THE SafeHarbor™ BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - June 2018

COMBATTING COMMON USER THREATS

User Education and Awareness - PART 3

Last month's newsletter discussed phishing and the common types of dangers that phishing can pose to a company's network or user's personal and financial data through information gathering techniques. One topic that is often associated with phishing, and the primary topic of this edition, is **malware**.

Phishing attempts can rely on just information gathering but more often they come with an attachment or website link for the user to click on. These attachments or web links usually have malware attached to them to affect the user's computer system and eventually the entire enterprise network.

Malware

Malware is short for **mal**icious soft**ware**. Malware is any program that is intended to damage or disable a computer or computer systems and is used as a general term to describe worms, viruses, trojans, ransomware, and rootkits.

Purpose of Malware

Damage or disrupt network functionality – Viruses and trojan bombs typically have set criteria written within their code and are used to damage a network by deleting critical data or damaging functionality of the system itself. Worms are typically used to disrupt network functionality because they replicate themselves through network systems and use a large amount of bandwidth causing the network to slow down. This results in a loss of productivity (not to mention the frustration of having a slow network) for the company followed by potential financial loss.

Steal Information – Spyware can be used to steal proprietary company information or personal and financial data of the infected user.

Extortion (monetary gain) – One of the newer methods to gain money from a user or company is with ransomware. Ransomware encrypts a computer system and threatens to delete the encrypted data unless a ransom is paid within a set amount of time.

Types of Malware

Adware – Software that automatically displays or downloads advertising material when a user is online. The primary purpose of legitimate adware is to display customized ads for the user based on their personal browsing and shopping preferences; however, adware

MALWARE ON THE RISE

Internet security company SonicWall recently announced its 2018 Cyber Threat Report, which recorded approximately 9.32 billion malware attacks last year.

MALWARE AND WEB-BASED ATTACKS ARE THE TWO MOST COSTLY ATTACK TYPES — COMPANIES CAN SPEND AN AVERAGE OF $2.4 MILLION IN DEFENSE

-ACCENTURE

IN 2017, OVERALL MALWARE VARIANTS WERE UP BY 88 PERCENT

-SYMANTEC

can also be used maliciously if the obtained data is sold to a third party to build a profile on specific users. Adware can also be considered spyware and should be avoided altogether.

Ransomware – malicious software designed to deny a user access to data on their computer system by encrypting the data. Users are promised to have their data returned once a ransom has been paid. There is no guarantee, however, that the data will be returned even after a ransom has been paid. The data is returned by the user given a encryption key.

Rootkit – Rootkits are often used in conjunction with other malware, such as viruses and worms, to hide its presence from anti-virus software. Rootkits enable access to a computer or areas of its software that is not otherwise allowed and often masks kits existence or the existence of other software.

Spyware – Software that aims to gather information about a user or their company without the user's knowledge. The data collected from spyware can be sent to a third party without the user's consent or knowledge. Spyware can consist of URL loggers and screen recorders, chat loggers and email recorders, keyloggers and password recorders, and browser hijacking.

Trojan Horse – Malware that hides its true intent from the user and presents itself as legitimate software. Exactly as the name implies, the trojan horse is named after the Greek subterfuge used to win the Trojan War and gain entry to the city of Troy. It is important for users to understand this concept and ensure that software is verified and trusted by the company and cybersecurity team before downloading any software to their computer system.

Worms – Self-replicating malware that can spread itself across a company's enterprise network causing a significantly increased load on infected computer system CPUs and network bandwidth. Worms can also have a "payload" or written code that seek to exfiltrate data from system, delete select system files, encrypt files for use in ransomware, or create a backdoor on the system to use the affected system.

Virus – Self-replicating malware typically used to destroy data or corrupt computer system integrity. Once a virus has infected a system it can delete software application code, corrupt or delete core system files, encrypt data for use in a ransomware, and use evasion or stealth techniques to hide itself from anti-virus engines. The key difference between a virus and worm is that a worm is a standalone program that can self-replicate without user or program intervention to spread whereas a virus needs the assistance of a user or program to spread the infected file.

Defense Against Malware

As with phishing, the first and most important defense against malware is user education and awareness.

1. Train your users regularly to ensure they know not to click on unsolicited links or attachments within email as they could be infected with malware. Implement spam filters, firewalls, and keep your anti-virus engines up-to-date.

Consider blocking most pop-ups through your web browser to prevent the inadvertent clicking of adware or spyware when using the internet.

2. Train users to identify suspicious activity on their computer systems, such as a significant slowdown in computer system performance, and report it to their cybersecurity team immediately.

Actions to take will depend on the activity of the malware and the boundary defense mechanism your company has deployed. For most viruses and worms, the system should be:

- Unplugged from the network immediately
- Handed over for inspection and repair by the cybersecurity team

It is very important when dealing with malware to regularly perform backups to maintain minimal loss of data, especially concerning ransomware; you may lose a day's worth of work but it is better than paying a malicious actor with no guarantee you will get your data returned intact!

About Gnostech Inc.

Gnostech Inc. is an applied engineering and consulting company with over 35 years of experience and expertise in information assurance and cybersecurity engineering, and major combat and space systems development and integration. Gnostech provides the necessary knowledge and technology to ensure success of critical missions for customers in both the defense and maritime industries. To learn more, visit www.gnostech.com.