# THE ANATOMY OF A MALWARE CAMPAIGN: FROM INFECTION TO EXFILTRATION


# WHO AM I?

This is Manivannan Arumugam from Tamil Nadu, India. I have been working as a Cyber Forensics Investigator for over 8 years and hold a Computer Hacking Forensics Investigator certification from EC-Council. I collaborate with the Tamil Nadu Government cyber cells to solve numerous cyber-related cases.

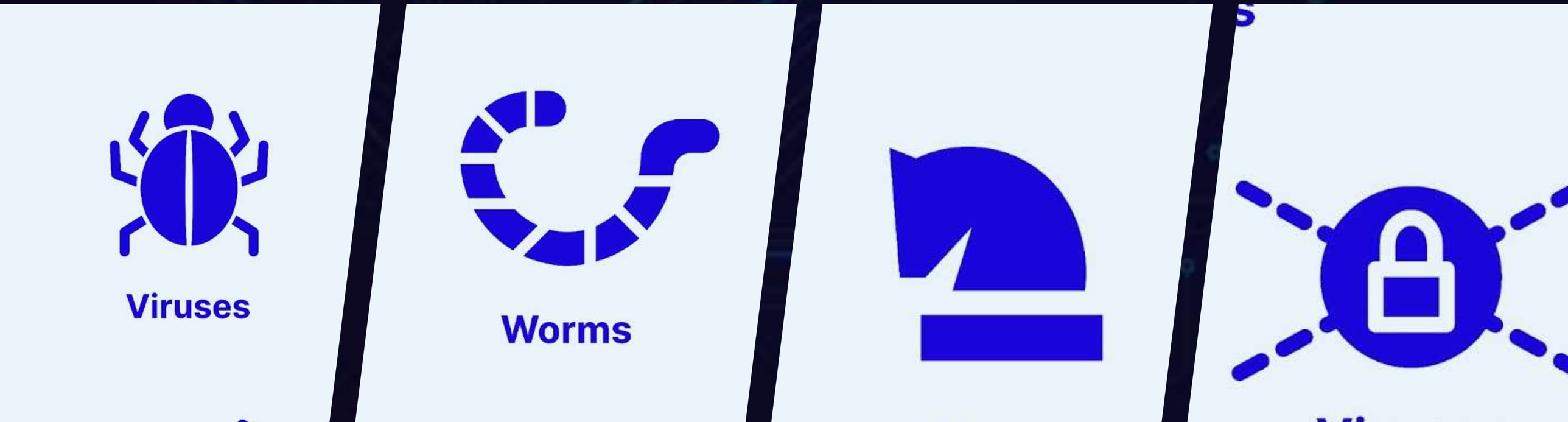
# AGENDA


1. UNDERSTANDING MALWARE
2. INITIAL INFECTION
3. PROPAGATION AND PERSISTENCE
4. PAYLOAD DELIVERY
5. COMMAND AND CONTROL (C2)
6. DATA EXFILTRATION
7. DEFENSE AND MITIGATION STRATEGIES

# UNDERSTANDING MALWARE

Malware, or malicious software, is any software intentionally designed to cause damage to a computer, server, client, or network. There are several types of malware:

Viruses, Worms, Trojans, Ransomware, Spy ware, Adware and Rootkit



# MOTIVATIONS BEHIND MALWARE

01 Financial Gain

02 Espionage

03 Sabotage

04 Political Motivations

# MALWARE CREATION

Attackers use programming languages like Python and C/C++ along with development kits such as Metasploit and Cobalt Strike to create their malware. These tools provide the necessary frameworks and exploits to craft sophisticated malware.

For example, the Mirai botnet used simple scripts written in Go language to compromise IoT devices, turning them into bots for a massive DDoS attack.

# INITIAL INFECTION

01 Phishing Emails

02 Malicious Downloads

03 Exploit Kits

04 USB Drives

05 Social Engineering

# INITIAL INFECTION

Case Studies

"Consider the WannaCry ransomware attack. It spread primarily through phishing emails containing malicious attachments. Once a user opened the attachment, the ransomware encrypted their files and demanded a ransom."

# PROPAGATION MECHANISMS

After initial infection, malware seeks to spread and persist.

**1) Network Worms**

Malware that spreads itself across networks by exploiting vulnerabilities. The Conficker worm infected millions of machines by exploiting a Windows vulnerability.

**2) File Infector Viruses**

Attaches itself to executable files and spreads when the file is executed. The CIH virus, also known as Chernobyl, is an example.

**3) Spear Phishing**

Targeted phishing attacks aimed at specific individuals or organizations. The 2013 Target breach started with a spear-phishing email to an HVAC contractor.

# PERSISTENCE TECHNIQUES

Malware uses various techniques to maintain persistence on a system.

**1) Registry Modifications**

Altering the system registry to ensure the malware runs on startup. For instance, the ZeuS Trojan modifies registry keys to achieve persistence.

**2) Scheduled Tasks**

Creating tasks that run the malware at specified times. APT29, linked to Russian intelligence, used scheduled tasks for persistence.

**3) Rootkits**

Concealing the malware's presence and maintaining control. The Sony BMG rootkit scandal involved software that hid on users' computers to prevent piracy.

# PAYLOAD DELIVERY

Once malware is on a system, it delivers its payload

**1) Data Theft**

Exfiltrating sensitive information such as login credentials or personal data. The Equifax breach involved malware that stole personal information of millions of people.

**2) Ransomware Encryption**

Encrypting files and demanding ransom for decryption. CryptoLocker is an early example of ransomware that encrypted user files.

