**“Identification of Payloads and attacks utilized today”**

**Table of Contents: Pages**

*Introduction*  ***(3)***

*Man-In-The-Middle-Attack (MITM) (4)*

*Phishing and Spear Phishing (4)*

*Drive-By Attack (5)*

*Bo-Net Attacks (5)*

*Social Engineering Attack (5)*

*SQL Injection Attack (5)*

*Malware Attack (6)*

*Cross-Site-Scripting (SXX) (6)*

*Password Attacks (6-7)*

*Denial-of-Service attack (DoS) (7)*

*Distributed-Denial-of-Service attack (DDoS) (7-8)*

*The Inside attack and Data Breach (8)*

*Eavesdropping attack (8)*

*SolarWinds Software Breach (8-9)*

*Supply-chain attack (8)*

Daniel Rao

Feb 7th, 2021

Vince Skinner

**Identification of Payloads and attacks utilized today**

Attackers use various different methods to exploit/attack a computer network or systems. Every type of attack serves a very unique purpose. Some are hard to defend against while some are relatively easy to deal with. In order to defend and recover from such attacks it is very important to understand how they are processed and structured in the first place. There are several types of attacks that include the use of payload. In this paper I am going to talk about at least 15 different types of attacks that are utilized today where some will utilize the use of payloads. Now to keep things clear let me introduce the idea of what payload is:

**Payload:** A payload in cybersecurity is a malware that a hacker intends to deliver to the victim.

For example: An attacker sends an email out with a malicious Macro as an attachment and say that the victim gets infected with ransomware. In this case the ransomware will be a payload.

Moving on further lets get started with several methods to attack that are used by attackers today as the world is getting complex each and every single day, among which some may type of attacks may utilize payloads and some may not. It totally depends on the intention of the attacker.

1. **Man-In-The-Middle (MITM) Attack:**

This type of attack is carried out by attackers by interrupting an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants.

Cyber Attackers carry out this attack by:

1. Hijacking
2. Active Eavesdropping
3. IP Spoofing
4. Replay

Common ways to defend against such attacks are:

1. Encryption
2. Tamper detection
3. Authentication of digital Certificate.
4. **Phishing and Spear-Phishing Attacks:**

In this type of attack, the attackers send fraudulent emails with clickable links. These types of attacks often aid the attackers to steal personal information that might be stored on the system. Attackers apart from this also attack computers to install malware on the system. This is delivered to the victim in the form of payload.

1. **Drive-By attack:**

Attackers often use this technique to spread malware. They often target insecure websites that have vulnerabilities. Once they find it, the attacker injects a malicious script into the HTTP or PHP code of the website page. This script compromises the network of the site visitor.

1. **Bot-Net attacks:**

If we talk about botnets, they are a collection of system networks in which attackers have already injected malware. The botnet attack is commonly used by the attackers to carry out a DDoS (Distributed Denial of Service attack) at a very large scale.

It is often very difficult to spot a DDoS attack as the attackers use a lot of proxies to hide themselves on the internet. This process of hiding oneself by using several proxies around the globe is called proxy chaining.

1. **Social Engineering attacks:**

Attackers often use this type of attack to use social engineering to access personal data of the victims. They use these type of attacks to carry out an educated guess to hijack accounts of the victim or for the purpose of identity impersonation or to perform unauthentic payments.

1. **SQL injection attack:**

This type of attack happens when the attacker injects malicious code in an SQL server.

This type of attack tricks the server to divulge information it doesn’t usually disclose.

1. **Malware attack:**

This is an umbrella term that is used for different types of cyber attacks that use malicious software to compromise computer security.

Steps on preventing a malware attack:

1. Using a trusted Antivirus software.
2. Being careful when opening emails from unknown sources.
3. Avoiding to click malicious pop-up and keeping the firewall up-to-date.
4. Updating the operating system regularly (Oftentimes these are bug fixes in the code).
5. **Cross-Site-Scripting Attack (XSS):**

This type of attack makes use of the third party website to inject malicious JavaScript code into the targets web browser. The attack can be utilized for capturing screenshots and discovering and collecting network information and gaining remote access and control over the victim's computer.

1. **Password Attack:**

This type of attack leverages the attacker or password authentication to gain access to users information. These types of attacks can take several forms such as:

1. **Brute Force Attack:** It is used by the internet fraudster to guess all the possible passwords. They commonly do this with advanced programs which help decipher passwords based on certain factors and algorithms.
2. **The dictionary attack:** This attack occurs when cyber criminals make use of the dictionary of common passwords to guess the targets password. This type of attack can be defended against if the user follows strong password policies by using special characters etc.
3. **Keylogger Attack:**

The cyber criminals make use of programs that can capture the keystrokes to get the passwords and user ID’s. Therefore it is extremely important to install an antivirus and be careful of what programs we install or be careful to not trust anyone's personal or public computers. This type of attack is very simple but yet quite dangerous when it comes to what it is capable of.

1. **Denial-of-Service (DoS):**

This is one of the most widespread type of cyber attack which is done by making a resource unavailable to the user. However this attack can easily be spotted with special analytical tools that are often used by the ethical hackers. These tools will help to investigate a strange traffic growth. These types of attacks can be prevented by keeping the network security system updated.

1. **Distributed Denial of Service Attack (DDoS):**

The attack occurs when many compromised network devices all over the internet such as IoT devices are compromised over the network and These devices are used to flood the bandwidth of the target system. DoS and DDoS attacks can occur through:

1. Session Hijacking
2. TCP-SYN flood attack
3. Tear drop attack
4. Smurf attack
5. Ping of death attack
6. Botnets
7. **The inside attack and Data Breaches:**

This type of attack occurs commonly through the activities of disgruntled employees or ex-employees. To defend against this type of attack it is important to access networks for current employees. At the same time it is important to drop the privilege of the employee who is fired or leaves.

1. **Crypto Jacking attack:**

It uses the bandwidth of the user's computer and processing power to mine crypto currency. These cyber attackers break into the network to accomplish this attack. Therefore it is very important to update and install good antiviruses and not to open fishy emails.

1. **Eavesdropping attack:**

It occurs when the attackers intercept the users network traffic. This attack helps the attacker gain passwords and other personal and financial information.

The best protection of this attack is knowing what devices are connected to a network and what softwares are installed on those devices.

**SolarWinds Software Breach:**

Now that we know these different types of attacks we can learn more about them and eliminate them that are harmful to us and our businesses. Finally we have supply chain attack:

1. **Supply-chain attack:**

Hackers managed to access a system that SolarWinds uses to put together updates to its Orion product, the company [explained in a Dec. 14 filing](https://www.sec.gov/Archives/edgar/data/0001739942/000162828020017451/swi-20201214.htm) with the SEC. From there, they inserted malicious code into otherwise legitimate software updates. This is known as a [supply-chain attack](https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html) because it infects software as it's under assembly.

It's a big coup for hackers to pull off a supply-chain attack because it packages their malware inside a trusted piece of software. Hackers typically have to exploit unpatched software vulnerabilities on their targets' systems to gain access, or trick individual targets into downloading malicious software with a phishing campaign. With a supply chain attack, the hackers could rely on several government agencies and companies to install the Orion update at SolarWinds' prompting.

The approach is especially powerful in this case because thousands of companies and government agencies around the world reportedly use the Orion software. With the release of the tainted software update, SolarWinds' vast customer list became potential hacking targets.