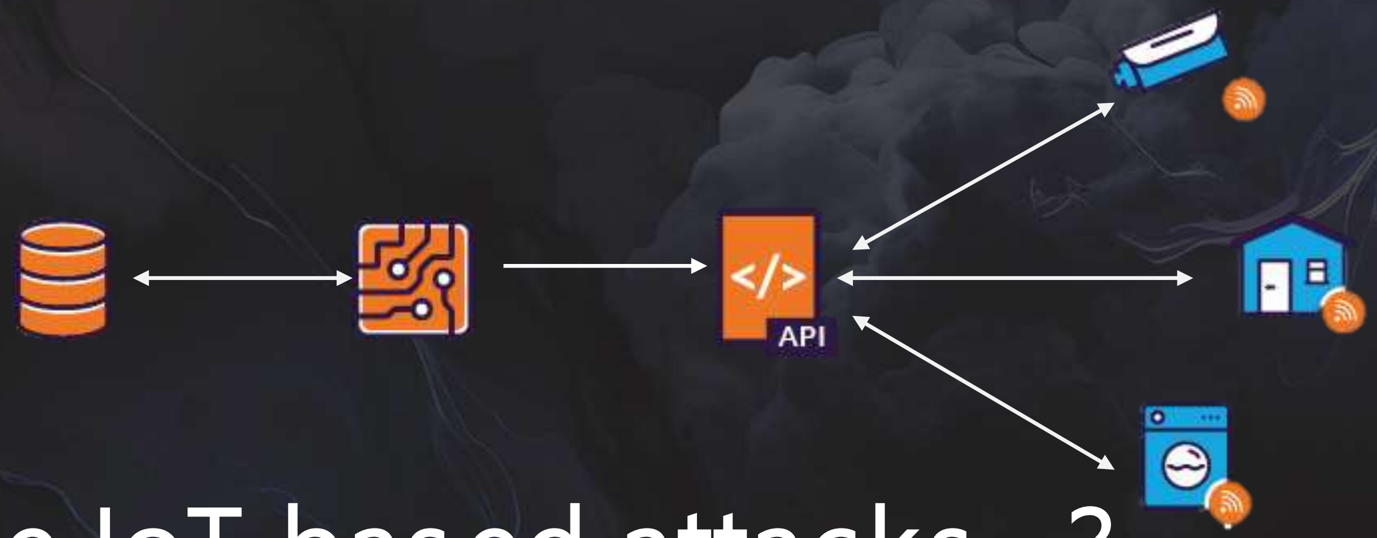
IOT-Based attack And IOT-Based testing

By :

- *Chaoui Manar*
- *Sahri Yousra*

What is IOT ?

the network of connected devices and the technology that facilitates communication, collecting and exchanging data between devices and the cloud, as well as between the devices themselves.. Like smart cars, smartcameras…



What are IoT based attacks ?

An IoT attack is a malicious attempt to exploit vulnerabilities in internet-connected devices, such as smart home devices, industrial control systems, and medical devices. Attackers may gain control of the device, steal sensitive data, or use the device as a part of a botnet for other malicious purposes.

IOT-based attacks

1 **DDoS Attacks (IoT-Based DDoS)**:

Distributed Denial of Service attacks targeting IoT devices or networks, overwhelming them with traffic and rendering them unresponsive.

2 **taking over-control attacks**

Attackers take control of IoT devices to use them for malicious purposes or to gain access to other systems.

3 **impersonation attacks**

Attackers impersonate IoT devices to trick users or access sensitive information.

4 **Detection attacks**

Attackers monitor and analyze data exchanged by IoT devices for confidential information.

IOT-based attacks

5 Man in the middle

the attacker intercepts the sender's messages, he can only read it (passive attacks) or modify it, delete it (active attacks).

6 Malwares attacks

The attacker attempts to install malware in your IoT device to gain unauthorized access to the Claud.

7 Ransomware

malware that encrypts your files and asks you to pay if you want to decrypt them.

8 Password cracking

Attacker tries to find the weak password of your IoT devices Using brute force attacks.

