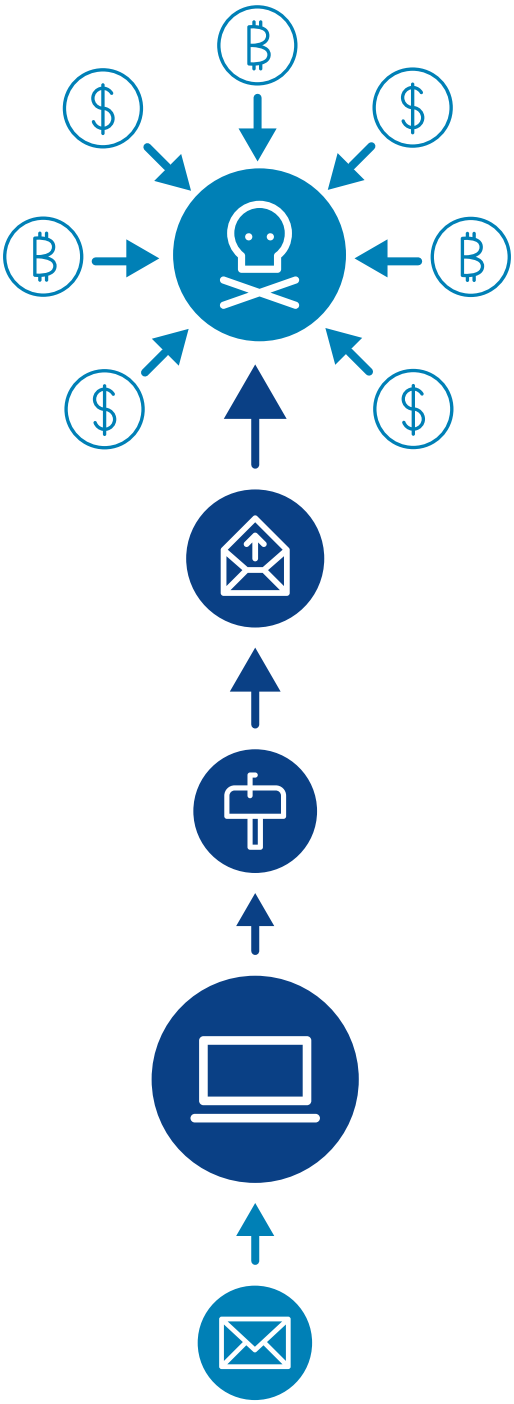
Deloitte.

Taking data hostage: The rise of ransomware

Table of contents

Introduction



It begins much like any other day at the office: you're working away on your computer when you receive an email informing you an invoice has arrived for your department. It directs you to download the invoice using the link provided. Without giving it much thought, you download and open the file. Sometime later, you discover you can no longer access your files and that several copies of a file named "DECRYPT_YOUR_DATA.txt" have been created.

It's a chilling moment. Sensitive files on your computer, and probably on the network you're connected to, have been encrypted. They've effectively been taken hostage in one of the fastest-growing forms of cybercrime: **ransomware attacks.**

Ransomware, as the name suggests, is a malware designed to make a target's data unusable or to prevent access to systems until a ransom – typically in hard-to-trace digital currency - is paid. The scene described above is of a typical ransomware incident, a trap any computer user can fall into. A newer and more sinister development is targeted ransomware, in which individual organizations are pursued and, once infected, might take a couple of months to paralyze a system before demanding a ransom.

Ransomware is becoming highly sophisticated: some recent variants can gain access without connecting to the Internet at all, making its source virtually untraceable. The lucrative and fast pay-off, combined with its stealth and relative anonymity of the transactions, has made this type of cyberattack increasingly attractive to criminals.

Indeed, ransomware attacks have reached epidemic levels across the globe. There have been more incidents in the first half of 2016 than in the past five years combined, and we expect the number to increase exponentially. Their severity has also increased, with more sophisticated campaigns being launched against targets with deeper pockets and more motivation to pay quickly.

Canada is not immune: ransomware attacks have been occurring here for the past three years, with the volume rising sharply in recent months. It now ranks among the top three biggest cybersecurity concerns of Canadian organizations.

Victims are often willing to pay whatever sum is demanded of them to get back to business as soon as possible. It's not unlike families being willing to pay kidnappers whatever is required to release their loved one from captivity. Given the parallels in criminal strategy, it may not be surprising that the methods used by teams dealing with human kidnap incidents can be successfully adapted to a cyber environment. We've found these strategies effective when negotiating with ransomware criminals to gain time, reduce the ransom amount, and resolve the issue quickly.

