Cyber Security

Most Common Threats

Types, Impacts and Mitigation

CREATED BY OISECOPS AGENCY

Distributed Denial-of-Service (DDoS)

In today's digital landscape, organizations face a multitude of cybersecurity threats that pose significant risks to their operations and data integrity. Among the most pressing threats are Distributed Denial of Service (DDoS) attacks, Man-in-the-Middle (MiTM) attacks, phishing attacks, and ransomware. Each of these threats employs different tactics to exploit vulnerabilities, resulting in potentially devastating consequences such as financial loss, data breaches, and reputational damage. The following are the topics your should expect in this quick ebook. **OiSecOps wishes you a good read!**

1 - Distributed Denial of Service

2 - Man-In-The-Middle attacks (MitM)

3 - Phishing Attacks

4 - Whaling & Spear Phishing Attacks

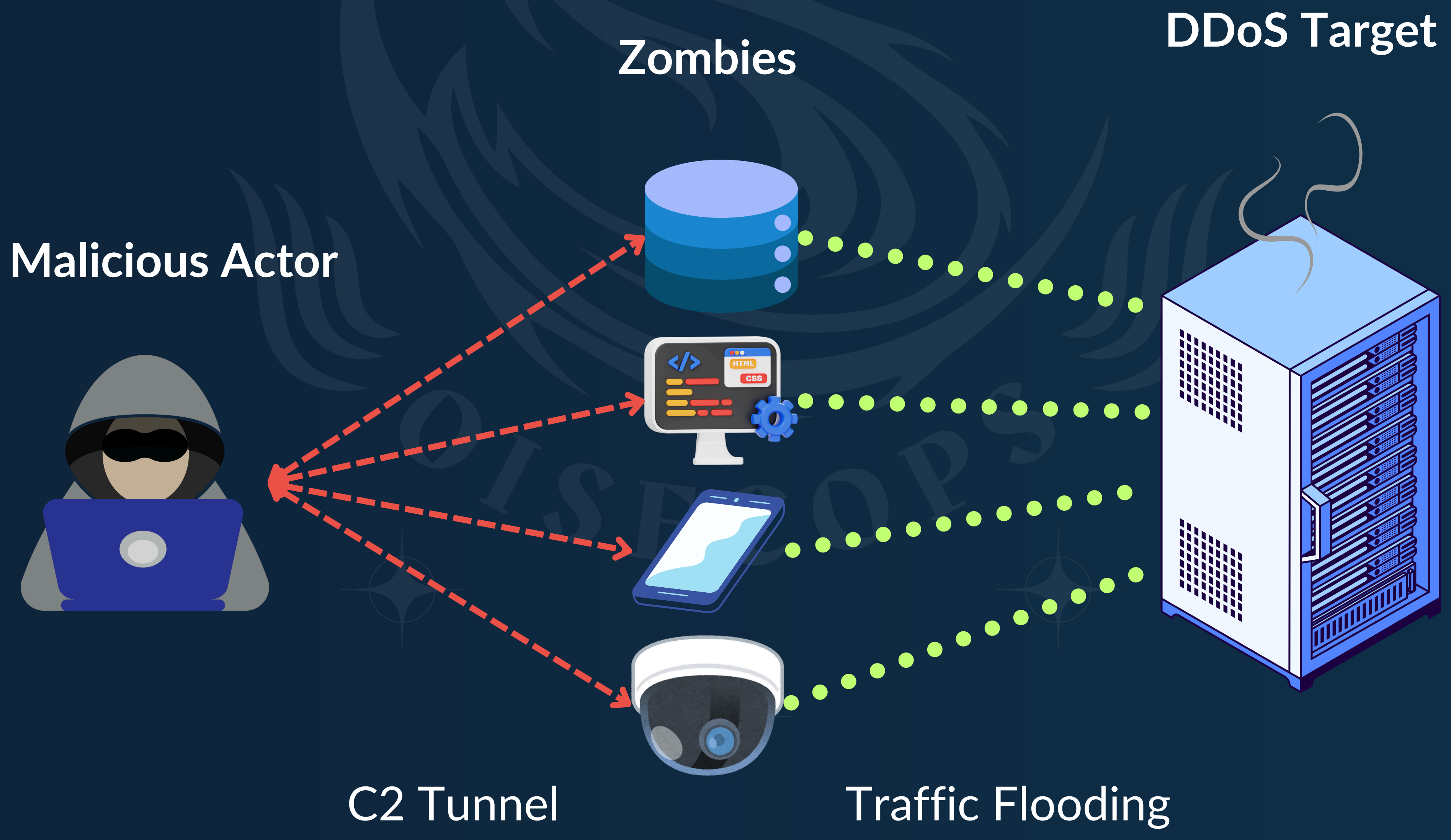
6 - Ransomware

7 - Enhancing Cybersecurity with OISecOps

Distributed Denial-of-Service (DDoS)