Exemples of IOT-based attacks

Security cameras hacking

Unauthorized access to connected security cameras allows attackers to monitor users or compromise their privacy..

IoT routers hacking

Insecure IoT routers can be compromised to access the home network and steal sensitive personal data.

Vulnerabilities in connected homes

Hackers can exploit vulnerabilities in connected homes to take control of security systems or home devices

Iot-based attack targets

User Data

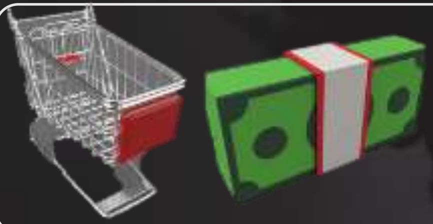
Many IoT devices collect and transmit personal and sensitive data, making them attractive targets for data theft, exploitation, or privacy breaches.

Consumer IoT Devices

Smart home devices, wearables, and connected appliances are potential targets for unauthorized access, data theft, or surveillance.

Healthcare IoT

Medical devices and healthcare systems can be targeted for data theft, remote manipulation, or threats to patient safety.



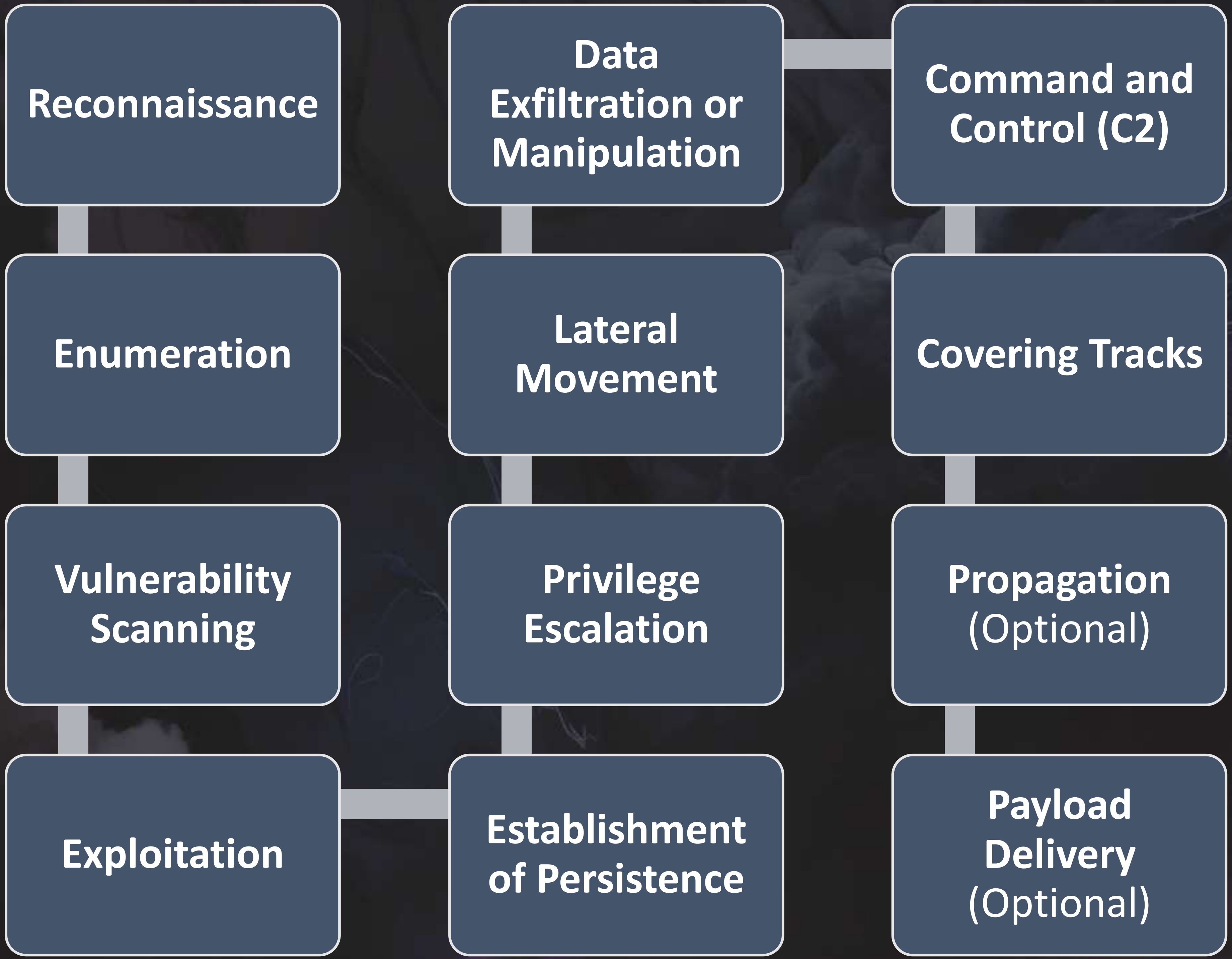
Retail IoT

Point of sale (PoS) systems may be targeted for credit card data theft or to disrupt retail operations.

IoT Networks

The communication networks connecting IoT devices can also be targets for disruption or data theft.

IoT-Based attack Stages



Reconnaissance

Enumeration

Vulnerability Scanning

Exploitation

Establishment of Persistence

Privilege Escalation

Lateral Movement

Data Exfiltration or Manipulation

Command and Control (C2)

Covering Tracks