Before exploring the parallels, it's important to examine what ransomware is and why it's becoming the malware of choice amongst cybercriminals.

A class of its own

Ransomware differs from other types of cyberattacks in that the objective is to make the victim pay money to the perpetrator directly. Other types of malware attacks often take more effort to monetize: stolen credit cards, for example, need to be divided into bundles of certain sizes and sold to different people, eventually working out to about $5 a card.

Ransomware also differs in that the goal isn't to steal data but to deny access to it until money has changed hands. That makes it about availability, whereas other cyberattacks seek to breach confidentiality (stealing personal data, credit card information, etc.) and compromise integrity (as privacy breaches must be disclosed to authorities).

With traditional ransomware, the strategy is to get in, get as much cash as possible, and get out as quickly as possible, because the longer it takes to get the money, the less likely the plan is to succeed. This made it different from the typical cyberattack. But things are changing: targeted ransomware, which is becoming more popular with criminals, plays a long game.

Once this malware has gained entry, it will identify an organization's most sensitive or prized data, corrupt the backups to make them useless, create backdoors in the system to make future infiltrations easy, and encrypt the data all before sending a ransom demand. It could be quietly wreaking this havoc for a couple of months before the victim is even aware of a problem. By then, the organization is on its knees.

Easy profit lures new players, changes the game

For years after the first known ransomware incident, executed in 1989 by way of floppy disks and demanding a US$189 ransom, perpetrators tended to seek a relatively small sum from a wide range of victims, including individuals. While such opportunistic entries are still the typical infection vector, criminals have become more interested in preying on specific organizations. Attractive targets include those with potentially limited cybersecurity resources whose data may be needed in life-and-death situations, such as hospitals. Several were targeted in early 2016, including a Los Angeles health centre that reportedly paid a US$17,000 ransom to regain control of its computer system. The stakes are extraordinarily high—imagine how much might be paid to retrieve a decade's worth of cancer research.

As they've shifted their target sights, perpetrators are also changing their methods. A few years ago, a typical tactic was the drive-by download, a passive approach. Today, attackers are also actively targeting potential victims with social engineering. An estimated 80 percent of ransomware is introduced by downloading macro-enabled Office documents sent by a party mimicking a legitimate source.

Today, the average negotiated ransom is in the $20,000 range, but it can be much, much higher. According to reports, US victims handed over more than US$325 million to the creators of the CryptoWall variant in 2015. The lucrative potential of this malware has attracted more sophisticated criminals, ushering in a new era in which ransomware attacks will likely proliferate further.

Lessons from kidnap-&-ransom services

As we've already noted, through our experience handling ransomware crises for clients, we noticed the paradigms between data and human kidnap-and-ransom situations are similar.

But physically capturing a person and holding him or her until demands are met takes a great deal of planning and creates a good deal of risk for the perpetrators. With ransomware, criminals can reproduce a similar situation by hijacking an organization's prized data without ever having to step outside, thus reducing risk and expense while increasing the potential payday – they can cripple an unprepared organization in a way taking a human hostage never could.

However, given the parallels between these types of criminal acts, we believe it's instructive to look at typical hostage management services/tactics to design a defence plan and negotiation strategy against ransomware:

	Typical human hostage management services	Potential data/systems hostage management services
Prevention	• Assess vulnerability of client (typically, affluent or high-profile individual). • Educate client about the risk, including attack detection and protection.	• Assess the vulnerability of the client (company or organization). • Educate client about the risk, and teach attack detection and prevention. Ensure adherence to a good cybersecurity hygiene routine. • Ensure client has a strategy/ methodology in place to follow closely in case of attack.
Insurance	• Sell insurance to cover ransom, legal fees, consultant fees, loss of business and replacement workers.	• Sell insurance to cover ransom, legal fees, consultant fees, loss of business due to operations slowdown/shutdown, data destruction, damage to reputation.
Crisis management	• Immediate response steps • Engage media relations and communication • Call on-site consultants • Arrange support for family/employer.	• Implement response strategy; follow step by step. • Resist urge to disconnect. • Call on-site consultants.
Negotiation	• Ask for proof of life. • Determine motive (politics or profits?) • Slowly reduce ransom price. • Assess risk of second ransom.	• Ask for proof of attacker's capacity to decrypt the data (e.g., proof of decryption key). • Slowly reduce ransom price. • Assess risk of second ransom.
Debrief	• Conduct compromise assessment. • Offer psychological support. • Profile attacker (gather intelligence for future). • Return to the prevention phase.	• Conduct compromise assessment. • Follow recovery plan. • Profile cyberattacker. • Return to the prevention phase.

