December 2016 Cyber Awareness Newsletter

Understanding and Preventing DoS and DDoS Attacks

Background

A hacktivist has been charged recently for two Distributed Denial-of-Service (DDoS) attacks on hospitals that occurred in 2014. The hacktivist overloaded hospital computers with unlawful internet traffic that caused the facilities' systems to experience disruptions in operations and resulted in hundreds of thousands of dollars in losses and damages.

How Denial of Service Attacks Work (DoS)

According to US-CERT, the United States Computer Readiness Team, Denial-of-Service (DoS) attacks occur when an attacker attempts to prevent legitimate users from accessing information or services. This is done by targeting a user system and its network connections, or the systems and network of the sites users are trying to access. An attacker may be able to prevent patients or healthcare personnel from accessing critical healthcare assets such as payroll systems, electronic health record databases, and software-based medical equipment (MRI, EKGs, infusion pumps, etc.).

These attacks occur commonly when an attacker floods a network with information. For instance, when a user types a URL (web address) for a particular website into a browser, the user is sending a request to that site's computer server to view the page. An attacker can overload a server with numerous requests so that valid users cannot get through to the site. An attacker can also utilize spam email messages to flood a user's email account. For example, countless or large email messages may be sent to email accounts causing the users to consume their email quota and preventing them from receiving or sending legitimate emails.

How Distributed DoS Attacks Work

In DDoS (Distributed Denial of Service) attacks, one system may be used to attack another system. For instance, an attacker may hijack or take control of a computer, forcing the computer to send huge amounts of illegitimate data traffic to particular websites or spew spam to particular email addresses. The attacker can also control multiple computers, called botnets or robot networks, with malicious software to launch a DoS attack.

Growth of the Internet of Things May Escalate Attacks

DoS and DDoS attacks may escalate in the near future, especially with the increased usage of IoT (Internet of Things) in the healthcare sector. IoT is a technology that allows multiple devices that have Internet access to communicate and transmit data with each other through the Internet, without the interaction of humans. This form of technology is used in the healthcare sector, for example, to allow healthcare facilities to monitor medical devices, patients, and personnel. The more our various smart devices are connected, the more harm can be done by a cyberattack.

How to Recognize an Attack in Progress

According to US-CERT, not all disruptions to service are the result of a DoS attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms *could* indicate a DoS or DDoS attack is underway:

- Unusually slow network performance (in opening files or accessing websites);
- Unavailability of a particular website;
- Inability to access any website;
- Dramatic increase in the amount of spam you receive.

Recommended Preventive Measures

US-CERT recommends the following best practices be implemented by healthcare covered entities and their business associates to prevent DoS and DDoS attacks:

- Continuously monitor and scan for vulnerable and comprised IoT devices on networks, and follow proper remediation actions.
- Create and implement password management policies and procedures for devices and their users. Ensure all default passwords are changed to strong passwords. Default usernames and passwords for most devices can easily be found on the Internet, making devices with default passwords extremely vulnerable.
- Install and maintain anti-virus software and security patches. Updating IoT devices with security patches as soon as patches become available is critical.
- Install a firewall, and configure it to restrict traffic coming into and leaving your network and IT systems.
- Segment networks where appropriate and apply appropriate security controls to control access among network segments.
- Disable Universal Plug and Play (UPnP) on routers unless absolutely necessary.
- Look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.
- Monitor Internet Protocol (IP) port 2323/TCP and port 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet) protocol.
- Practice and promote security awareness. It is important to understand the capabilities of IT systems, medical devices, and HVAC systems with network capabilities that are installed on Covered Entities and Business Associates networks. If the device has open Wi-Fi connection and transmits data or can be operated remotely, it has the potential to be infected.
- Follow good security practices for distributing email addresses. Applying email filters may help entities manage unwanted traffic.

For More Information

United States Computer Emergency Readiness Team (US-CERT) *Heightened DDoS Threat Posed by Mirai and Other Botnets* *https://www.us-cert.gov/ncas/alerts/TA16-288A*

United States Computer Emergency Readiness Team (US-CERT) *Understanding Denial of Service (DoS) Attacks* https://www.us-cert.gov/ncas/tips/ST04-015

OCR's monthly Cyber Awareness newsletters and other HIPAA Security Rule Guidance Material may be found at http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html