U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

November 2016

Understanding DoS and DDoS Attacks and Best Practices for Prevention

Recently, a hacktivist was charged over two hospital Distributed Denial-of-Service (DDoS) attacks that took place in 2014. According to an article posted on Naked Security website, 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.

According to US-CERT, 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 use. An attacker may be able to deter 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 are commonly done 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. Also, an attacker can utilize spam email messages to flood a user's email account. For example, an attacker may send countless or large email messages to email accounts causing the users to consume their email quota and preventing them from receiving or sending emails.

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

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 to allow healthcare facilities to monitor medical devices, patients, and personnel.

It was reported recently by US-CERT that an IoT botnet that included hundreds of thousands of IoT devices, was used to launch Domain Name System (DNS) DDoS attacks against multiple devices, causing customers of online properties to be without service. The IoT botnet used to launch the attacks was comprised mostly of internet–enabled digital video recorders, surveillance cameras, and additional enabled devices. These IoT devices were integrated, without the device-owner's knowledge, into the botnet when continuously scanned for well-known device vulnerabilities and exploited them.

How do you know if an attack is occurring?

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:

- unusually slow network performance (opening files or accessing websites);
- unavailability of a particular website;
- inability to access any website;
- dramatic increase in the amount of spam you receive in your account.

To prevent the possibility of being part or a target of DoS or DDoS attacks, US-CERT suggests that Covered Entities and Business Associates consider:

- Continuously monitoring and scanning for vulnerable and comprised IoT devices on their networks, and following proper remediation actions.
- Creating and implementing password management policies and procedures for devices and their users. Ensuring 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.
- Installing and maintaining anti-virus software and security patches. Updating IoT devices with security patches as soon as patches become available is critical.
- Installing a firewall, and configuring it to restrict traffic coming into and leaving your network and it systems.
- Segmenting networks where appropriate and applying appropriate security controls to control access among network segments.
- Disabling Universal Plug and Play (UPnP) on routers unless absolutely necessary.
- Looking for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

- Monitoring 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.
- Practicing and promoting security awareness. It is important to be aware and 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.
- Following good security practices for distributing email addresses. Applying email filters may help entities manage unwanted traffic.

References:

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