The Distributed Denial of Service attack is a malicious attempt to disrupt or interrupt the normal functioning of a target service, network, server, application or IoT devices by flooding the network with traffic.

This type of attack is commonly executed by multiple compromised devices (workstations, desktops, IoT, etc.) which are under hackers' control (Command & Control Techniques), these compromised machines are commonly called Zombies, Bots or BotNets.



There are several types of DDoS attacks, each with its own characteristics and mitigation strategies. The most common types are:

Volume Based

- Consumes Bandwidth
- UDP Flood
- ICMP Flood

Protocol Based

- Abuse Network Protocols
- SYN Flood
- Ping of Death

Application Layer Based

- Fake Requests
- Overwhelm the app
- HTTP Flood
- DNS Flood

Nowadays, there are different types of mechanisms and technologies to protect assets against DDoS attacks. These mechanisms are commonly implemented on both the client and server sides to ensure the best protection and resilience of a system. Some of these mechanisms include:

Content Delivery Networks (CDNs)

Load Balancers

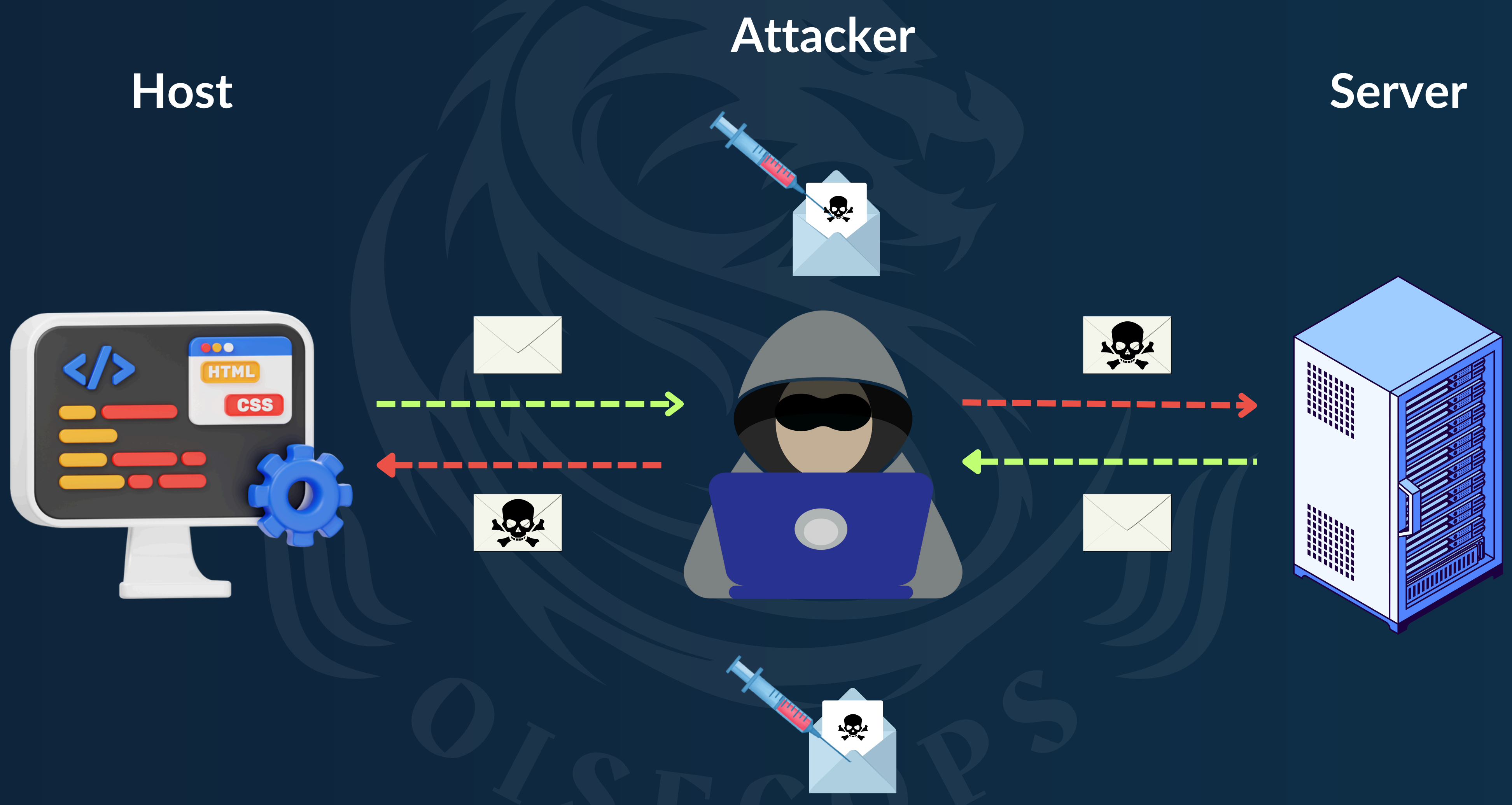
Web Application Firewalls (WAFs)