Propagation (Optional)

Payload Delivery (Optional)

Impacts

IoT-based attacks can have a wide range of impacts, depending on the type of attack, the target, and the attacker's objectives

Data Breaches

Unauthorized access or data theft can lead to sensitive and personal information being exposed, putting individuals at risk of identity theft or fraud.

Privacy Violations

Surveillance or unauthorized data collection through compromised IoT devices can infringe on user privacy and result in personal information exposure.

Financial Loss

Ransomware attacks, fraud, or theft of financial data can lead to financial losses for individuals or organizations.

Operational Disruption

Attacks on critical infrastructure or industrial IoT systems can disrupt operations, potentially causing safety hazards or significant financial losses

Safety Risks

In healthcare and automotive IoT, safety-critical systems can be compromised, leading to risks to patient safety or accidents on the road

Reputation Damage

Publicized IoT-based attacks can damage the reputation of organizations and manufacturers, eroding customer trust.

Loss of Control

Unauthorized access to IoT devices can result in a loss of control over physical and digital aspects, such as smart locks or security cameras

Network Congestion

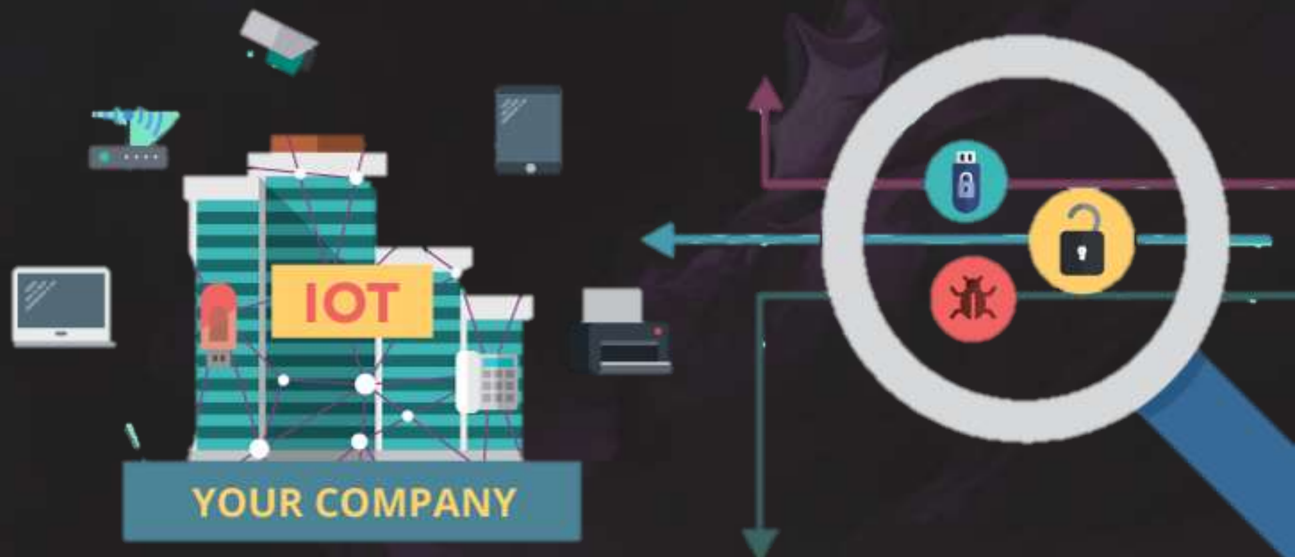
IoT-based DDoS attacks can congest networks, leading to service disruptions for IoT devices and other online services

