2020 eBook Series

Rise Above Your Risk

Ransomware Threats

Risk & Compliance Solutions
800.637.2676
RiskConsultant@cunamutual.com

CUNA MUTUAL GROUP

Lock • Encrypt • Demand

A ransomware incident is one of the most disruptive and costly attacks your organization can suffer.

Ransomware Attacks Continue As The Predominant Cyber Issue

TRENDING

"Financial institutions need to be looking out for ransomware techniques. These cyber attacks have no boundaries and are truly a global issue. Ransomware has grown in frequency and severity and extortion demands have risen significantly.

Ransomware claims increased 239% and the total cost of ransomware payments reported by Beazley has increased by 228% from 2018 to 2019.

In the past, they've threatened to release stolen data. 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."

Derek Laczniak, CIC
Director Cyber Liability
M3 Insurance

CUNA Mutual Group and M3 Insurance maintain a strategic relationship to manage brokered commercial products business and to share their expertise and insights with credit unions including on the topic of cyber liability. M3 is one of the top 50 largest brokers of U.S. Business.

Ransomware developers and affiliates have been telling victims that they must pay the ransom or stolen data and internal company secrets would be publicly released. Unfortunately, six and seven-figure demands have become routine among ransomware attacks.

> *"The average ransom payment in Q2 2020 was $178,254, a 60% leap from the $111,605 average in Q1. Average ransom payments have climbed exponentially since 2018."*
>
> Coveware Quarterly Ransomware Report - Q2 2020

In fact, ransomware payments in 2019 were **three times as large** as 2018 payments and **four times more extortion demands were paid** than in 2018, according to incidents reported to Beazley for US based middle market and private enterprise companies.

"What we've been seeing in the underground is threat actors advertising their access to organizations, no matter the industry, and trying to find partners who have ransomware that they can deploy deep in those networks in a very customized fashion," reported Sandra Joyce, senior vice president of threat intelligence at FireEye.

Credit Unions: Be on the Lookout. Manage Risk.

The fact that ransomware attackers can steal as well as encrypt data isn't a new phenomenon but the possibility that sensitive data might be revealed to the world is potentially more damaging than any short-term disruption caused by the malware. Data could include member financial records, employee personal information, termination letters, salaries, and much more.

An expected increase in targeted ransomware attacks that employ a "pay-or-get-breached" methodology. An uptick in **Remote Desktop Protocol (RDP) intrusions and spear phishing** comes as no surprise given the increase in amateur affiliate-based ransomware services; remote intrusion and malware delivery via phishing require little expertise.

Typical Ransomware Scenario

1. Initial compromise of your environment

Remote Access Security

- Microsoft RDP and Remote Desktop Gateway (RDG) can be used to provide remote access to computers and networks.
- RDP/RDG attacks are an attractive and common way for hackers to access systems and steal valuable information from devices and networks.

Phishing / Spear Phishing

- Fraudster or criminal group targets your organization with a phishing campaign.
- Spear phishing targets a select group with something in common – e.g. work or bank at the same organization.
- Malware is successfully delivered to one of your unsuspecting users via a malicious attachment or web link in an email.

2. Malware is installed

- The user opens the attachment and malware is unknowingly installed on the user's PC. The attackers now have a foothold in your environment.
- The hackers undetectably explore your network looking for vulnerable systems and sensitive data. This includes other users' PCs but also servers supporting critical applications and file stores.

3. Ransomware is deployed

- With access achieved, ransomware is spread across your network encrypting indiscriminately.
- The attackers have now encrypted and disrupted a material portion of your business. Some parts of your business are completely disrupted while other parts are partially disrupted.

4. Extortion

- The attackers demand a ransom – up to millions of dollars - for the decryption key.
- The attack can also become public knowledge which causes reputational damage.
- The regulator also wants to understand if there has been a mishandling of customer sensitive data. This means there is a risk of a significant fine.

"The average days of downtime resulting from ransomware that organizations are experiencing material business interruption is 16."

Coveware Quarterly Ransomware Report - Q2 2020

INQUIRING MINDS

Most Identified Infection Points

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

Increased Dwell Time

More effort is being placed towards remaining undetected on a breached network - commonly referred to as dwell time or the time that exists between the first execution of malware and its discovery inside the network.

Increased dwell time provides threat actors with opportunities to escalate hijacked privileges while searching for data caches of sensitive information that can be exploited. The average dwell time is 43 days for ransomware according to Infocyte.

Ransomware as a Service

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 pushed the barrier to entry extremely low. Deep technical expertise is no longer needed to participate in the cyber crime economy.

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 cyber crime.

Managing the Risk of Ransomware

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.