Cloud Based DDoS Protection

A company that is a victim of a DDoS attack may experience service disruption for a long time, commonly resulting in financial loss and/or security breaches.

Man-In-The-Middle attacks [MitM]

The Man-in-the-Middle attack, also known as MiTM, is a type of attack where a malicious actor intercepts communication between two hosts by posing as a router or another network device. The attacker can eavesdrop on the communication and impersonate one of the parties to steal or manipulate the data being transmitted.



There are different techniques to perform a Man-in-the-Middle (MiTM) attack. The attacker will analyze the network and the devices connected to enumerate possible entry points and weaknesses that could lead to a successful MiTM. Some of these techniques are:

Eavesdropping

The attacker listens to the communication between two parties.

Session Hijacking

The attacker takes over an active session between two parties to gain unauthorized access.

SSL Stripping

The attacker downgrades the secure HTTPS connection to an unencrypted HTTP connection to intercept data.

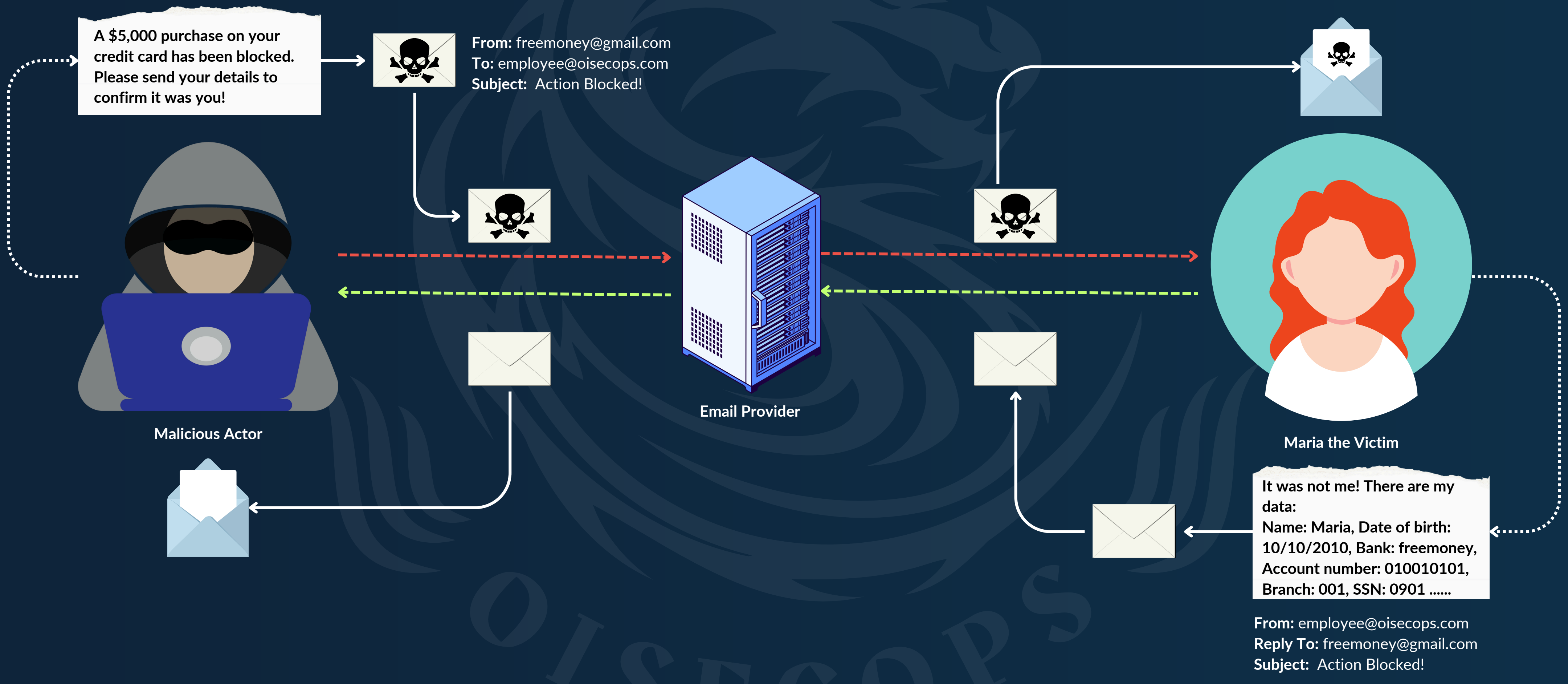
The MiTM attack commonly results in data theft, financial loss, and reputation damage since the attack can steal or manipulate identities, sensitive information, sessions, and in some cases, cause a network denial of service (DoS). To mitigate or reduce the risk of a MiTM attack, responsible personnel can implement one or more of the following:

- Encryption
- PKI
- VPNs
- DNSSEC

In addition, implementing a specialized team to monitor and triage network security events (NSOC) is essential to detect and mitigate MiTM attacks in real-time.

Phishing Attacks

Phishing attacks are among the most common threats faced daily by companies and general internet users. In this type of attack, the malicious actor tries to deceive the user into acting in a way that benefits the attacker, often by disclosing sensitive information. Typically, these attacks are conducted using online techniques such as email, messages, or ads.



A $5,000 purchase on your credit card has been blocked. Please send your details to confirm it was you!

From: freemoney@gmail.com
To: employee@oisecops.com
Subject: Action Blocked!

It was not me! There are my data:
Name: Maria, Date of birth: 10/10/2010, Bank: freemoney, Account number: 010010101, Branch: 001, SSN: 0901 ......

From: employee@oisecops.com
Reply To: freemoney@gmail.com
Subject: Action Blocked!

There are different types of phishing, each with its own target type, structure and objectives. The most common phishing types are:

Email Phishing

Vishing

Smishing

Email Phishing: The most common type of attacks, it consists of fake email messages designed to appear like a legitimate email coming from a trusted source.

Vishing: This attack is conducted over a telephone, generally over a voice call where the attacker act as a legitimate person or company.

Smishing: Performed over SMS messages, this type of attacks abuses the simplicity of the Shot Message Service (SMS).

Others: There are more types of phishing attacks which will be covered in the next sections.

Companies and peoples who fall victim to these types of social-engineering attacks are susceptible to get data breaches, financial fraud, identity impersonation, and other types of injuries.

Moreover, to ensure the protection against these types of attacks the user (CEO, CISO, Analyst, HR, etc...) should set up a defense-in-depth in their routines and systems. Examples of defense-in-depth:

Email Filtering

User Education

Multi-Factor Authentication

Anti-Phishing Software

Whaling & Spear Phishing Attacks

Whaling and spear are more sophisticated types of phishing attacks, now more focused on company's employees and executives.

Whaling Phishing

The Whaling attack has as its main target high-profiles within a company such as CEOs, executives or managers, to extract sensitive information or to approve fraudulent transactions.

