precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 23 JULY 2023

Today we will look at how ransomware has and can impact government organisations. We will also take a look at some of the methods that we can use to mitigate the risk of becoming a victim of ransomware.

Dr. Ronald Walcott
Managing Director

Welcome to the world of cybersecurity and ransomware! In today's issue we will discuss the digital age, where technology plays a vital role in our lives, it is essential to understand the importance of protecting our digital assets and information from malicious threats. Cybersecurity is the practice of safeguarding computers, networks, and data from unauthorized access, damage, or theft. One of the most prevalent and concerning threats in the cybersecurity landscape is ransomware. Ransomware is a type of malicious software that encrypts files and demands a ransom payment in exchange for their release. In this conversation, we will explore the impact of ransomware, its effects on government infrastructure, and the measures taken to combat this growing threat. So, let's dive into the world of cybersecurity and ransomware to better understand how we can protect ourselves and our digital environments.

HERE ARE FOUR TYPES OF RANSOMWARE:

1. Encrypting ransomware: This type of ransomware encrypts the victim's files, making them inaccessible until a ransom is paid. It typically displays a message with instructions on how to pay the ransom and regain access to the files.
2. Locker ransomware: Locker ransomware locks the victim out of their entire system, preventing them from accessing any files or applications. It often displays a full-screen message demanding a ransom to unlock the system.
3. Master boot record (MBR) ransomware: MBR ransomware infects the computer's master boot record, which is responsible for starting the operating system. It can render the system unbootable, displaying a ransom message when the computer is turned on.
4. Mobile ransomware: As the name suggests, mobile ransomware targets mobile devices such as smartphones and tablets. It can lock the device or encrypt files, demanding a ransom for their release.

It's important to note that these descriptions are general and there may be variations or new types of ransomware that emerge over time. It's always advisable to stay vigilant and take preventive measures to protect your devices and data from such threats.

In this Issue:

Government organizations can be significantly impacted by ransomware in several ways:

1. Disruption of critical services: Encrypting ransomware can paralyze government systems, leading to the disruption of critical services such as healthcare, emergency response, transportation, or public utilities. This can have severe consequences for public safety and well-being.
2. Financial losses: Governments may incur substantial financial losses due to ransom payments, recovery efforts, and system repairs. Additionally, the downtime caused by ransomware can result in lost productivity and revenue.
3. Compromised sensitive data: Government organizations handle vast amounts of sensitive data, including citizen information, classified documents, and national security data. If ransomware successfully encrypts this data, it can be permanently lost or fall into the wrong hands, potentially leading to identity theft, espionage, or other security breaches.
4. Damage to reputation and public trust: Ransomware attacks on government organizations can erode public trust and confidence in the government's ability to protect sensitive information and provide essential services. This can have long-lasting effects on the reputation of the government and its ability to govern effectively.
5. Potential for political manipulation: In some cases, ransomware attacks on government organizations may be politically motivated, aiming to disrupt government operations, influence public opinion, or gain leverage in negotiations. This adds an additional layer of complexity and potential harm to the affected government.

Here are some ways in which government organizations can mitigate the risk of becoming a ransomware victim:

1. Regularly update and patch systems: Keeping operating systems, software, and applications up to date with the latest security patches is crucial. This helps address vulnerabilities that ransomware may exploit.
2. Implement robust cybersecurity measures: Deploying strong firewalls, intrusion detection systems, and antivirus software can help detect and prevent ransomware attacks. Additionally, using advanced threat detection technologies and employing secure email gateways can help filter out malicious emails and attachments.
3. 3. Conduct regular employee training: Educating employees about the risks of ransomware and providing training on how to identify and avoid phishing emails, suspicious links, and malicious attachments is essential. Employees should also be aware of safe browsing practices and the importance of strong passwords.
4. 4. Backup data regularly: Regularly backing up critical data and storing it offline or in a separate network can help mitigate the impact of a ransomware attack. This ensures that even if data is encrypted or locked, it can be restored from a secure backup.
5. 5. Implement access controls and least privilege principles: Limiting user access to only what is necessary for their roles can help minimize the spread of ransomware within the organization. Implementing strong access controls and following the principle of least privilege can help contain the impact of an attack.
6. 6. Develop an incident response plan: Having a well-defined incident response plan in place can help government organizations respond effectively to a ransomware attack. This includes steps for isolating infected systems, notifying appropriate authorities, and restoring systems from backups.
7. 7. Engage in threat intelligence sharing: Collaborating with other government organizations, industry partners, and cybersecurity agencies to share threat intelligence can help identify and respond to emerging ransomware threats more effectively.

