Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cyber Blackmail And Ransomware: Everything Old Is New Again

Law360, New York (June 10, 2016, 11:48 AM ET) --


Kristofer Swanson


Louis Scharringhausen

In a modern-day twist on the criminal traditions of extortion, computer hackers are engaging in extensive blackmail and ransom efforts. In a cyber blackmail situation, hackers obtain sensitive data from an organization and then threaten to publicly disclose it unless a payment is received. In a ransomware situation, hackers plant a malicious program on a corporate network that encrypts data and denies the organization access to its own files until a payment is received. A wide range of businesses, nonprofits and municipalities have fallen victim to these extortion schemes.[1]

These attacks are particularly insidious as organizations must also deal with the possibility that regulated data (personally identifiable information, sensitive personal information, protected health information, payment card industry cardholder data) may have been taken from their networks, thereby triggering potential data breach notification obligations.

Since both cyber blackmail and ransomware threats usually have a short decision window before either the data is disclosed or the decryption key is destroyed, it is important for organizations to develop legal, business, ethical and tactical perspectives on these risks and issues prior to an incident.

This article defines and summarizes critical risk issues, identifies ways to reduce exposure and explains standard steps to make ransom payments via bitcoin or other cryptocurrency.

Cyber Blackmail and Ransomware

In a typical cyber blackmail scenario, hackers obtain inside information from the victim and threaten to publicly disclose it if their financial demands are not met. The inside information could include trade secrets, insider financial data, or allegations of an embarrassing nature. The victim is notified and given just enough evidence to reasonably confirm that the hackers actually possess the information that they claim.

In a typical ransomware scenario, a malicious software program encrypts files on a computer, network folders and/or backups (if they can be accessed from the infected computers), making the data unavailable for the victim's ongoing business and operational purposes. The hackers store a key to decrypt the files, which is not released until the ransom is paid. If the ransom is not paid within the initially specified time frame, the hackers may threaten to permanently destroy the decryption key as a way to increase pressure on the victim organization.

In both cases, the hackers usually demand payment in a cryptocurrency (such as bitcoin), which allows for the transfer of funds in an untraceable and nonrecallable method.

How Do These Attacks Unfold?

Though hackers have been known to leverage unpatched vulnerabilities in software and operating systems to gain initial access, attacks are more often crafted to exploit the target's own employees, as they are often the weakest link from a security perspective. In a method called "spear phishing," for example, hackers use specific information about employees and/or the organization to craft emails that appear legitimate. However, these emails may contain unauthorized program files, macro-enabled Microsoft Office files, or download links that point toward obscured malicious software.

Once the malicious software is downloaded and executed by the unsuspecting individual who clicks on the attachment or link, the installed software allows hackers to quickly identify additional targets inside the victim's network. Hackers may load malicious programs such as a key loggers (i.e., a program that records keystrokes to capture passwords), remote administration tools ("RATs," which enable a hacker to remotely control a system), memory scrapers (designed to steal passwords stored in active memory), and others. All of these tools are installed with a single goal: to gather intelligence and gain control of systems on the network. Once inside, hackers search for mission-critical systems, such as e-mail servers, file servers, payroll, and backup systems.

In a cyber blackmail scenario, hackers hone in on specific valuable information that an organization or its senior executives wouldn't want publicly disclosed. Once located, this information is copied from the network and uploaded to a concealed Internet location or file transfer protocol (FTP) site. The hackers then send an email with financial demands to the organization, and to provide added credibility to the threat, the email may contain information that only someone inside the organization can validate.

In a typical ransomware scenario, software installed by a malicious link or attachment begins to encrypt files on targeted computers or systems. If online backups are located, they may also be encrypted or deleted to make it harder for an organization to recover encrypted data without paying the ransom. Once the ransomware encryption process is complete, a splash screen appears, demanding payment and providing specific payment instructions, see Figure 1 for an example.

Figure 1: CryptoWall 3.0 instructional splash screen.

Source: SentinelOne.

How Can Organizations Help Prevent an Attack and/or Reduce Its Impact?

On the one hand, the most sobering aspect of long-loitering hackers is the amount of information they can amass. On the other hand, the longer the hackers are present in a network before launching a strike, the more opportunity the target has to detect and thwart the attack.