CEO Fraud

Impersonating executives to authorize financial transfers

Business Email Compromise (BEC)

Using compromised email accounts to conduct attacks.

Financial loss, identity fraud, data breach, and reputation damage are some of the consequences generated by this attack since it target personnel with a high-profile.

Spear Phishing

Spear Phishing aims specific individuals or organizations. In this case the attackers learn about the target, collecting and discovering personal information, increasing their arsenal to craft more convincing and persuasive approaches.

Email Spear Phishing

Customized emails that appear to come from known or trusted sources.

Social Media Spear Phishing

Using social media platforms to gather information and send personalized messages.

Individuals who fall victim to this attack are commonly harmed in different aspects, such as: Financial Fraud, Data Breaches, and Intellectual Property Theft.

The more effective mitigation approaches to evade or decrease the impact of Whaling and Spear Phishing attacks could be:

Email Authentication

Executive Training

Transaction verification

Advanced Threat Protection

Behavioral Analysis

Security Awareness Training

Ransomware

Ransomware is one of the most dangerous types of malware faced by security and cyber teams recently. This malware encrypts users' files making them inaccessible. The attackers commonly demands a payment in exchange for the decryption key. The attacker generally demands payment in cryptocurrency.

Today is possible to find many different types of Ransomware with different attack strategies, anti-malware evasion, persistence, encryption methodology, unusual extortion, etc... The most common variation of ransomware found are:

Maze (ChaCha) Ransomware

- Steals data before encryption
- Discloses the files when the payment is not executed