Remember, while these measures can significantly reduce the risk of becoming a ransomware victim, it's important to stay vigilant and adapt to evolving threats by staying informed about the latest cybersecurity best practices and technologies.

Upcoming Events

ISMG ENGAGE
August 1st, 2023
Seattle

BLACK HAT
August 5th, 2023
Las Vegas

ISMG ENGAGE
November 9th, 2023
Washington D.C.

Frequently Asked Questions:

WHAT IS RANSOMWARE?
Ransomware is a type of malicious software that encrypts files or locks a user out of their system, demanding a ransom payment in exchange for restoring access.

WHAT HAPPENS IF I PAY THE RANSOM?
There is no guarantee that paying the ransom will result in the restoration of your files or access to your system. It's also important to note that paying the ransom may encourage further criminal activity.

HOW CAN I PROTECT MYSELF FROM RANSOMWARE ATTACKS?
To protect yourself from ransomware, it's crucial to regularly update your operating system and software, use strong and unique passwords, be cautious of suspicious emails or attachments, and regularly back up your important files.

CAN ANTIVIRUS SOFTWARE PREVENT RANSOMWARE ATTACKS?
While antivirus software can help detect and block known ransomware strains, it may not be able to detect new or evolving variants. It's important to complement antivirus software with other security measures and best practices.

What should I do if I become a victim of a ransomware attack?
If you become a victim of a ransomware attack, it's recommended to disconnect from the network, report the incident to law enforcement, and seek assistance from a professional cybersecurity firm to assess the situation and explore potential recovery options.

Headline News

Ransomware Crypto Payments Poised to Set New Record in 2023

CRYPTO CYBERCRIME FALLS 65% OVERALL, BUT RANSOMWARE PROJECTED TO HIT $899M.

Cryptocurrency is the lifeblood of ransomware gangs, and their illicit use of crypto could hit record numbers this year. While overall crypto proceeds, including from crimes such as scams, fell dramatically over the past year, ransomware funds are expected to hit $899 million in 2023.

But ransomware-related funds continue to grow in 2023, the researchers said. Attackers extorted $175.8 million more in 2023 than they did during the same period in 2022.

Cybercriminals focused on big-value attacks, increasing the number of both very large and very small attacks and extorting at least $449.1 million through June this year. If the pace continues, they are likely to extort $898.6 million by the end of the year, trailing only 2021's $939.9 million.