Iot-based testing !

IoT-based attack testing is the process of simulating real-world cyberattacks to identify and exploit vulnerabilities in IoT devices and systems .

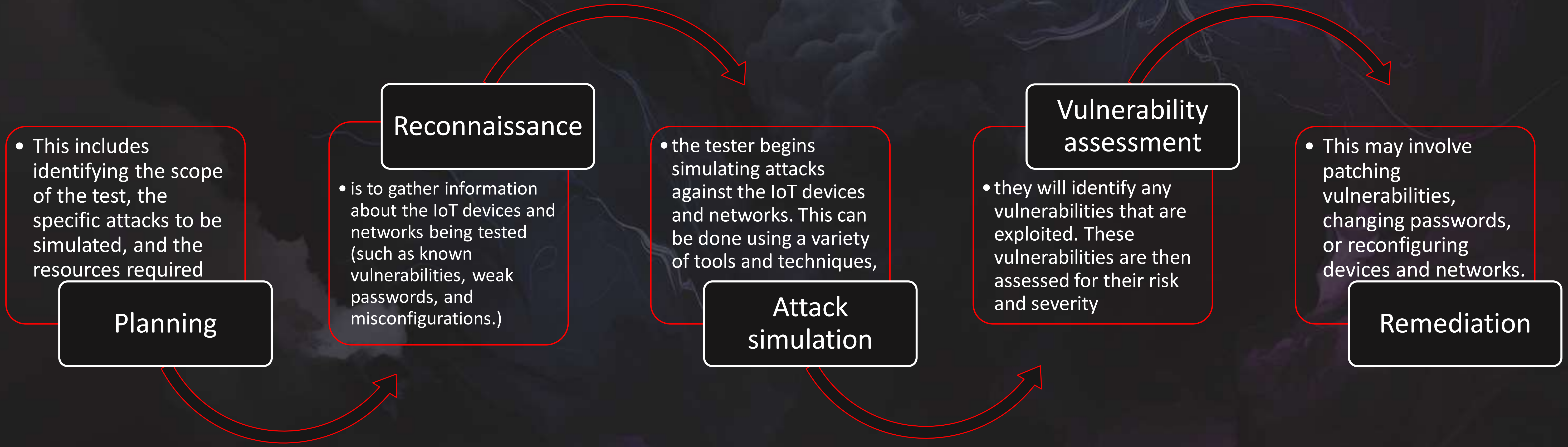
Why is IoT security testing important?

IoT devices are increasingly being targeted by cybercriminals. IoT devices are often poorly secured and can be easily exploited by attackers. By testing IoT devices and systems for security vulnerabilities, organizations can identify and mitigate these vulnerabilities before they are exploited by attackers.



Iot-based testing process

The IoT-based attacks testing process is a systematic approach to identifying and mitigating security vulnerabilities in IoT devices and networks. It involves simulating real-world attacks to see how well the devices and networks can withstand them.



Planning

- This includes identifying the scope of the test, the specific attacks to be simulated, and the resources required

Reconnaissance

- is to gather information about the IoT devices and networks being tested (such as known vulnerabilities, weak passwords, and misconfigurations.)