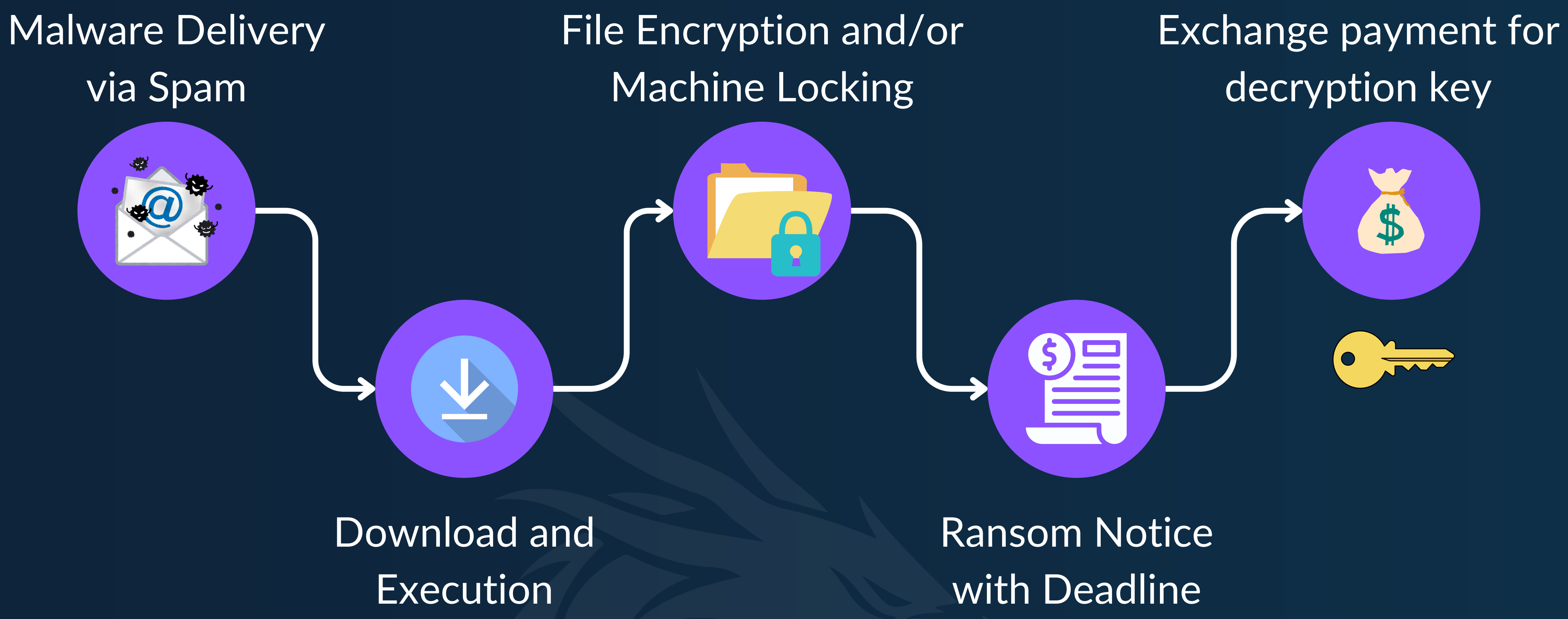
Conti (IOCP) Ransomware

- Make file copies to the malware operators
- Offers infosec help when the company is agreeing to pay

REvil (Sodin) Ransomware

- Use legitmate CPU functions to bypass security measures
- holds the record for the largest ever known ransom demand

Companies which are affected by an Ransomware commonly faces a large data breach, huge financial loss, long periods of DoS, reputation damage, legal restrictions and fines, etc...



Malware Delivery via Spam

Download and Execution

File Encryption and/or Machine Locking

Ransom Notice with Deadline

Exchange payment for decryption key

to mitigate, avoid, or decrease the risks of a ransomware incident may include the implementation of security mechanisms, information security awareness and training, system redundancy, regular data backup, incident response planning, business continuity plan, among other such as:

Endpoint Protection

Application Allowlisting

Network Segmentation

Patch Management

Enhancing Cybersecurity with OISecOps

As the threat landscape continues to evolve, organizations must adopt robust cybersecurity measures to protect their assets and maintain operational resilience. OISecOps is dedicated to providing comprehensive cybersecurity solutions tailored to meet the unique needs of your business. Our services are designed to help you effectively combat threats like DDoS attacks, MiTM attacks, phishing, and ransomware.

Information Security Consultation ✓

Our expert consultants conduct comprehensive assessments to identify vulnerabilities in your organization's security framework. We provide strategic guidance to enhance your cybersecurity posture, ensuring that your defenses are aligned with the latest threat intelligence and best practices.

Training & Awareness ✓

Empower your team with the knowledge and skills needed to recognize and counteract cybersecurity threats. Our training programs focus on educating employees about common attack vectors, such as phishing and social engineering, fostering a culture of security awareness within your organization.

Installation & Configuration

