IBM Security

Ransomware: How consumers and businesses value their data

IBM X-Force® Research

IBM

Click here to start ►

Contents

Executive overview

What would you do if today you found out that cybercriminals had managed to infect your computer with malware that has encrypted all your files? Would you be concerned about saved work? Would you lament the loss of pictures and videos from a once-in-a-lifetime trip, or the forever irreplaceable photos from your kids' early childhood? Would you pay to get them back, and if so, how much are you willing to spend?

Whatever your answer, it's likely to cost you five times that amount.

What if you are in charge of a company server on which all your organization's intellectual property gets locked up by a cyber-extortion gang? What if all the computers in the hospital you manage are encrypted and held hostage by cybercriminals? Will you pay? Attackers are counting on you to do just that!

About X-Force

The IBM X-Force research team studies and monitors the latest threat trends including vulnerabilities, exploits, active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, IBM X-Force also delivers security content to help protect IBM customers from these threats. Threat intelligence content is delivered directly via the IBM X-Force Exchange collaborative platform, available at xforce.ibmcloud.com

Contents

IBM fielded a US-based consumer and business research study to determine the value people place on data and their awareness and knowledge about ransomware. The results are alarming. For instance, despite high levels of confidence in their ability to protect personal devices, 59 percent of consumer respondents have not taken any action in the past three months to protect their devices from being hacked. The survey, which tallies responses from individuals and business executives, provides a clear picture of an overall lack of awareness and preparedness in the face of the rising risk of ransomware attack.

About the research study

This report summarizes the results of a 2016 US-based study fielded by IBM to determine the value consumers and business executives place on data and their awareness and knowledge of ransomware. The survey was designed with Ketchum Global Research and Analytics. Data collection was conducted by Braun Research Inc. for the business audience and ORC International for the consumer audience. The survey population includes:

- 1,021 US citizens aged 18 and older for consumer perspective
- 200 small-business executives (<100 employees)
- 200 medium-business executives (101-999 employees)
- 200 large-business executives (1,000+ employees)

The margin of error for the study for the total business audience is +/- 3.88% at the 95% confidence level (and +/- 5.5% at the 95% confidence level for individual company sizes). The margin of error for the consumer study is +/- 3.07% at the 95% confidence level.

Consumers are far more confident in their ability to protect personal devices than their actions indicate.

Contents

A brief overview of ransomware

Ransomware is a family of computer bugs that are programmed to lock up an endpoint, such as a PC, server, or mobile device, in various ways. Ransomware revokes access to the endpoint itself, or encrypts data on the endpoint, and then asks the victim to pay a ransom to regain control of the data or the endpoint. A ransomware attack can affect an individual or organization anywhere in the world.

Cybercriminals typically use social engineering such as unsolicited email, or spam, to lure victims into opening a malicious attachment. The attachment attempts to exploit a vulnerability in productivity software the user likely possesses in order to allow file execution, in this case ransomware. IBM X-Force has seen a quadrupling of spam volume in the last 23 months; even more worrying is the marked increase in ransomware attachment to spam, up from an average ransomware attachment rate of 0.6% in 2015 to nearly 40% YTD in 2016.

