Cyber Attacks

Josh Wilcox (jw14g24)

May 2, 2025

Table of Contents

1 Business Email Compromise Scams

2 Personal Document Ransom

3 Data Breaches

4 DDOS
- Case Study: Mirai

5 Influence Campaigns
- Web Defacements

6 Supply Chain Attacks

Business Email Compromise Scams

What is BEC

- Recent form of scam known as ”CEO fraud” or ”whaling”
- Requests large money transfers by pretending to be a CEO or Senior manager of the company
- Often involves grooming and back-and-forth between the attacker and the target
- Rely on the employee (target of the scam) being distant from the CEO and not understand theyre being scammed

Personal Document Ransom

Methodology

- Attacker sends email with subject reffering to an invoice or bill
  - Includes an attachment the user is lured to open
- The attachement is usually a PDF, office document, or script file
- When executed, the attachement could run a script which installed ransomware
- This ransomware encrypts some files which are only decrypted only by paying a random

Data Breaches

What is a data breach attack

- One of the most frequent cyber attacks
- Focuses on stealing **data** rather than money directly
  - Emails, Names, Passwords, Dates of Birth, Security Questions/Answers

What are the recent Trends?

- Threat Actors - Mostly **External**
- Motives - Mostly **Financial**
- Profiles - Mostly **Organised Crime**
- Attack Types - Mostly **Use of stolen credentials**

What happens to stolen data

- Public disclosure and exposure
  - Hacktivists - e.g. through WikiLeaks
  - Cybercriminals
- Private Intelligence
  - Done by nation states or conglomerates
- Sold on black market

DDOS

What is a Denial-of-Service Attack?

- Aims at making a service unavailable for intended users
- Disruption is usually done by overloading resource
- Commonly as a result of **flooding** of service requests
- If generated by many different sources - the attack is known as a **Distributed Denial of Service**

Botnets

- A botnet is a large group of computers that are networked together to use their combined power to cause DDoS attacks
- This recently has been done with **IoT** devices especially
  - Security is often not a priority
  - Set-and-Forget
  - Vulnerabilities are usually left unpatched

Case Study: Mirai

- Mirai is a DDoS system that scans for vulnerable IoT devices over the internet
- It uses a set of hardcoded, and common, usernames and passwords
  - Remember IoT is famously insecure for some reason
- It infects the IoT devices with a malware that forces them to report to a C&C server

Influence Campaigns

Methodologies of Influence Campaigns

- Cyber-Attacks and information release aimed to influence a large population's **choices** and **thinking**
- Use massive amounts of **bots** in social media platforms
  - Each is a small account automatically spreading specific ideas
  - As GenAI gets better, it is very hard to detect these

Web Defacements

- Changes the appearance of a website
- Mostly done by Hacktivists to show off

Supply Chain Attacks

Operation

- Compromisation of the weakest link in a supply chain
- Extorts the supply chain to eventually reach the target
- Example: Hacking github repositories of early software before release