Achieving maximum protection requires the correct setup and optimization of cybersecurity tools and systems. Our specialists ensure that your security infrastructure is configured to withstand sophisticated attacks, providing you with peace of mind that your defenses are robust and reliable.

Malware Removal & Cleaning

In the event of a malware infection, swift action is crucial to mitigate damage. Our team efficiently removes malicious software, restores your systems to a secure state, and implements measures to prevent future breaches, minimizing downtime and data loss.

Technical Support

OISecOps offers comprehensive technical support to resolve your cybersecurity issues promptly and maintain system integrity. Our experienced technicians are available to assist with troubleshooting, ensuring that your security systems operate smoothly and effectively.

Penetration Testing ✓

Regular penetration testing is essential to identify and address security weaknesses. Our thorough testing services simulate real-world attacks to uncover vulnerabilities, providing actionable insights to enhance your organization's security posture and protect against potential breaches.

Personal Security Advisement ✓

In an era where personal data is highly vulnerable, safeguarding your digital assets is paramount. Our tailored security guidance helps individuals protect their personal information and privacy, ensuring that your digital life remains secure from unauthorized access and exploitation.

At OISecOps, we are committed to delivering exceptional cybersecurity services that not only defend against threats but also empower organizations and individuals to thrive in the digital age. Partner with us to fortify your defenses and achieve a resilient cybersecurity strategy.

Don't hesitate—book a consultation with us today and fortify your defenses with a resilient cybersecurity strategy.

OiSecOps Main Page

https://leooliveoi.github.io/OiSecOps/

OiSecOps LinkedIn Page

https://www.linkedin.com/company/oisecops

OiSecOps Youtube Channel

https://www.youtube.com/@oisecops

OiSecOps X Page

https://x.com/OiSecOps

OiSecOps Upwork Portal

https://www.upwork.com/agencies/1810333607200694272/

OiSecOps Consultation for $5

https://www.upwork.com/services/consultation/development-it-leonardo-1800594918157428877