Be prepared

As with any malware threat, prevention is the best defence. It's especially important since, unlike other types of malware, contemporary ransomware is very difficult to detect: only a single call – if any – to the Internet is required to launch it. So, start by ensuring you have the right cybersecurity system for your organization. Develop a backup strategy for your critical systems and data. Practice good cybersecurity hygiene, such as keeping up-to-date with all patches, monitoring network activity, and proactively managing permission levels. Train employees to be wary of emails, as social engineering is the top way this type of malware gets into the networks of target organizations.

While prevention is a vital first step in protecting your organization, it cannot eliminate the risk altogether. It's also necessary to prepare for a successful breach by establishing a ransomware strategy with a well-defined protocol. This establishes clear negotiation guidelines you can use to gain more time or follow the right steps to make sure you recover your data and/or prevent another attack. A clear protocol can, in some cases, allow organizations to assess whether their data will be released upon payment; this has not always been case in recent incidents.

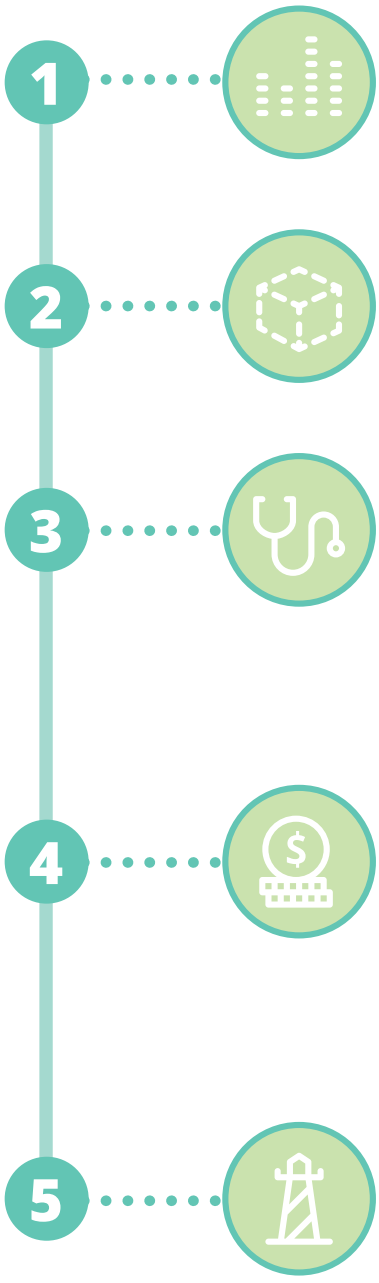
Once this strategy is in place, it's important to follow the steps of the methodology carefully. The first of these should be: "Resist urge to unplug from the network." You lose a tactical advantage if you pull the plug. If the system is still connected, you can watch the ransomware work and see how deeply it unravels. If the system's unplugged, you can't see if the malware's replicated itself, deleted recovery points, or opened a backdoor that will allow access to future infiltrations, which means you won't know if you'll be faced with further extortion sometime down the line.

An organization should also position itself to reduce the likelihood of having to pay a ransom by:

- Using advanced threat intelligence solutions to help you find indicators of compromise and respond to incidents more quickly.
- Implementing multi-layered endpoint security, network security, encryption, and strong authentication and reputation-based technologies. Partner with a managed security services provider (MSSP) to extend your IT team.
- Considering acquiring a retainer with a third-party expert to help manage crises. Implementing an incident management capability ensures your security framework is optimized, with measureable and repeatable processes, and that lessons learned are used to continuously improve your overall security posture.
- Establishing guidelines and company policies and procedures for protecting sensitive data on corporate computers and mobile devices. Regularly assessing internal investigation teams' effectiveness and run practice drills to ensure you have the skills necessary to effectively combat cyber threats.
- Setting up a tripartite agreement with a law firm and a cybersecurity firm. If you're hacked and the cybersecurity advisors you call in find that your organization hadn't taken necessary precautions, their report could be subpoenaed for a lawsuit by stakeholders. With a tripartite agreement, however, the report belongs to the law firm, and as such is privileged.
- Developing a sound backup strategy that uses off-site or cloud-based solutions to enable an effective recovery in the case of a successful ransomware attack.