**3) Botnets**

Compromising machines to be used for malicious purposes, like DDoS attacks. Mirai Botnet, which targeted IoT devices, is a notable example.

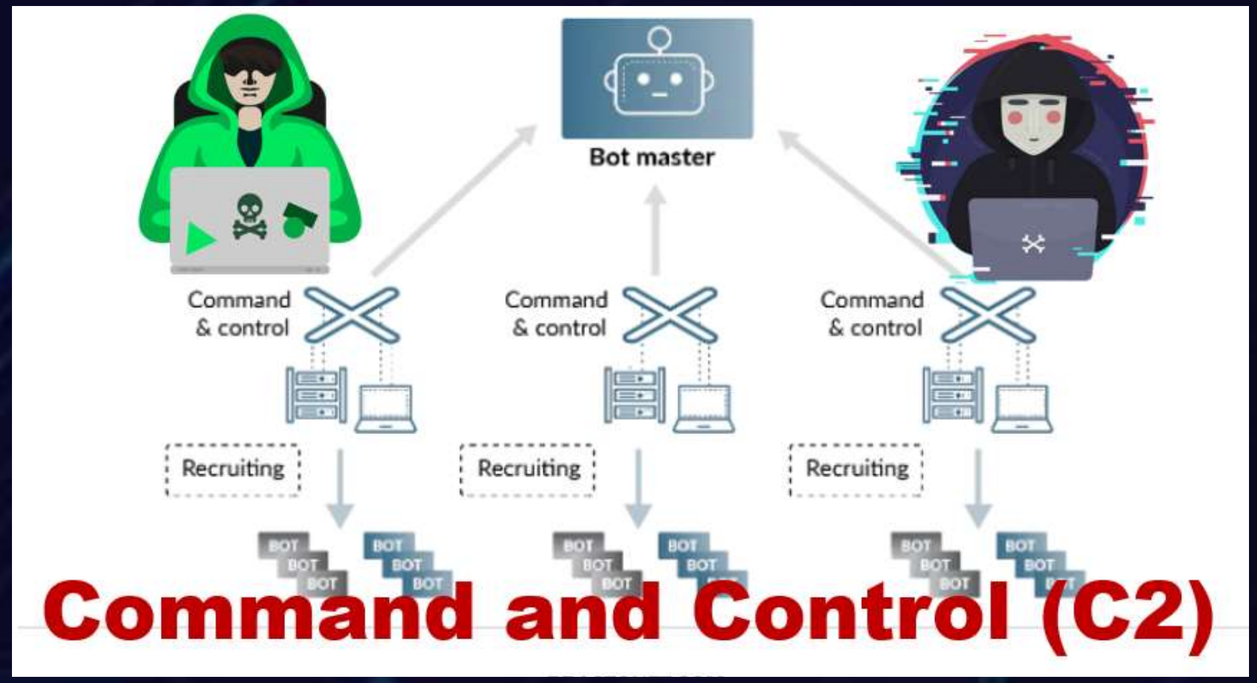
**4) Keyloggers**

Recording keystrokes to capture sensitive information. The SpyEye malware toolkit included keylogging capabilities.

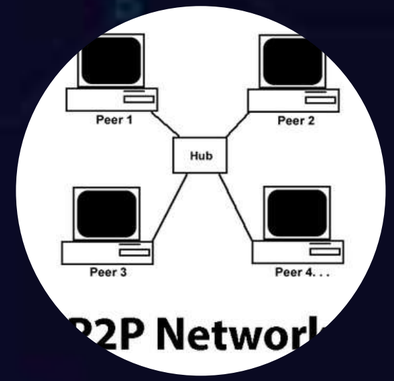
# COMMAND AND CONTROL

Malware needs to communicate with its operators. This is done through Command and Control (C2) infrastructure

1) Server
2) DNS
3) Fast Flux



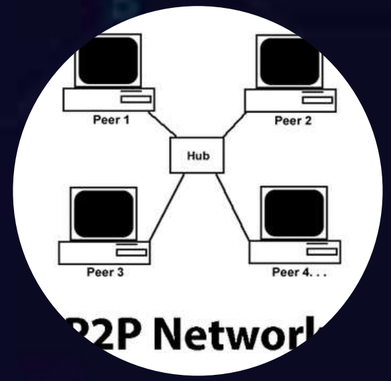
# COMMUNICATION METHODS


- **HTTP/HTTPS:** Using web traffic to communicate, making it harder to detect. The Dridex banking Trojan used HTTP for C2 communication.
- **IRC:** Internet Relay Chat used for C2 communication. The GTbot family used IRC to receive commands.
- **Peer-to-Peer:** Decentralized control without a central server. The GameOver Zeus botnet employed a peer-to-peer network.
- **Social Media:** Using platforms like Twitter or Facebook to send commands. The Stegano exploit kit hid malicious code in advertising banners.

# DATA EXFILTRATION

**Once data is stolen, it needs to be exfiltrated:**


- **Direct Download:**
  Transferring data directly from the victim to the attacker. The TJX data breach involved direct download of credit card information.

- **Email:**
  Sending stolen data via email. The Operation Aurora attack involved exfiltrating intellectual property via email.

- **DNS Tunneling:**
  Encoding data in DNS queries to bypass firewalls. The Feederbot malware used DNS tunneling for data exfiltration.

- **Cloud Services:** Uploading stolen data to cloud storage services. Attackers have used services like Dropbox and Google Drive for this purpose.

# THANK YOU