Types of Cyberattacks That Threaten Businesses, Part I: Malware and Ransomware

By Ryan Zanoni

The global cost of cyber crime is projected to exceed a staggering $6 trillion by the end of 2021, according to the Official Annual Cybercrime Report by Cybersecurity Ventures. Successfully preventing such attacks is extremely important to businesses of all sizes in terms of security, operations, customer service and retention as well as revenue; for *small* business owners, it can mean the difference between staying financially afloat and permanently losing their spot in the marketplace. It is therefore crucial for all professionals doing web-based work to understand the types of threats that might harm their companies' digital spaces.

Cyberattack Basics

A cyberattack is considered any breach of a computer system by an outside party. It can target individuals, organizations, companies or governments. A common goal of hackers is to steal and take advantage of sensitive data such as credit cards, Social Security numbers or other personal identity details. Small businesses are particularly vulnerable to cyberattacks because they fall into what *Business News Daily* calls a hacking "sweet spot:" large enough to provide valuable information but lacking the security of larger organizations.

However, in the recent past, the world has seen even major corporations assaulted and, in some cases, significantly harmed by cyber criminals. Over the last couple of years, large enterprises with more than 1,000 employees have been the most impacted by cyberattacks: Each breach cost affected organizations an average of 500,000 U.S. dollars in 2020.

The shift from in-office to at-home work has made companies even more vulnerable to these threats. Many employees have been using home broadband connections for both personal and business purposes, increasing the number of locations and access points that hackers can target in order to compromise organizations.

Home networks are often less secure than corporate ones, which has raised major concerns among employers and prompted IT teams to augment their defenses with better identity access management (IAM), ensuring that only designated people have the proper access to the right resources at the right time, as well as enhanced data encryption, managed services and extra authentication where needed.

When approaching cybersecurity, it helps to assume that every business is a potential victim. In doing so, companies can begin to think about their points of digital weakness and respond accordingly. IT professionals are usually helpful in identifying vulnerabilities, such as unintended flaws in computer systems, and then pointing out exploitable features and explaining possible user errors.

With the knowledge of how attacks are possible and the ways in which they've been executed in the past, business owners can effectively protect themselves as well as their employees, customers and partners. To that end, an increasing number of such owners and other professionals have been turning to online education programs to gain an in-depth understanding of cybersecurity and practical training in how to prepare for a cyberattack.

Different Types of Cyberattacks

In this article series, we'll cover a total of seven types of cybersecurity threats; in this first installment, we'll concern ourselves with one of the most well-known ones, which comes in two main varieties. However, it is important to remember that even the overall list of seven types is not exhaustive.

A key element of basic cybersecurity is the awareness that networks and the threats they face are subject to constant evolution and change.

Malware and Ransomware

Among the most common types of cyberattacks, malware and ransomware infect computers in order to steal, corrupt and/or destroy confidential information. Malware comes in many different forms, such as viruses, Trojan horses, worms and spyware, all of which are designed to exploit specific computer functions. Malware can do any number of harmful things, including:

- Delete files
- Collect personal information and share it with third parties
- Record keystrokes and watch users through webcam technology
- Use a single computer to hack other computers
- Disable security settings
- Send spam
- Hijack web browsers

Ransomware is a version of malware that inhibits users' ability to access their computer and demands payment to restore functioning. It has remained a popular type of cyberattack even as newer threats have emerged: According to data from IBM Security X-Force, 25 percent of the attacks stopped or remedied in 2020 from the start of the year to September were linked to ransomware.

Fileless malware and ransomware attacks are especially insidious cybersecurity threats that use existing, approved platforms or software tools within corporate networks, allowing them to circumvent familiar detection controls like file scanning. They often begin with a phishing email, i.e., an authentic-looking but fraudulent communication containing a website link or attachment. When the recipient clicks on the link or file, a program, e.g., Flash, is launched, triggering an administrative tool, such as Microsoft Windows PowerShell, to give the command to download and execute the malware in the computer's memory. Scripts and executable files then carry out the command.

Since the malicious payload is contained within the computer's trusted programs, files and/or tools, the security applications do not detect a threat. This is because of the trust model on which they operate: they're instructed not to monitor these "whitelisted" programs, files and tools. This also means the hackers are not required to build their own framework, allowing them to develop and deploy fileless attacks more quickly than other types.

Real-World Examples

Colonial Pipeline Hack

In May of 2021, hackers from a group known as DarkSide, believed to be Russian, perpetrated a ransomware attack against Colonial Pipeline, shutting down crucial channels for transporting fuel from Gulf Coast refineries to major East Coast markets in the southern U.S. This resulted in a surge in gasoline prices as well as panic buying and fuel shortages.

As Joseph Blount, the president and CEO of Colonial Pipeline, told U.S. senators, the attack was executed through a legacy Virtual Private Network (VPN) system that lacked multifactor authentication — making it accessible by way of a single stolen password without an additional step, such as a text message or hardware token. Such extra steps have become common security measures in more recent software, and the majority of major companies now require this two-factor authentication for all internal applications.

Colonial did not have a plan in place to prevent this kind of attack and ultimately paid the ransom in the cryptocurrency Bitcoin, as instructed by the hackers. While the US government was able to recover $2.3 million worth of the nearly $5 million payment, the market value of the funds dropped greatly when the unit price of Bitcoin fell from $63,000 to less than $35,000.

