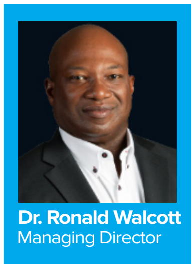
precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 22 JUNE 2023

In this month's newsletter issue, we will be diving into Ransomware attacks and discussing the increase in frequency and the different types of these attacks.



Dr. Ronald Walcott
Managing Director

THE MENACE OF RANSOMWARE GROWS

Ransomware, a type of malicious software designed to encrypt and hold data hostage until a ransom is paid, has become a lucrative business for cybercriminals. The past couple of years have seen a sharp rise in ransomware attacks, with high-profile incidents capturing global attention. These attacks not only affect large corporations but also target small businesses, healthcare providers, government agencies, and individuals, highlighting the widespread impact and indiscriminate nature of this cyber threat.

THE EVOLUTION OF TACTICS

Cybercriminals have continually refined their techniques to maximize their chances of success. They exploit vulnerabilities in outdated software, use sophisticated social engineering methods, and often infiltrate systems by targeting unsuspecting employees through phishing emails or malicious links. Once the ransomware takes hold, it spreads rapidly throughout networks, encrypting critical data and causing widespread disruption.

Here are some of the tactics used by hackers/threat actors:

1. **Initial Infiltration:**
   Ransomware attacks typically start with the initial infiltration of a target's system or network. Attackers often exploit vulnerabilities in software, employ social engineering techniques, or utilize malicious email attachments and links. Phishing emails, for instance, are a common method to trick users into downloading malware or providing sensitive information unwittingly.

2. **Encryption:**
   Once the attackers gain access to the victim's system, their primary objective is to encrypt valuable files and data, making them inaccessible to the victim. Ransomware employs sophisticated encryption algorithms to lock files, ensuring that only the attacker possesses the decryption key required to restore access.

3. **Evolution and Adaptation:**
   Ransomware tactics are constantly evolving to overcome security measures and exploit new vulnerabilities. Attackers frequently update their malware to bypass antivirus software, utilize zero-day vulnerabilities, or target specific industries or organizations. They may also employ advanced techniques like spear-phishing or privilege escalation to gain deeper access and inflict more damage.

THE HIGH COST OF RANSOM

The financial consequences of ransomware attacks are staggering. The ransom demands have escalated dramatically, with cybercriminals demanding millions of dollars in cryptocurrency, often Bitcoin, for

In this Issue:

THE MENACE OF RANSOMWARE GROWS

NEW ENTRANTS TO RANSOMWARE UNLEASH FRANKENSTEIN MALWARE

UPCOMING EVENTS

the release of encrypted data. The costs extend beyond the ransom itself, encompassing the expenses associated with incident response, system restoration, legal services, reputation damage, and lost productivity. Moreover, there is no guarantee that paying the ransom will result in the safe recovery of the data or prevent future attacks.

PROTECTING AGAINST RANSOMWARE

While the threat of ransomware attacks may seem overwhelming, there are proactive steps we can take to bolster our defenses:

1. Regularly update software and operating systems: Keep all software, including antivirus programs, up to date with the latest security patches to mitigate vulnerabilities.
2. Implement robust cybersecurity measures: Employ strong and unique passwords, enable two-factor authentication, and use reputable security software to detect and block potential threats.
3. Educate employees and raise awareness: Training employees to recognize phishing attempts, suspicious links, and malicious email attachments can significantly reduce the risk of a successful ransomware attack.
4. Regularly back up data: Create secure backups of critical data and verify their integrity regularly. This practice ensures that, even in the event of an attack, you can restore your systems without succumbing to ransom demands.
5. Develop an incident response plan: Prepare for a potential ransomware attack by developing a comprehensive incident response plan that outlines steps to mitigate damage, communicate with stakeholders, and restore systems effectively.

UNITING AGAINST RANSOMWARE

Fighting the ransomware menace requires a collective effort. Governments, law enforcement agencies, cybersecurity firms, and technology providers must collaborate to combat this threat. Improved information sharing, stringent regulations, and the development of cutting-edge cybersecurity technologies will be vital in defending against these attacks and bringing the perpetrators to justice.

Upcoming Events

ISMG ENGAGE
August 1st, 2023
Seattle

BLACK HAT
August 5th – 10th, 2023
U.S.A

ISMG ENGAGE
November 9th, 2023
Washington

Frequently Asked Questions:

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software that encrypts a victim's files or locks their computer systems, rendering them inaccessible until a ransom is paid to the attacker. It is designed to extort money from individuals, organizations, or businesses.