Attack simulation

- the tester begins simulating attacks against the IoT devices and networks. This can be done using a variety of tools and techniques,

Vulnerability assessment

- they will identify any vulnerabilities that are exploited. These vulnerabilities are then assessed for their risk and severity

Remediation

- This may involve patching vulnerabilities, changing passwords, or reconfiguring devices and networks.

IoT-based testing methods

1

Vulnerability assessment

is the process of identifying and assessing security vulnerabilities in iot devices. can be performed manually or using automated tools.

2

Penetration testing

is a simulated attack on an iot devices to identify and exploit vulnerabilities. Penetration testers use a variety of tools and techniques to attempt to gain unauthorized access to devices and networks, steal data, or disrupt operations.

3

Red team vs. blue team exercises

involves simulating real-world cyberattacks and defense scenarios. Red teams attempt to exploit vulnerabilities and breach iot systems, while blue teams defend the systems and respond to attacks

Detection

IoT devices are often poorly secured and can be used as targets for cyberattacks to gain access to larger networks.

There are a number of techniques that can be used to detect IoT-based attacks, including:

Network traffic

This involves monitoring network traffic for unusual patterns or spikes in activity that could indicate an attack. For example, if an IoT device is suddenly sending a large volume of data to an unknown IP address, this could be a sign of a botnet attack.

Security event

This involves collecting and analyzing security events from IoT devices to identify potential attacks. For example, if an IoT device logs a number of failed login attempts, this could be a sign that an attacker is trying to brute-force the password.

Device behavior

This involves monitoring the behavior of IoT devices for unusual activity, such as unexpected changes in configuration or performance. For example, if an IoT device suddenly starts using more CPU or memory than usual, this could be a sign that it has been infected with malware.

Threat intelligence

This involves using threat intelligence data to identify and track known threats to IoT devices. For example, if a new malware sample is identified that targets IoT devices, organizations can use this information to update their security systems to detect and block the malware.

Prevention

- Have strong passwords for all IoT devices. Regularly change and update them.
- give access to the essential users only.
- Back up data regularly to a secondary device.
- Encrypt data between the IoT devices and the server.
- Place the device in a safe location to prevent any unauthorized access
- Give users limited data and device access, to ensure data confidentiality
- Configure and detect all the devices, This ensures that the data is accounted for and prevents unwanted traffic.

