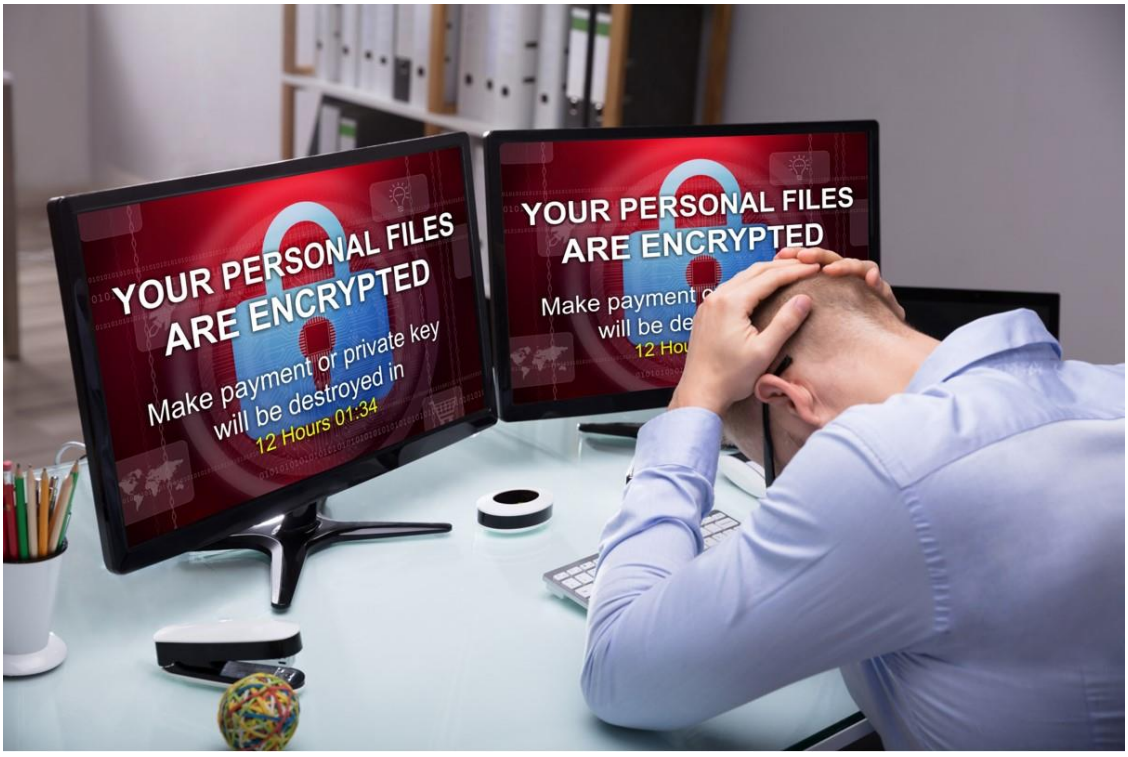
Electrosoft

# TECHNOLOGY REPORT:

# MALWARE AND RANSOMWARE




**Prepared November 9, 2022**

# INTRODUCTION

Malware is any kind of malicious software that is installed on a computer or mobile device that surreptitiously compromises its integrity. Malware can take many forms including ransomware, adware, botnets, rootkit, spyware, trojan, virus and worm, among others.

The Federal Bureau of Investigation (FBI) advises that individuals can "unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware." Once downloaded, the ransomware typically works in one of two ways. Cybercriminals either lock users out of their device or prevent them from accessing their files. The FBI indicates "more menacing versions can encrypt files and folders on local drives, attached drives and even networked computers."

Upon encryption, the hackers demand a ransom, usually in the form of bitcoins, to return control of the device, network or data to the organization. Typically, they establish a payment deadline, often accompanied by a countdown device. Deadlines and frozen operations serve as powerful incentives to pay. Additional leverage arises from threats to make exfiltrated data public.

Ransomware-as-a-service (RAAS) has recently come into being as a business model. It operates much the same as software-as-a-service. For a subscription fee or a designated percentage of any ransoms payments received, ransomware "organizers" allow "affiliates" to use their tools to carry out their extortion activities.

# THE THREAT LANDSCAPE

In the past, cybercriminals were lone wolves who enjoyed the sport of gaining unauthorized systems access. If a ransom were demanded at all, it usually was a minimal amount. Today, cybercriminals are employed by sophisticated organizations staffed with a full complement of C-suite executives, software developers, market analysts, customer relations specialists and others. Their sole mission is to extort as many ransoms as possible. Notably, these groups often work on behalf of, or in concert with, nation-states such as Russia, China, Iran and North Korea.

Victim selection has evolved into a sophisticated market analysis process that seeks to identify organizations with both the ability and the propensity to pay large ransoms. The existence of

cryptocurrencies is contributing to the growing incidence of ransomware attacks. So, too, is the availability of cyber insurance. Bitcoins are difficult to track, making it harder to identify and prosecute perpetrators. Similarly, as companies look to protect themselves by purchasing cyber insurance, criminals recognize money is readily available to meet their ransom demands.