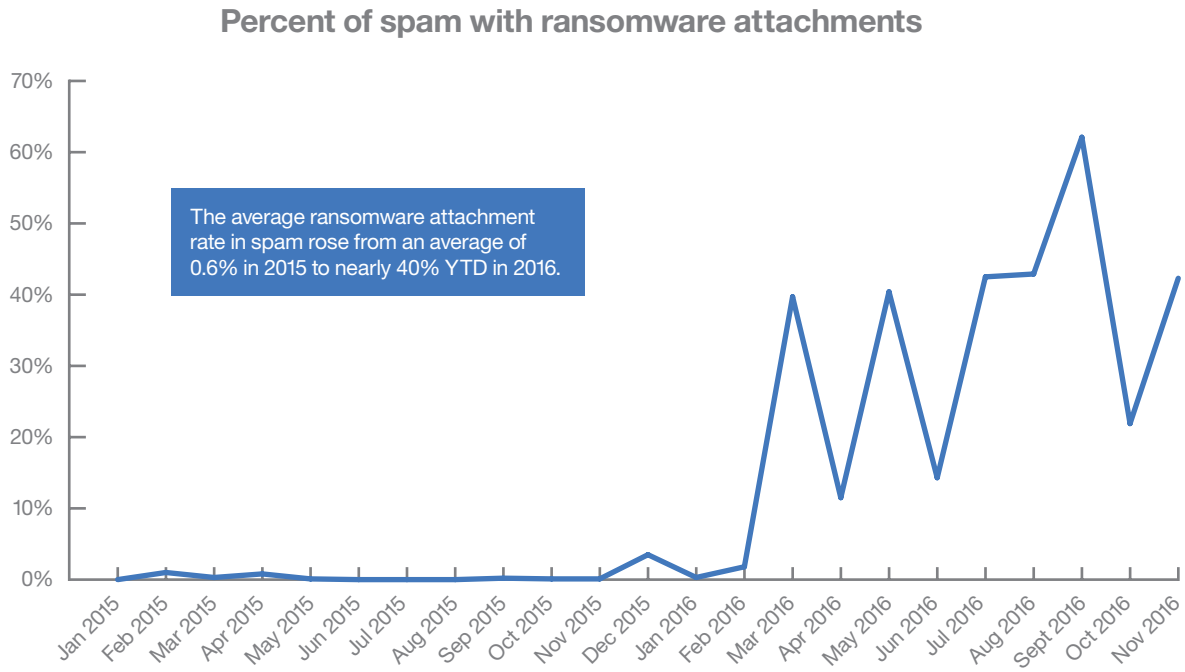

Figure 1. Source: IBM X-Force, 2016

Contents

The ransomware code is designed to scan the file system on the endpoint and find all the locations where the victim keeps files, including shadow copies and backup files and including network repositories and even external drives attached to the endpoint. The files are then encrypted and users are prevented from accessing them.

The key to unlocking the files remains in the cybercriminal's hands until the victim pays a ransom to obtain the key and attempts to restore the files.

Although ransomware has been increasingly rampant only since 2014, the concept dates all the way back to 1989, when PC-locking malcode was snail-mailed to victims on floppy disks. Ransomware has since gained tremendous momentum with improved encryption capabilities exploited by cybercriminals and the growing use of cryptocurrency like Bitcoin.

Victims all around the globe have been receiving on-screen ransom requests averaging $500USD, demanded most often in the form of cryptocurrency. Businesses are now seeing larger-scale ransomware attacks on their servers and networks, along with demands for 4- to 5-digit ransom payments, all the way up to millions demanded in some cases.

Ransomware attacks have been proliferating and becoming much more sophisticated. As a result, consumers and businesses alike are losing large amounts of money to ransomware operators—groups of cybercriminals who emulate legitimate businesses, making them highly efficient and ROI-aware. Europol recently warned that ransomware is one of the biggest online threats affecting consumers and businesses this year. That is unlikely to change in the foreseeable future.

Increasingly rampant ransomware attacks are becoming more sophisticated, and their perpetrators are demanding higher and higher payments from business victims.

Contents

According to US government statistics, ransomware attacks quadrupled in 2016, with an average of 4,000 attacks per day. The FBI reported that in just the first three months of 2016, more than $209 million in ransomware payments have been made in the United States—a dramatic 771 percent increase over a reported $24 million for the whole of 2015. The FBI estimates ransomware is on pace to be a $1 billion dollar source of income for cybercriminals this year.

Startlingly, most targets of this highly prolific threat are completely unaware of its existence. According to the IBM survey, only one-third (31 percent) of consumers have actually heard of ransomware.

The situation is no better on the enterprise side, where most employees are unaware of what ransomware is, or how it can affect the company. Ponemon Institute's 2016 State of Endpoint Report reveals that 56 percent of companies surveyed said they are not ready to fend off ransomware attacks, and just 38 percent said they have a strategy to deal with destructive software.

Consumers surveyed about ransomware

This report summarizes the results of an IBM ransomware survey conducted in the United States. For the consumer segment of the study, we asked over 1,000 individuals in the US about their knowledge of ransomware and, in the event of an attack, their perceived willingness to pay cybercriminals to get their data back.

The survey's goal was to map consumers' awareness about ransomware and their ability to protect themselves from its potential harm. It provided clear insight. Most people are unaware of ransomware. While they are concerned about losing access to their devices or data, they are doing nothing to protect themselves—all while being quite confident that they would know how to respond if the worst-case scenario were to arise.

Big picture: lack of awareness, unfounded confidence

The results show a lack of awareness about ransomware, which may be resulting in little or no action taken to protect devices and data. More than half the consumers interviewed do not take any proactive measures to protect themselves from this type of malware, despite high levels of confidence in their ability to protect personal devices.

Contents

Statistically, responses show:

- Just one-third of consumers (31 percent) have actually heard of ransomware.
- Three-quarters of consumers (75 percent) are confident they can protect personal data on a computer they own, compared to 67 percent for data on mobile or tablet devices.
  - Confidence drops notably for work or school computers (48 percent), cloud storage (48 percent) and smart TVs (42 percent).
- Although confidence levels are relatively high, six in ten consumers (59 percent) have not taken any action in the past three months to protect their devices from being hacked. However, those who are aware of ransomware are more likely to take protective actions (59 percent versus 33 percent).
- The most common preventive action, noted by 71 percent of consumers taking action in the past three months, is to avoid opening suspicious attachments or clicking on links in emails and texts.
  - Other protective measures include regularly changing passwords (59 percent) and avoiding public Wi-Fi access points (48 percent).

