SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
E: sales@sonmax.com
T: +1 732.591.1512
F: +1 732.591.5424
www.sonmax.com

The Threat of Malware

Malware is not a one size fits all threat. Specifically, malware is any malicious software intended to damage, disrupt, steal from or disable computers and computer systems that are used for your business. The question is not **IF** you will experience a technology-based attack, but **WHEN**. The types of malware threats are described below and how disruptive they are to businesses and personal technology systems.

Common types of malware include:

- Botnet
- Phishing
- Ransomware
- Rogue Security Software
- Rootkit
- Spam
- Spyware
- Trojan Horse
- Virus
- Worm

Botnet is a confederation of internet-connected devices (computers, tablets, smartphones, etc.) that have been attacked by a specific type of virus. Each individual infected device is known as a zombie, as the operator of the device will not know that their system is engaged in malicious activity. The botnet is controlled by a "bot master" who uses these unwitting devices to propagate the malicious behavior. This can be as simple as using the zombie's contact list to distribute spam to every contact. If the botnet has enough zombies, it can be used to initiate a website attack, effectively knocking the website out of service – known as a denial-of-service ("DoS") attack. The result is you lose the ability to conduct business online.

Phishing scams are attempts by cyber attackers to obtain private information such as Payment Card Industry information ("PCI"), personally identifiable information ("PII") or protected health information ("PHI"). Phishing scams come from multiple sources such:

- Emails from seemingly legitimate sources (banks, utilities, cellphone/cable providers, stores etc.)
- Phone calls with apparently legitimate numbers that don't match the name of the caller
- Text messages that typically have a tiny web address in them, such as a bit.ly address
- Calls from the "IRS" telling you that you are about to be arrested
- Calls claiming that a loved-one has been kidnapped and will not be released without payment

These will often appear to be urgent in nature.

Ransomware is a particularly damaging type of malware that prevents any access to critical systems. It prevents individuals or a company from using the computer/server or access files (sometimes data, sometimes executables, and often ALL files) unless a ransom is paid. In essence, the files, programs and business activities are held 'hostage' when the hacker changes the passwords, encryption and other forms of 'locking down' executable program files needed to run the business. Examples of ransomware include CryptoWall, Reveton, WannaCry and CryptoLocker.

Ransomware often infiltrates an IT environment as a Trojan Horse malware program disguised as a legitimate file. After installation, the server or computer will likely display a 'lock screen" with a message stating that a ransom must be paid to regain the use of the infected computer or system. The ransom message typically includes instructions regarding how to pay the fine by credit card or bitcoin.

Ransomware is extremely sophisticated and now comes with two distinct components; hunter and malware. The malware is what typically encrypts your files, denying you access. The hunter is a very specific piece of code that searches for every other device connected to the device's network and infects those devices as well.

The mid-2017 WannaCry ransomware attack impacted 100 of the Fortune 1000 businesses, with cost estimates as high as

The Threat of Malware

$350 Million.

Paying the ransom is NOT recommended and hackers do not give guarantees that payment will remove the ransomware from the computer or network servers. The bottom line; you cannot rely on the hackers giving you back your data.

Rogue Security Software is a form of malware that usually shows up when you suddenly get a pop-up window on your screen, advising you that you have a security update or alert about malware. It looks real and offers you the opportunity to click on a button to remove the threat or to install an update to block future threats. These are almost always phony security tools, specifically designed to entice you to download malware.

Rootkit is a collection of utilities designed to obtain privileged and/or administrative access to computers or networks. One of the most notorious rootkit attacks was uncovered in 2005, when a rootkit copy-protection tool was placed in Sony BMG Music Entertainment. Every time a customer bought and copies a CD from Sony, the rootkit was surreptitiously installed on the user's system. This rootkit allowed for full, external access to all files.

Spam primarily refers to unwanted emails. While unwanted emails are usually just a nuisance, opening and clicking on embedded links in these emails will often go to websites that will download and install malware on your device.