Data taken hostage? Don't panic

As soon as you realize ransomware may have entered your system, refer to your protocol and follow the steps in sequence. These generally will include, but aren't limited to, the following:



Determine the extent

Find out how many files have been encrypted and how the particular strain of ransomware is affecting your operations. Assess, too, the potential impact to your reputation should the breach be made public.

Isolate the affected systems

Most ransomware is designed to spread through your network as quickly and quietly as possible. Identify which systems have been affected and segregate them quickly to prevent further infection.

Check your backups for infection

Using backups is your best option to restore operations swiftly, but only if the malware hasn't affected them too. Inspect them before you deploy.

Should you pay?

If your network is compromised and you've exhausted your options, such as deploying backups or stalling for time, consult before deciding to pay the ransom. Experienced cybersecurity professionals can negotiate with your adversary to resolve the situation efficiently and quietly. In the meantime, don't refuse to pay since you don't know what the consequences may be; the attacker could destroy the unique decryption key so that you can never regain your data, for example. Tell them you will, but that you need to sort out payment details. This buys you time to follow the steps of your ransomware protocol.

After the incident, improve your prevention strategy

Use the threat intelligence gathered from the attack, establish clear security policies, and educate all your teams.

In summary

Profitable and with a potentially fast payout, ransomware is an attractive tactic that's unlikely to wane in popularity. While large organizations with deep pockets will continue to be prime targets, those that don't necessarily have much money but do have data of a sensitive and/or critical nature – such as matters of life and death – may increasingly find themselves in the crosshairs of criminals.

Like preparing a very affluent person to be kidnapped, minimizing the risk and limiting the potential damage of a ransomware attack begins with having a good cybersecurity system and practicing good cyber hygiene, establishing a solid protocol specific to such incidents, and training everyone how to steer clear of the malware.

No one wants to be locked out their home when the baby's inside. Make sure there's a plan to regain control of your domain before it's necessary.

Ransomware realities

Major disruption:

Ransomware prevents a victim from operating as usual. It may also cascade into privacy breaches, loss of reputation, financial fraud, and infections to other entities in your supply chain.

Tailored attacks:

More sophisticated ransomware is designed to infiltrate and disrupt specific organizations. Using social engineering tactics (tricking individuals with legitimate-looking messages), attackers can gain knowledge of the company's structure to increase the malware's infiltration and damage capabilities to its most important data and backups.

Phishing expeditions:

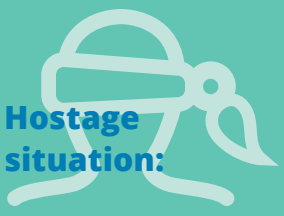
The vast majority of such ransomware is now distributed via phishing email campaigns, or spear phishing, to employees at targeted organizations. Recipients are encouraged to open attached documents, most of with macros. Attackers may also infect a system through ads on legitimate websites, having taken advantage of ad networks with poor security.

A new business model:

Ransomware-as-a-Service, or RaaS, emerged in 2015 as a new threat model. Attackers are re-investing the profits from successful exploits to develop increasingly complex malware and attacks. They may even operate 24/7 hotlines to help victims having technical problems either paying the ransom in bitcoins or decrypting their data.

Monetization guaranteed:

Attackers now seek victims who have the financial means and strong motivation to pay up. Businesses are attractive targets as their incentive to regain control over data and operations can justify the rapid settlement of a ransom payment. And since businesses are not required to disclose to regulators breaches that do not compromise privacy laws – for instance, personal information about clients – then they have a better chance of keeping the incident from going public; paying the criminal to stay quiet.



Hostage situation:

A successful attacker controls the fate of your most important data. Time to respond is limited and the ransom can increase rapidly if no actions are taken. The attackers may destroy the unique encryption key if payment is slow to come.

Learn more

If you have been a victim of Ransomware or would like to learn more, please talk to us.

Cyber breach response has become a multifaceted process that requires One Response, a proactive, coordinated and orchestrated approach. Reach out to us to learn how your organization can implement a One Response approach.

Rob Masse

National Resilience Leader
Partner, Cyber Risk Services

514-393-7003

rmasse@deloitte.ca

Deloitte.

Designed and produced by the Deloitte Design Studio, Canada. - 16-4333M