Case studies

1.Mirai Botnet Attack

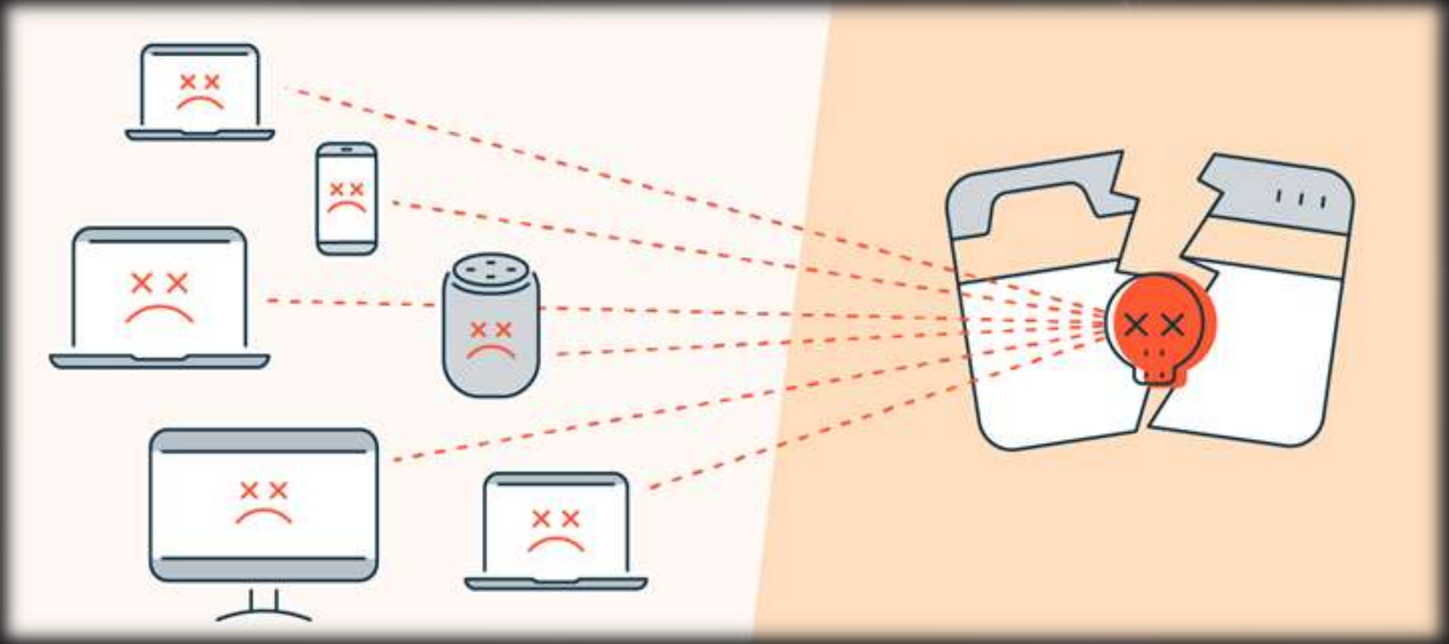
2. DNS changer Malware

3. Jeep hack

1.Mirai Botnet Attack

In 2016, the Mirai botnet launched a massive distributed denial-of-service (DDoS) attack against Dyn, a major DNS provider. The attack caused widespread outages for many popular websites, including Twitter, Amazon, and Netflix.

The Mirai botnet was composed of millions of IoT devices, such as webcams, routers, and DVRs. These devices had been infected with malware that allowed attackers to control them remotely. The attackers then used the botnet to generate a massive amount of traffic, which overwhelmed Dyn's servers.



Response:

Dyn was able to mitigate the attack by filtering out traffic from the botnet. However, the attack highlighted the vulnerabilities of IoT devices and the need for better security measures.

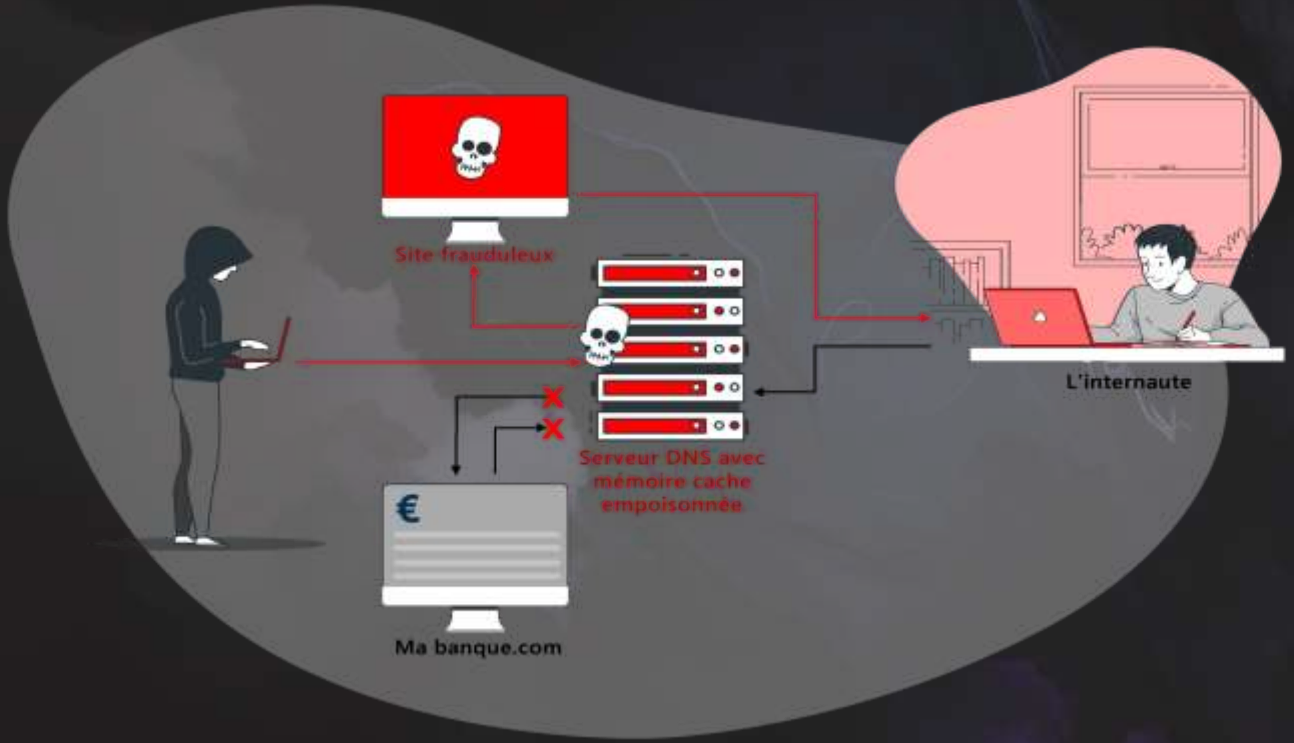
Measures Taken:

