CASE STUDY ON CYBER ATTACK INCIDENTS AND AN ATTACK MODEL

Contents

- Major cyber attack incidents
- APT attack
- Attack model- cyber kill chain
- conclusion

Maroochy water breach(2000)

- Hacked into a water control system and flooded the grounds of a hotel and a nearby area with sewage in Maroochy Shire, Australia
  - attacker: employee fire by Hunter Watertech Co.
  - Attack origin : outside the system
  - Attack operation
    - Hacking via a wireless link
    - Installing malicious programs at the pump control computer
    - Causing malfunction of pumping equipments, and blocking reports to the central system
    - Hacking 46 times, flooding about a million liters sewage

Davis-Besse nuclear power plant (2003)

- The SQL slammer worm infected the Davis Besse nuclear power plant in Ohio, US.
- The worm infected the contractor’s network, and breaked in the cooperate network. The line between the cooperate network and contractor’s network was interconnected without any firewall.
- Infected the system within 30min.
- Undetected the attack for 6 hrs.
- Typical backdoor attack which could intrude the network without being monitored by operators

US northwest blackout(2003)

- Cascading outage in the northwest of the US.
- Guessing its cause would be the blaster worm
- The blaster worm degraded the performance of communication lines of a core data center to manage power system network.
- Because critical control data could not delivered in time, operators couldn’t control the cascade effect of outage, causing wide area outage.
- The Blaster worm infected a host using Window RPC DCOM, and the infected host made SYN flooding attack using a disguised source address.– DOS attack

US Georgia Hatch nuclear plant (2008)

- An engineer at the Southern Company did SW update on the computers to operate the intranet of the power plant.
- After update, the plant operation stopped for 48 hrs.
- The computer to be updated had been used to monitor the diagnostic data on the plant control system.
- When the updated computer rebooted, data of the control system was reset. Presumed that the reset caused misinterpretation of the control system data, and eventually forced to stop the operation.
- So, unintentional error caused the malfunction.

Stuxnet (2010년)

- The Stuxnet can be said to be a watershed incident of cyber attack history.
- The attack took place at the uranium enrichment facility at Natanz, Iran.
- The attack targeted the Siemens PLC software to control the speed of centrifuge rotors, more specifically Siemens PLC(6ES7-315-2 and6ES7-417).
- How could the worm infiltrate into the air-gapped SCADA network?
- How could the worm spread all over the system?
- The technical details will be explained in other slides.

Ukrainian Power Grid Attack (2015)

- A regional electricity distribution company reported service outages which were due to a third party’s illegal entry into the company’s computer and SCADA systems.
- 7 100KV and 2335KV substations were disconnected for 3 hrs, causing 225,000 customers to lose power.
- Attack operation
  - Preliminary infection of networks with the help of conterfeit emails using social engineering methods
  - Using remote access to the administrative computers of the ASDU inside the corporate networks or directly to the ASDU servers using the ADS client software, and performed the execution of shutdown operations at the substations.
  - Destruction of information on servers and workstations (KillDisk utility)

Advanced Persistent Threat(APT)

- A new class of threats
- What is different from legacy attacks?
  - a specific target
  - Advanced methods: unknown methods or zero-day vulnerability
  - in a stealthy way, disguise themselves and morph for defenders to identify them.
  - Persistently pursue the goals repeatedly over an extended period of time.

Kill Chain

- In US military term, it is a multi-phased model to describe the stages of an attack.
  - Find: locate the target
  - Fix the locations, make it difficult for attackers to move
  - Track: monitor the movement
  - Target: select an appropriate weapon or asset to use the target
  - Engage: apply the weapon
  - Assess effects of the attack

Cyber kill chain as an attack model

- Lockheed-Martin co. applied the military kill chain concept to computer security in 2011.
- A multi-stage attack model
  - Like the military kill chain, it models an attack as stepwise activities, each of which has a specific goal.
  - It helps defenders to clarify the process of attacks
- A layered defense strategy
  - Defenders can apply appropriate defense actions to each stage of attacks.
  - At the earlier stage they detect an attack, the easier they defend, and the less impact of the attack.

Cyber Kill Chain

- Reconnaissance
  - Probe for a weakness.
  - gaining login credentials or information useful in a phishing attack
  - Social engineering
- Weaponization
  - Build a deliverable payload using an backdoor.
  - Spear-fishing, trojan in a file

- Delivery
  - Send a weapon to the victim
  - ex, a malicious link in a legitimate email
- Exploit
  - Execute code on the victim’s system
- Installation
  - Install malware on the target asset

- Command & Control
  - Create a channel where the attacker can control a system remotely
- Action
  - Remotely carries out intended goals.

Phases of the Intrusion Kill Chain

Reconnaissance

Research, identification, and selection of targets

Weaponization

Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

Delivery

Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

Exploitation

Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems

Installation

The weapon installs a backdoor on a target's system allowing persistent access

Command & Control

Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.

Actions on Objective

The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

A course of defense actions

- Detect
- Prevention
- Disrupt
  - – Make attacks less effective and take long time to carry out, so for the attack to become unprofitable.
- Degrade
  - – Weaken the power of attack, consequently its effectiveness.

- Deceive
  - Force attacker make wrong assumptions about the system, so select an ineffective attack vector

My incomplete matrix of attacks and defense actions

	detect	prevention	disrupt	degrade	deceive
Reconnaissance	Traffic analysis	Firewall ACL			
Weaponization	NIDS	NIPS			
delivery	NIDS(?)	Proxy filter	In-line Anti virus	queuing	
exploitation	HIDS	patch			
installation	HIDS		Anit virus		
Command And control	NIDS	Firewall ACL	NIPS		DNS redirect
Action on objective	Log analysis			Quality of service	Honeypot

conclusion

- The “air gap” is not safe to SCADA/ICS network, nor do the current defense methods guarantee security to critical networks.
- The cyber kill chain provides an attack model for the advanced attacks and the understanding of a possible layered defense architecture.
- But, as usual, attackers follow their own rules, not following the playbook. The question is how to adapt security strategies in order to confront inexorably evolving attacks.