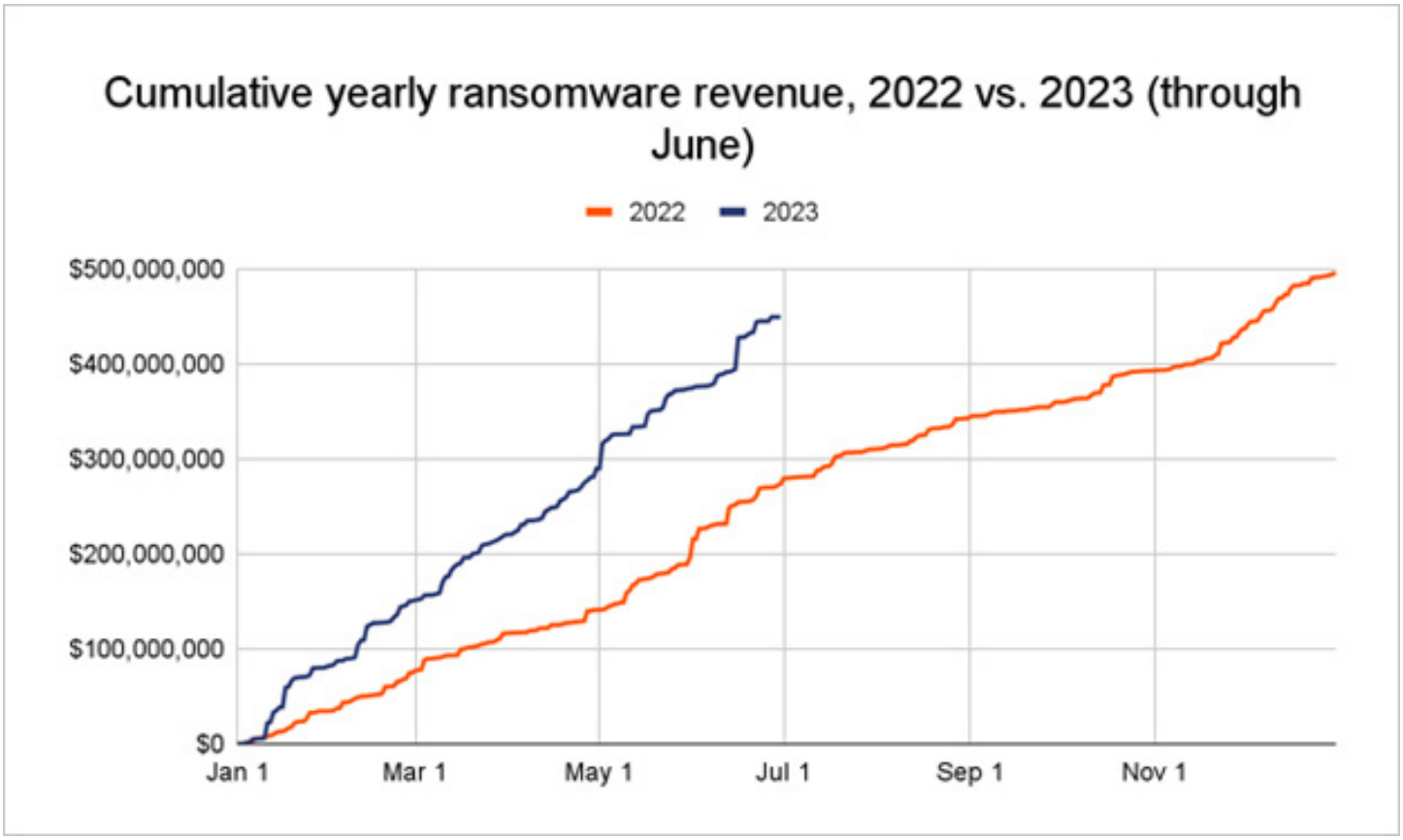
"Big game hunting - that is, the targeting of large, deep-pocketed organizations by ransomware attackers - seems to have bounced back after a lull in 2022," Chainalysis said. The rebound is seen in payments and attacks.

"The payment size distribution has also extended to include higher amounts compared to previous years," the company said.

For instance, Clop had an average payment of $1.7 million and a median payment of $1.9 million, while BlackCat had $1.5 million and $305,585, respectively. Dharma had $265 and $275, and Phobos had $1,719 and $300.

Amateur hackers typically use low-level ransomware-as-a-service Dharma and Phobos to attack smaller targets in "spray and pray" attacks. They use sophisticated strains such as BlackBasta and Clop to hit bigger organizations for more money.

Both types of strains, the researchers said, have been more active in 2023 than last year.



Ransomware-related revenue in 2022 and the first half of 2023 (Image: Chainalysis)

Cybersecurity and incident response firm Kivu told Chainalysis that a notable shift occurred in 2023 in ransomware payment size patterns. The shift aligns with the "growing number of extremely high initial demands, ranging in the tens and hundreds of millions of U.S. dollars," said Kivu General Counsel and Risk Officer Andrew J. Davis.

Factors such as improved cybersecurity and data backup practices by large organizations, law enforcement efforts, increased availability of decryptors, and sanctions against services offering cashout services to ransomware gangs are helping to mitigate attacks to some degree, Davis said. The trend of companies opting to not pay ransom also continues.

"But the nonpayment trend may be prompting ransomware attackers to increase the size of their ransom demands, perhaps with the intention of squeezing the most money possible out of the firms still willing to pay ransom," he said.

The threat actors are also resorting to extreme extortion techniques, such as harassment of employees from victim firms who have not yet paid, he said.

In contrast to ransomware, cyber scams declined the most, and crypto scammers made $3.3 billion less this year than they did in 2022.

The market pullback is a key factor, but not the only one, according to Chainalysis.

"Transaction volumes are down across the board, but declines are much less severe for legitimate services, which have seen just a 28% drop in inflows. In other words, there's been a market pullback, but illicit crypto transaction volume is falling much more than legitimate crypto transaction volume," Chainalysis said.