Prevention and business continuity considerations published by the Federal Bureau of Investigation include:[2]

Prevention Considerations

- Implement an awareness and training program. Because end users are targeted, employees and individuals should be made aware of the threat of ransomware and how it is delivered.
- Patch operating systems, software, and firmware on devices, which may be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege: no users should be assigned administrative access unless absolutely needed; those with a need for administrator accounts should only use them when necessary.
- Configure access controls, including file, directory and network share permissions, with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

Business Continuity Considerations

- Back up data regularly, and regularly verify the integrity of those backups.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware; if you are infected, this may be the best way to recover your critical data.

Other Considerations

- Implement application whitelisting; only allow systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units.

In the Aftermath of a Ransom Incident, What Steps Can Companies Take?

In the event of an attack, computer incident response teams ("CIRT")[3] are typically activated to confirm the nature and extent of the threat. Due to the nontrivial possibility of downstream litigation and/or regulatory scrutiny, many companies structure their response efforts under the leadership of external legal counsel to benefit from the protections against compulsory production that privilege can provide.

In a cyber blackmail event, the clues in the hackers' notification may help determine where the sensitive information came from and what else could be compromised. If the data is only available from inside the corporate data stores, this strongly suggests a compromised IT security situation. The information leak could be from a disgruntled or recently departed employee, so a careful assessment is often conducted to determine if the threat originated from inside the organization. Once the information has been reasonably validated and the event is deemed to be appropriately material, clients typically notify their boards and external auditors, while the response strategy is being concurrently executed.

In a ransomware attack, some or all of the organization's live data is transformed into an unusable state. The CIRT will assess what data is impacted, evaluate backup systems, and determine how current and complete the accessible data is. Any current backup activity will be suspended to prevent overwriting any existing full backups with corrupted information.

In both cases, situational information will affect how the organization responds, and how deeply the board and general counsel may want to be involved. For example, if the majority of encrypted data can be recovered quickly through alternate means, the business benefits of paying ransom may quickly dissipate. In addition, there are important corporate and public policy considerations around the possibility that the attacking group may be indirectly or directly affiliated with terrorist organizations, foreign nation-states, and/or organized crime syndicates. And of course, even if initial payment demands are met, there is no guarantee that the hackers will not eventually release the stolen information, and/or resurface later to activate embedded malware and re-encrypt systems.

Cryptocurrency Explained

Most payment demands are for amounts denominated in cryptocurrency, such as bitcoin, which allows for anonymous and permanent transactions. Cryptocurrencies are virtual currencies where the amount in any wallet's possession is shared with the entire cryptocurrency community in a shared ledger system called a blockchain. The shared ledger is designed to prevent the double spending of cryptocurrency. "Miners" (computers running algorithms) confirm blockchain ledger transactions.

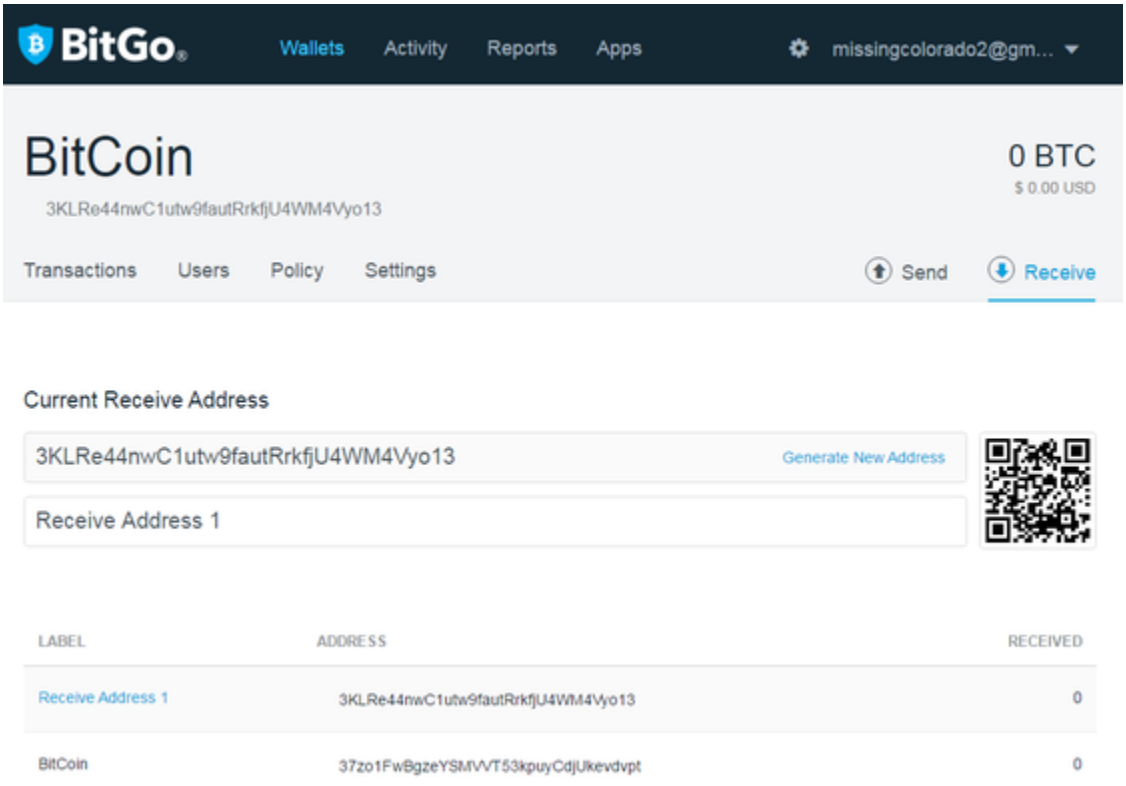
It is important to note that the FBI does not support paying a ransom, but there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect

