intent?
- Who is the target?
- What form does the attack takes?
- How are the attack vectors sent out?
- Expertise level of the attackers
- Resources available to the attackers to conduct their schemes
- Time period of the attack

Targeted Attack

- What is the intent?
- Who is the target?
- What form does the attack takes?
- How are the attack vectors sent out?
- Expertise level of the attackers
- Resources available to the attackers to conduct their schemes
- Time period of the attack

Targeted and Untargeted Attacks

innovate achieve lead

Untargeted Attacks

- According to a CNN report,
  - In 2014, more than 317 million new items of malware were created and distributed
  - It only takes 82 seconds for someone to get tricked into opening an email that contains an untargeted attack
- Although this seem daunting, these types of attacks are very easy to avoid
- For example:
  - Don't click on random ads that pop up on your computer
  - Don't open any unfamiliar emails where the source seems questionable
  - Don't download something unless you're sure it's from a secure source
- The Internet can be tricky, and it can create a lot of vulnerability, but there are many options out there that help keep your data safe.

Source: https://www.anomali.com/blog/targeted-attack-vs-untargeted-attack-knowing-the-difference

Targeted and Untargeted Attacks

Targeted Attacks

- In 2015, 5 out of 6 large companies fell targets to cybercriminals
- The prime goal is to gather vital information about the company so that they can sell it on the black market
- This causes massive amounts of damage to the company while its competitors profit
- The main way to prevent this type of threat is by ensuring an up-to-date cybersecurity system that works for the business
- This type of attack isn't specific to big businesses
  - It's all about how juicy the data is and how poorly it is protected

Source: https://www.anomali.com/blog/targeted-attack-vs-untargeted-attack-knowing-the-difference

Reducing Exposure to Cyber Attacks

Reducing Exposure to Cyber Attacks

innovate achieve lead

Top Security Tools to Use Across the Cyber Kill Chain

- Reconnaissance
  - To handle threats in this phase, you might consider
    - threat intelligence feeds
    - perimeter controls
    - identity and access management
    - system hardening
    - honeypot
  - The goal here is to put in place prevention and detection processes and technology to prevent a threat actor from obtaining too much information

Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

Reducing Exposure to Cyber Attacks

innovate achieve lead

Top Security Tools to Use Across the Cyber Kill Chain

- Weaponization
  - At this stage, your organization should be leveraging
    - vulnerability scanners
    - patch management systems, and
    - Intrusion Detection Systems
  - Your security team may want to leverage the Dark Net to study the latest malware and become familiar with what's out there on the black market
  - The team may even be able to reverse engineer malware to combat a hacker's attack.

Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

Reducing Exposure to Cyber Attacks

innovate achieve lead

Top Security Tools to Use Across the Cyber Kill Chain

- Delivery
  - The goal in this phase is to detect and respond as quickly as possible to an active threat
  - Potential security controls during the delivery phase include
    - next-gen firewalls
    - next-gen Intrusion Prevention System (IPS)
    - email and web gateway security
    - DDoS mitigation tools
    - network behavior analysis
    - user and entity behavior analytics (UEBA)
    - DNS security
    - NetFlow
    - packet analysis, and
    - security awareness

Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

Reducing Exposure to Cyber Attacks

innovate achieve lead

Top Security Tools to Use Across the Cyber Kill Chain

- Exploitation
  - To put a stop to a threat actor in this phase, you can leverage:
    - Security information and event management (SIEM)
    - log management
    - firewalls
    - Endpoint Protection Platforms (EPP)
    - web application firewalls (WAF)
    - advanced threat detection technology
    - user and entity behavior analytics, and
    - threat intelligence
  - All of these technologies will aid in detection and prevention when a threat actor has entered into your network
  - These tools will also allow your incident responders to address a security breach quickly

Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

Reducing Exposure to Cyber Attacks

innovate achieve lead

Top Security Tools to Use Across the Cyber Kill Chain

- Installation
  - The helpful tools and technologies in this phase include
    - Endpoint Protection Platforms (EPP) solutions
    - Managed Detection and Response
    - Identity and Access Management (IAM) tools
    - incident response workflows
    - backups, and
    - incident reporting

Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

Reducing Exposure to Cyber Attacks

innovate achieve lead

Top Security Tools to Use Across the Cyber Kill Chain

- Command and Control
  - Your incident responders should be equipped with
    - Security information and event management (SIEM)
    - log management
    - application security
    - Network Behavior Analysis (NBA) tools
    - reputation filtering
    - network monitoring,
    - etc

Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

Reducing Exposure to Cyber Attacks

innovate achieve lead

Top Security Tools to Use Across the Cyber Kill Chain

- Action on Objective
  - The technologies and tools that can help put a stop to data leaving the organization may include
    - Data Loss Prevention (DLP)
    - Security information and event management (SIEM)
    - User and Entity Behavior Analytics (UEBA)
    - Identity and Access Management (IAM)
    - Next Generation Firewalls (NGFW)
    - backup and restore capabilities.
  - Across each phase, your organization has an opportunity to put a stop to a threat actor
  - Strategies, tools, and technologies can aid significantly in protecting your organization and preventing it from becoming a victim of a significant data breach.

Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!