Malware, DOS, and Web Attacks, Oh My!

Ryan Coon

CYB-505

Professor Devin Ogg

August 28, 2024

|  |  |
| --- | --- |
| **Malware Attack Type** | **Definition and Characteristics of Attacks** |
| HTTP Flood | An HTTP Flood is a type of Distributed Denial of Service (DDoS) attack that targets web servers by overwhelming them with a massive volume of HTTP requests. The goal is to exhaust server resources, leading to degraded service or complete unavailability of the website.  Prevention:  Use rate limiting, Web Application Firewalls, analyze traffic |
| Protocol Attacks | Protocol Attacks are a category of Distributed Denial of Service (DDoS) attacks that exploit weaknesses in network protocols to disrupt the normal functionality of a network or service. These attacks typically target the transport and network layers of the OSI model, aiming to overwhelm systems with a flood of malicious traffic.  Prevention:  Use Intrusion Detection Systems, Use firewalls, Limit rates |
| Slowloris | Slowloris is a type of Denial of Service (DoS) attack that targets web servers by holding connections open and consuming server resources without completing the requests. This allows the attacker to exhaust the server’s maximum connection limit, effectively preventing legitimate users from accessing the service.  Prevention:  Set timeout values for HTTP connections, Set rate limits for connections from certain IP addresses, Use Web Application Firewalls, Limit connections from certain IP addresses |
| SYN Flood | SYN Flood is a type of Denial of Service (DoS) attack that exploits the TCP handshake process to overwhelm a target server with a flood of SYN (synchronize) requests. This attack aims to consume server resources, leading to service disruption for legitimate users.  Prevention:  Use SYN cookies, Set connection limits, Use firewalls and Intrusion prevention systems, Set rate limits on SYN packages from individual IP addresses |
| Ping of Death | Ping of Death is a type of Denial of Service (DoS) attack that involves sending malformed or oversized ICMP (Internet Control Message Protocol) packets to a target system, causing it to crash, freeze, or become unresponsive. This attack exploits vulnerabilities in the way operating systems process large packets.  Prevention:  Update systems regularly, Use firewalls, Use intrusion detection systems, Set rate limits on ICMP traffic |
| Botnets | A botnet is a network of compromised computers or devices, often referred to as bots or zombies, that are controlled by a central command and used to perform coordinated tasks, typically without the knowledge of the device owners. Botnets are commonly utilized for malicious purposes, including DDoS attacks, spam distribution, data theft, and more.  Prevention:  Perform regular software updates, Use security software, Use firewalls and intrusion detection systems, Monitor network traffic |
| DDoS | DDoS stands for Distributed Denial of Service. It is a malicious attack aimed at disrupting the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic. Unlike a standard DoS attack, which originates from a single source, a DDoS attack is launched from multiple compromised systems, making it more challenging to mitigate.  Prevention:  Monitor traffic, Use DDoS protection services, Implement redundant systems, Set rate limits, Update incident response plans |
| Session Hijacking | Session hijacking is a type of cyberattack where an attacker takes control of a user's active session after successfully exploiting a vulnerability in a web application or network. This allows the attacker to impersonate the legitimate user and gain unauthorized access to sensitive information or services.  Prevention:  Use secure session management, Use HTTPS, Implement SameSite Cookies, Perform regular security audits |
| Spear Phishing | Spear phishing is a targeted form of phishing where attackers focus on a specific individual or organization to steal sensitive information.  Prevention:  Verify sources of sender, Use security tools, Enable two-factor authentication, Educate employees |
| Dictionary Attacks | A dictionary attack is a method used by attackers to gain unauthorized access to a system or account by systematically entering every word in a predefined list, or "dictionary," of likely passwords. In today’s society though most places have certain requirements for passwords to get away from people using common word.  Prevention:  Strong complex passwords, Longer passwords, Account lockout mechanisms, Multi-Factor Authentication |

References:

Amazon Web Services. (n.d.). What is a DDOS Attack & How to Protect Your Site Against One. Amazon Web Services, Inc. https://aws.amazon.com/shield/ddos-attack-protection/

Chinnasamy, V. (2021, March 11). What is SYN Attack and How to Prevent the Attack? | Indusface Blog. Indusface. https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/

Dictionary Attack - an overview | ScienceDirect Topics. (n.d.). Www.sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/dictionary-attack

Dictionary Attacks Explained | NordVPN. (2020, November 20). What is a dictionary attack? How to prevent it. NordVPN. https://nordvpn.com/blog/dictionary-attack/?srsltid=AfmBOoo5NikmWjVZ61vFCZydTkGOPesJOgbg10vhPS26YXjyYt0OFddf

EC-Council. (2022, March 29). What Is Session Hijacking, and How Can It Be Prevented? Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/how-to-prevent-session-hijacking-attacks/

Imperva. (n.d.-a). What is a TCP SYN Flood | DDoS Attack Glossary | Imperva. Learning Center. https://www.imperva.com/learn/ddos/syn-flood/

Imperva. (n.d.-b). What is Ping of Death (PoD) | DDoS Attack Glossary | Imperva. Learning Center. https://www.imperva.com/learn/ddos/ping-of-death/

Imperva. (2021). DDoS Attack Types & Mitigation Methods | Imperva. Learning Center. https://www.imperva.com/learn/ddos/ddos-attacks/

KasperSky. (2019). What is a Botnet? Kaspersky.com. https://usa.kaspersky.com/resource-center/threats/botnet-attacks

OWASP. (2020). Session hijacking attack. Owasp.org. https://owasp.org/www-community/attacks/Session\_hijacking\_attack

Ping of Death DDoS attack | Cloudflare. (n.d.). Cloudflare. https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/

Rafter, D. (2023, September 1). What is a botnet? Us.norton.com. https://us.norton.com/blog/malware/what-is-a-botnet

Website Security and Prevention of a HTTP Flood Attack ⚔️. (n.d.). Www.wallarm.com. https://www.wallarm.com/what/website-security-and-prevention-of-a-http-flood-attack

What does DDoS Mean? | Distributed Denial of Service Explained | Imperva. (n.d.). Learning Center. https://www.imperva.com/learn/ddos/denial-of-service/#:~:text=Distributed%20denial%20of%20service%20(DDoS)%20attacks%20are%20a%20subclass%20of

What is a Protocol DDoS Attack? | Glossary. (n.d.). A10 Networks. https://www.a10networks.com/glossary/what-is-a-protocol-ddos-attack/

What is an HTTP Flood | DDoS Attack Glossary | Imperva. (n.d.). Learning Center. https://www.imperva.com/learn/ddos/http-flood/

What is Slowloris? | DDoS Tools | Imperva. (n.d.). Learning Center. https://www.imperva.com/learn/ddos/slowloris/

What Is Spear Phishing? (n.d.). Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-spear-phishing.html

Wright, G. (2024, February). What is a dictionary attack? - Definition from WhatIs.com. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/dictionary-attack

(2019). Kaspersky.com. https://usa.kaspersky.com/resource-center/definitions/spear-phishing