RANSOMWARE ATTACKS EXTORTING SIZEABLE RANSOMS CONTINUE AS PREDOMINANT CYBER ISSUE

Ransomware developers and affiliates have been telling victims they must pay the ransom or stolen data and internal company secrets will be publicly released. Unfortunately, not everyone has been a believer. Six and seven-figure demands have become routine among ransomware attacks with the average ransom payment in quarter two of 2020 reaching $178,254, a 60% leap from the $111,605 average in quarter one according to the Coveware Quarterly Ransomware Report.[1]

"Credit unions need to be looking out for ransomware techniques. These cyber attacks have no boundaries and are truly a global issue," reports Carlos Molina, Senior Risk Consultant at CUNA Mutual Group. "Ransomware has grown in frequency and severity significantly. The average ransom payments have climbed exponentially in the last few years."

Ransomware payments in 2019 were three times as large as 2018 payments and four times as many extortion demands were paid in 2019 versus 2018, according to incidents reported to Beazley. In fact, ransomware claims increased 239% and the total cost of ransomware payments has increased by 228% from 2018 to 2019.[2]

According to Derek Laczniak, Director of Cyber Liability at M3 Insurance, "Ransomware developers threatened to release stolen data in the past. However, now with the actual release of confidential information, credit unions need to treat these attacks more like data breaches. Business interruption from these events has become a regular occurrence leaving both reputational and financial impacts."

How does Ransomware work?

Ransomware is a malicious software that restricts access to an infected machine, usually by systematically encrypting files on the system's hard drive. Then the cyber-criminal demands payment of a ransom in exchange for the key or keys to decrypt the data. Ransomware can be devastating.

The most identified infection points used to deploy ransomware:

- Phishing emails
- Corrupt attachments
- Weak or poorly secured remote desktop protocols (RDP)
- Unpatched system vulnerabilities and untimely anti-virus updates
- Extensive reuse of passwords
- Lack of multi-factor authentication

Molina points out more criminal effort is being placed towards remaining undetected on a breached network. The time that exists between the first execution of malware and its discovery inside the network is commonly referred to as dwell time. "Increased dwell time provides threat actors with opportunities to escalate hijacked privileges while searching for data caches of sensitive information that can be exploited," said Molina. The average dwell time is 43 days for ransomware according to an Infocyte report.[3]

There has also been a significant increase in criminals who purchase ransomware kits on the dark web, launch attacks in the hope of getting some payment, and care little about the data restoration experience of their victims.

"Ransomware code on a reseller distribution network is a very lucrative business for cybercriminals. The availability of free, do-it-yourself ransomware-as-a-service (RaaS) kits, and cheap attack ingredients has pushed the barrier to entry extremely low and deep technical expertise is no longer really needed." according to M3's Laczniak. "It is also possible that the increase of RaaS usage is related to the economic impact of the pandemic driving more financially-stressed individuals towards a career in cybercrime."

"There's no foolproof way of preventing ransomware attacks from occurring; however, all too often ransomware can be avoided with the right IT security and risk management procedures," adds Molina. "Proactive prevention is the most effective for credit unions."

Key Prevention Tips

- Keep all systems including hardware, mobile devices, operating systems, software, cloud locations, and content management systems (CMS), patched and up to date. If possible, a centralized patch management system should be used.
- Activate two-factor / multi-factor authentication (2FA/MFA) on all systems — including managed service provider software platforms, administrator systems, and end-user systems wherever possible.
- Backup data regularly and verify the integrity – ensure backups are not connected to the computer or networks that are being backed up (i.e. securing backups in the cloud or physically storing offline).
- Apply the principles of least privilege and network segmentation in which an end user should be given only the privileges necessary to completes tasks related to their role in the credit union. If an employee does not need an access right, the employee should not have that access right.
- Provide frequent social engineering and phishing training to employees so they are your first line-of-defense. Reminders to not to open suspicious emails, not click on links or open attachments contained in such emails, and to be cautious before visiting unknown websites should be made regularly.
- Vet and monitor third parties that have remote access to the credit union network and connections to third parties. Ensure they are diligent with cybersecurity best practices.
- Credit unions who may facilitate ransomware payments for commercial or consumer members should familiarize themselves with FinCEN's Advisory (October 1, 2020) and list of 10 financial red flag indicators to assist in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks.

Security experts are reporting a potential increase in ransomware attacks for the foreseeable future. Molina emphasizes, "As ransomware tools and deployment methods advance, criminal groups will continue to launch more targeted attack campaigns resulting in increased paid ransom demands and more negative impact to credit unions' reputation and bottom-line."

Need More Info?

To learn more about ransomware, cyber risks, and insurance, go to the Protection Resource Center at cunamutual.com/prc for additional resources and RISK Alerts or contact a Risk Consultant at 800.637.2676 or riskconsultant@cunamutual.com.

Beazley cyber insurance policyholders can also access additional resources at www.beazleybreachsolutions.com (User ID / Password required). In addition, Beazley offers many loss mitigation services at a discount for credit unions.

[1]Coveware, "Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase", August 3, 2020, [2]Beazley, "Beazley's 360° approach to ransomware protection" 2018 - 2019, [3]Infocyte, "2019 Mid-Market Threat and Incident Response Report", Q2, 2019