Common threat scenarios

On consumer endpoints, ransomware typically does the following:

- **Encrypts all files on the endpoint:** Ransomware can scan the target endpoint or device, find the locations where all files are saved and rapidly encrypt all folders, rendering all data inaccessible.

  The Locky ransomware is one of the more infamous variants encrypting files in 2016, and Jigsaw is ransomware that will delete groups of files over time, the longer the victim delays in paying the ransom (see Figure 2).

IBM Security has already seen cybercriminals actively masking malicious files in emails sent to consumers, disguised as Amazon Black Friday and Cyber Monday deals and package shipment tracking details. When a user clicks on the tracking URL, instead of going to Amazon, they download the Locky Ransomware—which then encrypts all their files, requiring them to pay a ransom to regain access.

Contents

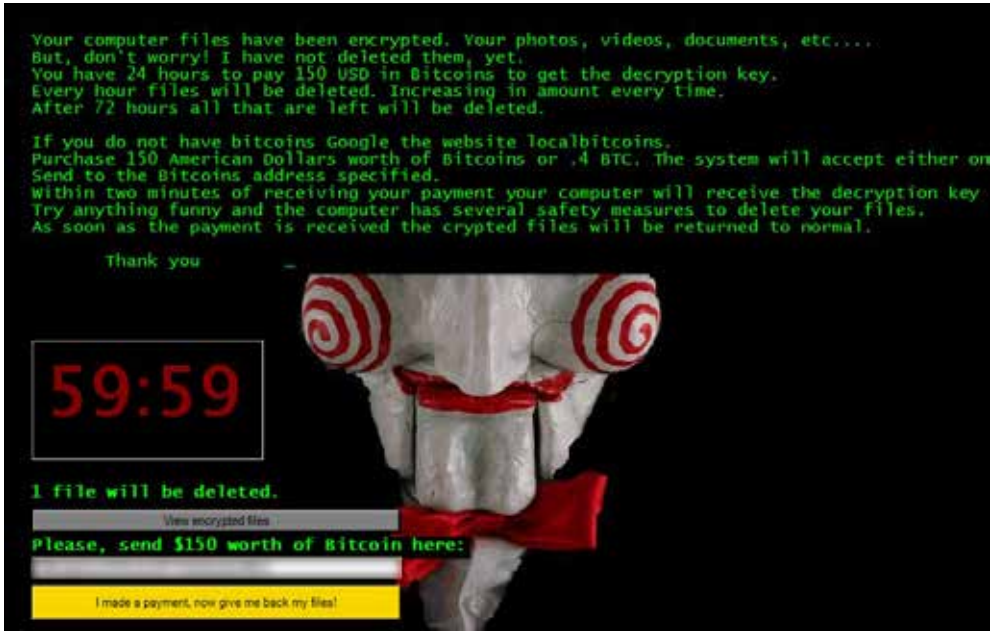

Figure 2. The Jigsaw ransomware's instructions to victims on paying ASAP

- **Locks access to the device itself:** Ransomware can lock access to the device by infecting the master boot record (MBR). The victim can no longer reboot their machine or access the computer until they pay a ransom to have it unlocked. For example, the Petya ransomware overwrites the computer's MBR to achieve this type of restriction.
- **Locks a mobile device** and potentially replicates into a paired smart device, like a smart watch, thereby locking it as well.

Contents

Most meaningful data: the consumers' take

When asked "How important are your health records? How about family photos and personal data?" it turned out that data was not as important to consumers as one might think. The IBM study has found that:

- Over half the consumer respondents would forfeit their health records and family pictures to avoid paying to get them back. The one exception is financial data, for which 54 percent of respondents would pay.
- Millennials, however, valued their data more highly than the overall average. On average, half of them were willing to pay for the return on various types of data.
- Most consumers have not experienced a hacking case, but would be most concerned about online passwords and financial information being compromised. Parents would be particularly concerned about digital photos.
- A majority of consumers (68 percent) do not have personal experience with a data attack or know anyone who has. Consumers would be most concerned if their online account passwords (79 percent), financial information (79 percent), and personal computer access (78 percent) were held for ransom or access was blocked.
- Parents (71 percent) are much more concerned than non-parents (54 percent) about family digital photos being held for ransom or access blocked.

The incident response factor

Who would consumers call to report being infected by a ransomware attack? The FBI urges victims to report infections to federal law enforcement—no matter the outcome—so it can understand the total loss and associate criminal activity to broader victim trends.

Who individuals call first—the incident response factor—varies greatly, from family and friends to the device vendors from whom the endpoint was bought:

- Consumers are extremely likely (88 percent on average) to turn to another person if personal, work or school data is stolen from one of their devices.
- Friends and family members consistently rank among the top two go-to sources, with police topping the list in the case of a home computer (25 percent) but less likely for other devices.
- Consumers are more likely to go to a local electronic store if their smart TV gets locked up by malware (24 percent).