Proactive prevention is the most effective:

- **Patch and Update** - 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. Implement application white-listing and software restriction policies (SRP) to prevent the execution of programs in common ransomware locations, such as temporary folders.
- **Multi-Factor Authentication** - 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. Efforts should also be made to understand the current state of 2FA / MFA strategies, upcoming enhancements and multi-vendor relationships with third parties who are provided credit union network access. MFA provides a critical second source of identity confirmation that can eliminate a vast majority of data breaches within an organization.
- **Data Backup** - 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). Backup systems should allow multiple iterations to be saved, in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure it is properly operational, accessible, and protected. Ransomware has the capability to lock cloud-based backups when systems continuously back up.
- **Apply the principles of least privilege and network segmentation -** The principle of least privilege states that 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. Categorize and separate data based on organizational value and where possible, implement virtual environments with logical separation of networks and data.
- **Engage Employees** - 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 to click on links or open attachments contained in such emails, as well as to be cautious before visiting unknown websites should be made regularly. Hold employees accountable for not following policy.
- **Monitor Third-Parties** - 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.
- **Consider FinCEN's Red Flag Indicators** - 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.

FinCEN's Financial Red Flag Indicators of Ransomware and Associated Payments

FinCEN has identified these financial red flag indicators of ransomware-related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks. As no single financial red flag indicator is indicative of illicit or suspicious activity, financial institutions should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.

1. IT enterprise activity is connected to cyber indicators that have been associated with possible ransomware activity or cyber threat actors known to perpetrate ransomware schemes. Malicious cyber activity may be evident in system log files, network traffic, or file Information.
2. When opening a new account or during other interactions with the financial institution, a customer provides information that a payment is in response to a ransomware incident.
3. A customer's convertible virtual currency (CVC) address, or an address with which a customer conducts transactions, appears on open sources, or commercial or government analyses have linked those addresses to ransomware strains, payments, or related activity.
4. A transaction occurs between an organization, especially an organization from a sector at high risk for targeting by ransomware (e.g., government, financial, educational, healthcare), and a digital forensics and incident response (DFIR) companies and cyber insurance companies (CICs), especially one known to facilitate ransomware payments.
5. A DFIR or CIC customer receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a CVC exchange.
6. A customer shows limited knowledge of CVC during onboarding or via other interactions with the financial institution yet inquires about or purchases CVC (particularly if in a large amount or rush requests), which may indicate the customer is a victim of ransomware.
7. A DFIR, CIC, or other company that has no or limited history of CVC transactions sends a large CVC transaction, particularly if outside a company's normal business practices.
8. A customer that has not identified itself to the CVC exchanger, or registered with FinCEN as a money transmitter, appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions between various CVCs, which may indicate that the customer is acting as an unregistered MSB.
9. A customer uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.
10. A customer initiates multiple rapid trades between multiple CVCs, especially Anonymity-Enhanced Cryptocurrencies (AECs), with no apparent related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.

Cyber Service Considerations

Data exfiltration, along with increased ransom demands, continues to become more common and has resulted in ransom payments even where ransomware recovery from backups was possible.

Consider cyber services that can assist with your loss mitigation efforts. Beazley offers many of these services at a discount for credit unions including:

- Ransomware Hardening Assessment from Lodestone Security;
- 25% discount on KnowBe4's anti-phishing tools and training;
- 50% discount on RSA's SecurID Access solution for identity and access management; and
- up to 60% discount on FireEye Email Security.

In addition, CUNA Mutual Group policyholders can receive a 20% discount on OKTA's market-leading multifactor authentication tools (new credit union customers of OKTA only) for both internal and external users of a credit union.

Related Resources

Beazley cyber insurance policyholders can access additional resources at www.beazleybreachsolutions.com (User ID / Password required). BBR resources include interactive online training on phishing and social engineering.

Protection Resource Center

You can also access CUNA Mutual Group's Protection Resource Center (User ID / Password required) at cunamutual.com for exclusive resources to assist with your loss control efforts including:

- Cybersecurity Threat Outlook eBook
- Ransomware Risk Overview
- Ransomware Prevention & Response Checklist
- Partner Perspective: Beazley
- Mobile Device Risks & Security Risk Overview
- Business Email Compromise Risk Overview
- An Employee's Guide to Phishing Emails
- RISK Alerts
- On-Demand Webinars
  - The Assault on Authentication
  - Cybersecurity Threat Outlook

To learn more about ransomware, cyber risks, and insurance, go to cunamutual.com or contact a Risk Consultant at 800.637.2676 or riskconsultant@cunamutual.com.

Risk & Compliance Solutions • 800.637.2676 • riskconsultant@cunamutual.com

Data presented in this overview is derived from incidents reported to Beazley in 2019 according to the Beazley 2020 Breach Briefing. The website / resources at beazleybreachsolutions.com are a product of Beazley Insurance Group, which is solely responsible for its content.

This resource is for informational purposes only. It does not constitute legal advice. Please consult your legal advisors regarding this or any other legal issues relating to your credit union. CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates. Cyber policies are underwritten on an admitted basis through Beazley Insurance Company, Inc., located at 30 Batterson Park Road, Farmington, CT 06032, are available on a surplus lines basis through Beazley syndicates at Lloyd's, or through other nonaffiliated admitted carriers. CUNA Mutual Insurance Agency, Inc., our insurance producer affiliate, may assist us in placing coverage with these other insurance carriers in order to serve our customers' needs. The website and resources at beazleybreachsolutions.com are a product of Beazley, which is solely responsible for its content.

800.637.2676 | cunamutual.com
P.O. Box 391 | 5910 Mineral Point Road
Madison, WI 53701-0391

CUNA MUTUAL GROUP