HOW DOES RANSOMWARE INFECT A COMPUTER OR NETWORK?

Ransomware can enter a computer or network through various methods, including phishing emails, malicious downloads, drive-by downloads from compromised websites, or exploiting vulnerabilities in software systems.

WHAT HAPPENS WHEN A COMPUTER OR NETWORK IS INFECTED WITH RANSOMWARE?

Once ransomware infects a computer or network, it encrypts files or locks the system, making them inaccessible. Victims typically receive a ransom note that outlines instructions on how to pay the ransom to obtain the decryption key or regain access to their files or systems.

SHOULD I PAY THE RANSOM DEMANDED BY RANSOMWARE ATTACKERS?

It is generally advised not to pay the ransom demanded by ransomware attackers. Paying the ransom does not guarantee that you will regain access to your files or systems, and it may encourage further attacks. Instead, it is recommended to report the incident to law enforcement and seek assistance from cybersecurity professionals.

Headline News

New Entrants to Ransomware Unleash Frankenstein Malware

Opportunistic, Less Sophisticated Hackers Test Limits of the Concept of Code Reuse. Ransomware hackers are stretching the concept of code reuse to the limit as they confront the specter of diminishing returns for extortionate malware. Users are more reluctant to pay even as opportunistic entrants, perhaps less sophisticated than their predecessors, join the market and show less willingness to abide by the ransomware trade-off: money for system restoration.

At the beginning of the year, experts who work with victims and track the cybercrime ecosystem, including via cryptocurrency flows, reported seeing fewer ransoms being paid and less being paid on average when victims did pay.

Cyber insurer Corvus reported that the percentage of its policyholders who paid a ransom dropped from 33% in 2021 to 28% in 2022. Ransomware incident response firm Coveware reported that for victims it assisted, 41% shelled out in 2022 versus 79% in 2019.

That constricting market - the result of hardening attitudes toward mainly Russian extortion groups and cyber defender activity - isn't deterring new actors from attempting to cash in on the shrinking bonanza. In their haste to make money, some new players are picking over the discarded remnants of previous ransomware groups, cobbling together ransomware rather than going through the trouble of coding bespoke crypto-locking software.

Call it Frankenstein ransomware, said Allan Liska, principal intelligence analyst at Recorded Future. Victims are getting hit by malware built by attackers using bits of stolen or leaked code. Liska said that technically speaking, it should be Frankenstein's monster - he of the grave-robbed bits jelled together - but you get the drift.

The ESXiArgs malware being used to target VMware systems starting in February is one such monster, borrowing a "ransom note from one ransomware, the encryption scheme from another ransomware, kind of put together to make a new ransomware," Liska told me at the recent RSA Conference in San Francisco.

"A lot of what we're seeing in terms of new ransomware variants are really just stolen code that's being repurposed by another ransomware guy," he said.

Other newcomers embracing this approach include Rapture, which appears to have adapted Paradise crypto-locker source code that leaked in 2021. GazProm, named for the Russian gas giant and with a ransom note featuring ASCII art of Russia's president, uses leaked Conti source code. Newcomers RA Group, Rorschach and RTM Locker also use source code from Babuk that leaked in September 2021.

Unfortunately for attackers and their victims, mileage varies - not least based on criminals' technical chops.

Malware research site vx-underground has called on criminals to stop wielding the leaked Babuk source code unless they patch the many code-level problems - including an inability to decrypt large file types - that helped precipitate the group's implosion (see: Gouda Hacker: Charges Tie to Ransomware Hit Affecting Cheese).

"If you're going to be a criminal group, do it correctly. Your victims won't be able to recover files," vx-underground said to users of Babuk.

Big Risks: Bad Bugs, Old Code

As ransomware continues, is there anything defenders should be doing more of, to better blunt attacks? Verizon's latest annual data breach report includes a call from Jen Easterly, director of the U.S. Cybersecurity and Infrastructure Security Agency, to employ multifactor authentication much more widely. This will often block outright the use of credentials, which can be easily stolen.

"In particular, it's critical that 'high-value targets' like system administrators and software-as-a-service staff use phishing-resistant MFA," Easterly wrote.

Source: www.databreachtoday.com/blogs