their shareholders, employees and customers.[4]

Should a business decide to make a payment in cryptocurrency, one must first acquire a “wallet,” which is effectively a string of letters and numbers used as a private encryption key. Most wallet programs are designed for mobile devices, computers or online access, although a limited number of hardware wallets are also available. Unless a web-based wallet is used, the block chain must be downloaded, a process that can take up to a week or more; however, using a desktop wallet instead of a web-based wallet is viewed to be more secure.

Bitgo is an example of a web-based bitcoin wallet that offers links to funding options through www.coinbase.com:

Figure 2: Bitgo.com wallet screen showing receive wallet addresses. The send screen is similar with fields for addresses to send bitcoin to.



Once a wallet is created, it is funded with cryptocurrency at an exchange. Just as one country’s currency can be exchanged for another, government-issued monies (fiat currency) can be exchanged for virtual currency. Each wallet account has the ability to create a temporary “receive” address for the wallet. This is a unique address the exchange service needs to complete the transaction. Each transaction can take several days while the exchange waits for the checks or money orders to clear. There are not many bitcoin exchanges, so it may take up to a week to get a bank account set up for funds transfer.

Cryptocurrency exchanges are neither synchronized nor highly liquid, so prices can fluctuate between and among them, depending upon the trading volume. For this reason, a company may want to consider spreading out a large purchase over several smaller transactions in an effort to keep the exchange price lower.

Large orders may take time to fill as individual bitcoin owners must decide to sell at any given price.

Summary

Ransom and blackmail extortion techniques are not new, but increasing innovations by hackers present new challenges for all businesses. Having a risk-based plan to deal with these attacks, including a robust CIRT, is critical. Preparations to reduce the likelihood or impact of an attack can reduce the ultimate exposure and costs to the organization, including investigative expenses, reputational harm, employee morale and downstream litigation. And from an ethical and values-based perspective, having discussions now with the board and C-suite about how to handle these events should they occur, may help facilitate a more efficient and effective response.

—By Kristofer Swanson and Louis Scharringhausen, Charles River Associates

Kristofer Swanson is a vice president at CRA in Chicago and leader of the forensic and cyber investigations practice. Principal Louis Scharringhausen is a principal in the firm's Dallas office.

[1] Ben Dickson, "How to Deal with the Rising Threat of Ransomware," TechCrunch, April 16, 2016, accessed April 17, 2016, http://techcrunch.com/2016/04/16/how-to-deal-with-the-rising-threat-of-ransomware/.

[2] Ransomware, US Department of Justice, Federal Bureau of Investigation, Cyber Division, https://www.fbi.gov/about-us/investigate/cyber/ransomware-brochure#disablemobile

[3] Per the SANS Institute, the composition of a computer incident response team will depend on the needs and resources of each company, but may include representatives from inside the company – such as senior management, information security, information technology, legal, human resources, public relations -- and external resources, such as legal counsel and independent forensic investigators. (https://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641, accessed May 25, 2016).

[4] See supra note 2.