Spyware can gather data from a user's system without the user knowing it. The information retrieved can include web pages that a user visits, email messages, user names, passwords, credit card information and other private identity-based data such as telephone number, address, social security number, birthdate, and banking information. If not discovered and disabled, the software can transmit this data to another computer over the internet – typically, the hacker's computer.

Spyware, just like viruses, can be installed when you open an email containing malicious software or when downloading applications with the malicious program attached. Because spyware is intended to be 'stealth', most people don't discover the infiltration unless caught and eliminated by an anti-virus security program.

The Trojan Horse. As legend goes, when the Greeks could not penetrate the heavily guarded city of Troy, Greek soldiers brought the people of Troy a large wooden horse as a peace offering. Once inside the city walls under the shield of nightfall, the Greek soldiers hiding inside the seemingly harmless gift jumped out of the horse and took over the city.

In the computer world, Trojan Horse software programs disguise as regular programs such as disk utilities, games and even anti-virus applications. When double clicked to open or run the program, it starts writing over certain parts of the hard drive, corrupting the data. Although Trojan Horse programs don't replicate themselves, they can attach to a virus file that can spread to multiple computers or servers over a network if the systems are not partitioned or segregated with sufficient firewall protection.

Virus is a generic name for malware that causes havoc on a computer's hard drive by corrupting files, deleting files or directory information.

Worms have two very different definitions. One refers to a computer virus and the other is an 'optical storage technology'. We will be describing the computer virus worm, as the optical storage technology is not a security or malware threat, but stands for "Write Once Read Many", such as a CD or DVD.

The Worm computer virus is not dissimilar to worms that tunnel through dirt. Computer worms tunnel through the computer's memory and hard drive to replicate itself, but does NOT alter any files on your machine. However, the damage is caused when the worm replicates itself so many times that they take up all the computer's memory and hard disk space, causing the system to run very slowly, and inhibiting the user's ability to access files, save or create new files, until the worm is eradicated.

Worms are hard to detect because they are usually invisible files and go unnoticed until the computer starts to exhibit performance issues or an anti-virus program detect the intrusion.

What to do: **The best way to address the malicious IT breaches is to prevent them by protecting your personal devices,**

computers, servers, and networks or have a quick and easy way to recover from the attack.

- Install Antivirus and anti-spyware utilities on the devices/hardware that will seek and destroy the malicious attack programs.
- Only download files from trusted sources and websites.
- It's always a good idea to run new applications and attachments through the virus scan program before opening, running, or downloading.
- Keep all virus scan and anti-spyware programs current with the latest virus definitions for detecting and eliminating new threats introduced by hackers.
- Computer Operating System ("OS") updates should be installed promptly upon release to patch security holes and keep your computer and network virus and worm free.
- Keep all login names and passwords secured to avoid a physical breach by an intruder.
- **Back up** your system and files daily (or continually, if needed) to an external or cloud based environment to revert back to a saved state before ransomware infected the computer, server or network.
- For businesses, ensure segmentation of applications and systems necessary to keep the business running. Physically partitioning ERP applications, data warehouses, human resource, e-commerce and executable files is critical to contain the damage to a single server or stack.

Why SonMax: SonMax Consulting understands that running the daily operations and growing your business doesn't leave time for the executive team to fully understand and scope the extent of how cybercrimes and malicious viruses will impact the viability of the company. As an executive, your obligation is to protect the core assets of the business. To adequately address this fiduciary responsibility, your organization needs to know how best to assess the endemic risks within the business environment through a **Risk Assessment** for **Data Loss Prevention** and designing an **Incident Response Plan**. *To guard against the loss of critical Intellectual Property and costly disabling business interruptions, being AWARE of vulnerabilities and PREPARED with a Resilient Pre-emptive plan against cybercrime infiltration, you are taking prudent action to protect customers, shareholders, the company reputation, and ensuring corporate viability.*

The first step toward change is awareness.
The second step is acceptance.
- Nathan Brandon

The third step is preparation.
- SonMax Consultants Inc.