Kaseya Software Company holds the distinction of being the recipient of the highest ransom ask to date: $70 million from the Russia-linked cybergang known as REvil. Other attacks targeted SolarWinds (Nobelium, believed to be under the direction of Russian intelligence), New York City Metropolitan Transportation Authority (by a group thought to be associated with the Chinese government), Colonial Pipeline (DarkSide, a gang linked to Russia) and JBS (REvil).

In 2022 so far, hackers have targeted many organizations including Nvidia (Lapsus$), RR Donnelly (Conti), McDonalds (Snatch), Samsung (Lapsus$), Coca Cola (Stormous), Cisco (Yanluowang) and CommonSpirit Health, Inc. (undisclosed) with varying degrees of reported success.

Every organization is a potential victim. Hackers deem local/state governments, medical centers and universities, among others, as especially attractive targets. The rationale is thought to center around the perceived lack of strength of their cybersecurity measures. When it comes to medical facilities, hackers know these organizations must have access to up-to-date medical records in order to deliver timely patient care. Thus, hospitals are more likely to pay the ransom.


Ransomware attacks are not as pervasive in the federal space because hackers seek to extort money, and the United States government does not pay ransoms or buy cyber insurance. Moreover, the government has enforced the principles of least privilege and least functionality for over two decades, strictly limiting what end users can do online. So, in the rare instance of a ransomware attack against the government, any involvement is typically limited to a single workstation or one network share that is backed up and can be readily restored.

# RESPONSE OPTIONS

Faced with an inability to continue operations, organizations have two options: pay the ransom or refuse to do so. A recent Electrosoft blog, “To Pay or Not To Pay … Is That the Ransomware Question?” explores key issues surrounding this dilemma.

Law enforcement agencies, such as the FBI and Secret Service, recommend that organizations not pay the ransom and immediately report the attack to them. They suggest that paying ransoms

only emboldens others to undertake this illegal activity, thereby increasing the number of attacks. Given the advent of RAAS, a key barrier to entry is removed for many would-be hackers.

Notably, paying the ransom often does not end an organization's problems. Some never recover their data, while others experience only a partial data return. Returned data may be corrupted and unusable, even when the attacker's decryption key is used.

The ransom payment is often followed by secondary ransom demands weeks or months later. In some instances, the cyber criminals create backdoors whereby they can reenter the system and launch a second attack. In other situations, the criminals employ a tactic known as "double extortion." First, the organization pays a ransom to regain control of its network. Later, the attackers levy a ransom demand to prevent posting of exfiltrated data on a leak site and/or its sale on the Dark Web.

# RANSOM RECOVERY

To date, cybercriminals have demanded that ransom payments be made in bitcoin, thinking this currency was untraceable. However, the U.S. Department of Justice (DOJ) is now disabusing cybercriminals of this notion. The FBI recovered $2.3 million of the $4.4 million ransom Colonial Pipeline paid to hackers.

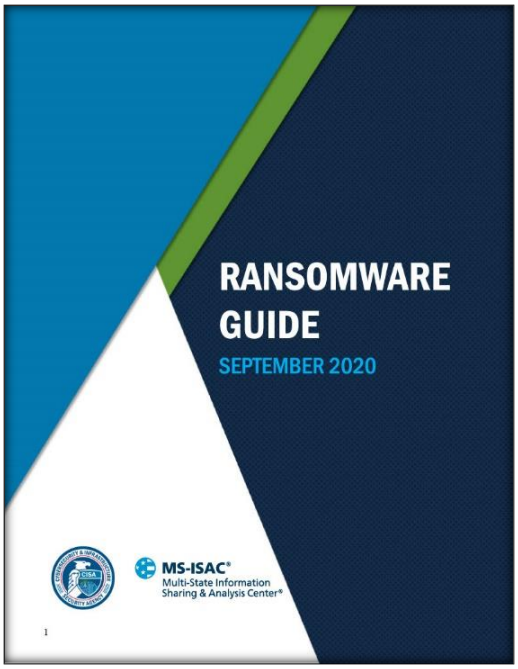
More recently, DOJ successfully retrieved approximately $500,000 of bitcoin ransom payments. A Kansas hospital fell victim to a North Korean state-sponsored group using a new ransomware strain called "Maui" to encrypt its files and servers. The medical center opted to pay the ransom but notified the FBI after doing so; it then cooperated in the investigative effort. The FBI successfully traced the cryptocurrency to China-based money launderers and seized their accounts. Investigators later noted another bitcoin ransom made by a Colorado health care provider and recovered it along with several other victim ransom payments.

# MITIGATION AND DEFENSE

Cyberattacks have plagued organizations for over 25 years. The experts agree that cybersecurity hygiene remains the best way to ensure a sound enterprise security posture. Organizations must be proactive in securing their networks and adopt strict security procedures and compliance standards. The experts also recommend that private sector organizations adopt the federal government's standards of least privilege, least functionality, segmentation and Zero Trust Architecture (ZTA).