NotPetya

Another prominent example of this type of cyber crime was the NotPetya breach in 2017, considered the most devastating and costly cyberattack in history. During the war between the Ukraine and separatists loyal to the Kremlin, the Russian GRU, a military spy agency, embedded malware disguised as ransomware that incapacitated multinational companies and *permanently* locked people out of tens of thousands of computers in the Ukraine, the United States, Denmark and India.

The hackers irreparably wiped out data from banks, energy firms, high-ranking government officials and an airport. However, the deceptive virus also encrypted victims' data and would decrypt it only if a ransom was paid, which made it seem as though independent criminals, rather than agents of a nation state, were the perpetrators.

The criminals employed what is called a "watering hole" attack, infecting a website which they knew their targets would visit — a Ukrainian site providing tax and accounting software updates. Their objective was to disrupt Ukraine’s financial system, as stated by Jake Williams, who founded

cybersecurity firm Rendition Infosec. This form of contamination is a tactic that Russian government hackers have used in the past to compromise industrial control system networks.

WannaCry

Earlier in 2017, the North Korean government launched a ransomware attack known as WannaCry, a worm that affected over 230,000 computers running Microsoft Windows in 150 countries around the world. Like NotPetya, the virus effectively held valuable files hostage by encrypting them, so that users were unable to read them; then, the hackers demanded payment in the form of Bitcoin in return for decrypting the files, saying that they would permanently delete the information if the ransom was not paid in three days' time. The attack impacted businesses, individuals and governments, costing billions of dollars and putting lives at risk by preventing people from getting needed medical care.

The criminals exploited a weakness in the Windows operating system with a hack known as Eternal Blue, which was supposedly developed by the U.S. National Security Agency — and later publicized by a different group of hackers. Microsoft produced and distributed a security patch to protect users' computers against the hack two months prior to the WannaCry attack, but many individuals and businesses failed to install the patch before the breach occurred. Thus, their computers were infected, and the perpetrators were able to install a backdoor into their networks.

In response to the cyberattack, Facebook and Microsoft swiftly disabled North Korean accounts. Former Homeland Security Advisor Thomas Bossert credited those companies for their action and implored all American companies to help defend the U.S. and its allies against future cyberattacks, stressing that government and industry must collaborate more than ever before to defend cyberspace.

Lessons and Solutions

General Guidelines

The easiest way to protect against a malware or ransomware attack is to ensure that your computer's firewall security is enabled and that both the firewall and your operating system are updated consistently. This will allow your computer to install patches released by software manufacturers or providers to defend against threats.

Other strongly recommended measures include installing internet security software as well as using a VPN when accessing public Wi-Fi. Multifactor authentication should also be considered a must-have for all networks and internal applications, so that criminals will not be able to break into your system by simply stealing one password. And always remember to safeguard against data loss by backing up your information to an external hard drive or cloud-based system; when using the former, be sure to remove it when the backup is complete so as not to leave it vulnerable to a ransomware attack.

User Accountability

Additionally, users must take responsibility for their digital and online actions and stay hyper-vigilant, so they can detect and report red flags in emails and text messages as well as on websites and social media channels.

By refraining from risky behaviors, such as clicking suspicious links, opening questionable attachments, downloading files from websites that are not trusted and inserting USB drives or other storage devices from dubious sources, business professionals can often avoid malware contamination.

Government Progress in Keeping Businesses Safe

On the government side, agencies have used what they have learned from these cyberattacks to step up their game and better protect companies. Bitcoin seizures, such as the one executed by the US government after the Colonial Pipeline hack, are infrequent, but authorities have enhanced their skills in tracking the flow of digital currency as ransomware has become a greater national security threat, due to the activity of gangs of hackers — many of which are based in Russia.

In another positive sign that the efforts of the US government are working, security research firms have reported that DarkSide announced it is ceasing its operations; the hacking group's statement was further evidenced by the shutting down of its website.

However, experts caution that cyber-defense requires constant vigilance from both government and businesses, as such ransomware groups have a history of disbanding and later reforming to launch attacks under different names.

In the wake of the WannaCry attack, U.S. officials announced that the American government had released specific technical information about North Korean cyber tools and operational infrastructure, and had been coordinating with other nations to reduce North Korea's ability to perform further tests or produce illegal funding. These protective measures are important ways to curb digital threats while hopefully avoiding more severe tactics, such as military combat operations or additional sanctions against already heavily penalized countries like North Korea.

Your Future in Cybersecurity

Because computers affect nearly all aspects of modern business and government, protection against malware, ransomware and all other types of cyberattacks is paramount. For individuals who wish to be part of an exciting field full of opportunities, the Bachelor of Arts, Bachelor of Science or Bachelor of Applied Science in Cybersecurity degree from Eastern Oregon University provides the education and training necessary to face the challenges of today and tomorrow, featuring a curriculum taught by experienced instructors who are real-world industry professionals. Designed for ultimate flexibility, the program allows students to study on their own schedules while still giving them the ability to interact with their professors and classmates.

To learn more, fill out the form located here or call 855-805-5399.