Since the Mirai attack, there has been a growing awareness of the need to secure IoT devices. Manufacturers have begun to implement more robust security measures, such as strong passwords and default security settings. Additionally, there has been an increase in the availability of security tools and services for IoT devices.

2 . DNS Changer Malware

In 2007, the DNS Changer malware was discovered to be infecting millions of computers worldwide. The malware changed the DNS settings on infected computers to redirect traffic to malicious websites. These websites then served up malware or attempted to steal personal information from users.

The DNS Changer malware was able to infect IoT devices as well as computers. This is because many IoT devices use the same operating systems and software as computers.



Response:

The FBI launched an operation to take down the DNS Changer botnet in 2012. The operation was successful in disrupting the botnet and preventing it from redirecting traffic to malicious websites.

Measures Taken:

Since the DNS Changer attack, there has been an increase in the awareness of the need to secure DNS settings. Many internet service providers (ISPs) now offer DNS filtering services to protect their customers from malicious websites. Additionally, there are a number of third-party DNS filtering services available.

3 . Jeep hack

The 2015 Jeep Cherokee hack was a groundbreaking event in the cybersecurity landscape, demonstrating the potential for remote cyberattacks on modern vehicles. In this incident, two security researchers, Charlie Miller and Chris Valasek, successfully hacked a Jeep Cherokee remotely, taking control of its steering, acceleration, and brakes. This hack highlighted the growing vulnerabilities of connected cars and the need for robust cybersecurity measures in the automotive industry.

3 . Jeep hack

1.Remote Access:

Miller and Valasek exploited vulnerabilities in the Jeep Cherokee's Uconnect infotainment system to gain remote access to the vehicle's network. This access allowed them to send commands to the car's electronic control units (ECUs), which control various vehicle functions.

3 . Jeep hack

2.Steering Control:

The researchers were able to take control of the Cherokee's steering, causing it to swerve dangerously. They achieved this by sending commands to the car's electric power steering (EPS) module.

3 . Jeep hack

3. Acceleration and Braking Control:

Miller and Valasek also gained control of the Cherokee's acceleration and braking systems. They could remotely accelerate and slow down the vehicle, demonstrating the potential for life-threatening attacks.

3 . Jeep hack

Response:

Fiat Chrysler Automobiles (FCA), the manufacturer of Jeep, issued a recall for the affected vehicles. FCA also released a software patch to fix the vulnerabilities that were exploited by the researchers.

Measures Taken:

The Jeep hack highlighted the need for better security measures in vehicles with connected features. Automakers have begun to implement more robust security measures, such as encryption and authentication. Additionally, there has been an increase in the availability of security tools and services for vehicles.

Finally, to conclude, IoT devices are vulnerable to be attacked due to their weak security system.
there are a lot of attacks that damage your devices and steal your data... so be careful and protect your IoT.