A recent Electrosoft blog, "Are Your Shields Up?," discusses a Cybersecurity and Infrastructure Security Agency (CISA) initiative aptly named "Shields Up" that provides updates on cyberattacks and guidance for organizations, corporate executives and individuals to help protect them from

malicious cyberactivity. Notably, the blog also cites the Ransomware Guide, jointly developed by CISA and the Multi-State Information Sharing and Analysis Center, which includes a detailed checklist to follow should a ransomware attack occur.




Essential cybersecurity practices include:

- Inventorying the operating environment and managing risks
- Developing a continuity plan
- Backing up data regularly and verifying the success of each backup/restore effort
- Storing backed up data off-site
- Installing software patches immediately
- Hardening systems using a variety of techniques including segmentation and multifactor authentication
- Installing antivirus and antimalware software
- Filtering emails at the server level
- Training users so they are not susceptible to common ransomware infection techniques
- Determining baseline network activity and analyzing it over a period of months for future monitoring purposes
- Assuring Managed Service Providers and Cloud Service Providers follow strict security protocols

Many of the aforementioned recommendations address ways to apply cybersecurity best practices to extant systems. The experts understand that as organizations modernize their IT systems, cybersecurity must be built into them from inception. Design must incorporate a security perspective, contemplating potential attack vectors and their remediation during system conceptualization. ZTA also is gaining prominence as we move toward the next generation.

# ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

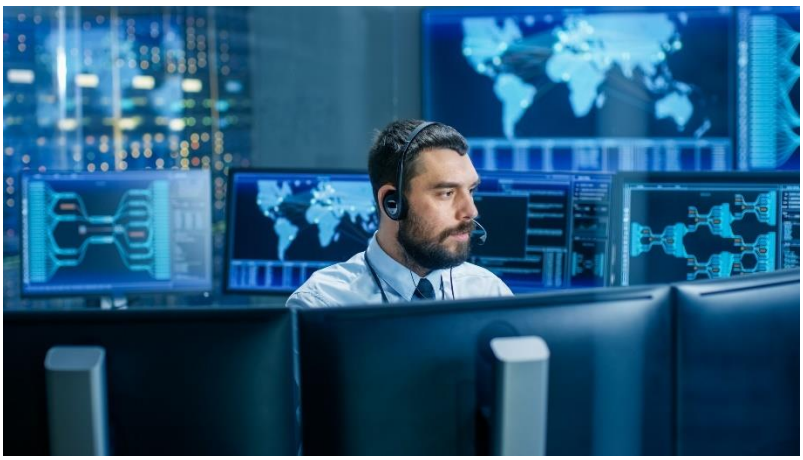
Artificial intelligence (AI) and machine learning (ML) offer new and exciting methodologies for detecting anomalies, unusual activity, malware installation and potential email threats. Their biggest advantage is their ability to incorporate lessons learned into their algorithms going forward. This adaptational quality only serves to heighten their effectiveness.

On the downside, AI and ML can and is being used offensively by the very attackers organizations seek to defend against. The challenge ahead is substantial, as cybercriminal activity is becoming more sophisticated through the support of nation-states such as Russia, China, North Korea and Iran as well as the use of collected ransoms as a funding source for research and development.

# CONCLUSIONS

The Colonial Pipeline attack was an eye opener; it was the first time that individuals from all walks of life directly felt the impact of a cyber incident. Its occurrence reinforced the notion that every organization must fully understand their cyber posture and practice cyber hygiene from the top down. The alternative option is to attempt to recover from an attack, which is difficult in terms of restoring reputation, finances and operations.

Executives must ask: If all our data were lost today, would we be able to function and stay in business? Knowing exactly how a cybersecurity breach could affect an organization enables impact definition in terms of mission accomplishment. Likewise, it is a prerequisite to developing a data breach response plan, a detailed document outlining both a step-by-step response process and the role to be executed by each key player.



Merely creating the plan is not enough, however. It is vital to schedule and hold regular tabletop exercises to practice its implementation. Such drills help identify missing components, prepare staff to execute their assigned roles and isolate any skill/talent gaps for immediate correction.

Ongoing staff training is similarly important. As the FBI indicates, employee actions in the form of opening email attachments, clicking on ads and links, and visiting unsafe websites are the common mechanisms for launching malware and ransomware attacks. Organizations can spend millions on prevention, but people still remain the weakest link. Regular training and skills testing serve to familiarize staff with common tactics, facilitating recognition and avoidance.

• • •

Electrosoft provides mature, innovative technology-based services and solutions to power critical IT programs and protect our country from cybersecurity attacks. To further knowledge sharing and idea development, we recently assembled thought leaders from government, industry and academia to discuss “The Ransomware and Malware Conundrum.” The topics discussed herein reflect both our cybersecurity expertise and content presented during this virtual two-hour technology summit. Readers interested in watching the video of the summit can access it on our website or our YouTube channel. The associated PowerPoint presentation also is available for download in the Resources section of our website.