Contents

Consumer attitudes toward paying to recover data

When it comes to paying for lost data, statistics from IBM's ransomware study found that 54 percent of consumers say they would pay up to $100 to get their financial data back, with 55 percent of parents saying they would open their wallets to retrieve their precious memories (digital photos), while only 39 percent of non-parents would pay.

The typical ransom demanded by cybercriminals is between $200 and $10,000, so while consumers report themselves willing to pay a relatively small amount of cash for data, in reality—when faced with their data disappearing—they are likely to pay much more for it.

Information gathered on cybercriminals' illicit profits supports the fact people do end up paying, and pay much more than they reportedly would pay when presented with a hypothetical ransomware demand. For example, while each type of ransomware is different, CryptoLocker's operators boasted a 41 percent "success rate"—meaning that more than one in three victims ended up paying the ransom, according to a survey by the University of Kent in the UK. According to various estimates, criminals using CryptoLocker are believed to have stolen between $3 million and $27 million. In another staggering example, criminals using the CryptoWall ransomware stole an estimated $325 million in illicit ransom payments from hundreds of thousands of victims across the globe.

In payment demands, according to IBM X-Force, Bitcoin is the top and most popular payment method linked with ransomware attacks, being the choice of cybercriminals thanks to the anonymity it offers and the difficulty of tracing transactions to their actual recipient.

More than one in three victims of ransomware pay the ransom, which can range from $200 to $10,000.

It is worth noting here that often consumers are not familiar with Bitcoin and may opt to lose their data if they do not understand how to make the payment, even if they are initially inclined to pay. Even more notable is the fact that some ransomware operators understand this as a factor in non-payment and therefore provide detailed instructions on obtaining Bitcoin or set up customer support lines to guide the inexperienced (see Figure 3).

If you believe you've been the victim of a ransomware scheme or other cyber fraud activity, it is recommended that you report it to the FBI's Internet Crime Complaint Center. The FBI has also discouraged people from paying the ransom since paying doesn't guarantee the victim will regain access to their data.

Figure 3. The CryptoWall ransomware's instructions to victims on obtaining Bitcoin

Contents

Businesses surveyed about ransomware

Six hundred business executives based in the US were asked about ransomware awareness and their perceived willingness to pay cybercriminals to get their organizations' data back in the event of a ransomware attack. Interviews were spread over businesses of different sizes as follows:

- 200 small-business executives (<100 employees)
- 200 medium-business executives (101-999 employees)
- 200 large-business executives (1,000+ employees)

Big picture: experience and company size define awareness level and willingness to pay

The responses from business executives show that both knowledge about ransomware and the perceived willingness to pay to regain control of data depend on business size and previous experience with similar attacks.

Overall, small to medium businesses (SMBs) are less "data attack" prepared than larger businesses:

- When it comes to electronic data being hacked, medium- to large-sized companies are more likely than smaller-sized businesses to have taken action in the past three months to protect electronic data.
- In protecting electronic data from being hacked, large companies are more likely than small and medium companies to use the following tactics to defend from ransomware:
  - Require employees to change passwords regularly (74 percent of large companies versus 56 percent of small companies)
  - Block some websites from being used in the workplace (74 percent of large companies versus 56 percent of small companies)
  - Offer training on workplace IT security (58 percent of large companies versus 30 percent of small companies)

Among business executives who have experienced a ransomware attack during their career, the concern for data security was found to be more significant. Almost one in two executives (46 percent) has some experience with ransomware attacks in the workplace, and 70 percent of that 46 percent have paid to get data back.

Contents

It's even more telling that according to this survey, 20 percent have paid more than $40,000 for their data. In the US, hospitals, educational institutions and utilities have paid amounts that average $20,600, but those cases are just the few that made it to the media. A blog post uncovering sums paid by US companies that were caught in the crosshairs of a ransomware attack reports that victims paid amounts as high as $45,000. Some were willing to pay even more for advice from the very hacker who compromised their servers on how to patch and secure them.

The IBM study found:

- Experience with ransomware attacks is more common among medium and large companies (57 percent and 53 percent) than among smaller companies (29 percent).
- Prior experience with a ransomware attack contributes to higher levels of concern about loss of data. For those with prior experience, data loss concern is 50 percent, compared to 35 percent for those without prior experience, across all device types, whether company or employee owned.
- Per the IBM survey, seven in ten of those who have experience with ransomware attacks (70 percent) have paid to get data back. Resolution has come at a hefty price for some, with more than half paying over $10,000.
  - 20 percent paid more than $40,000
  - 25 percent paid $20,000 – $40,000
  - 11 percent paid $10,000 – $20,000

Can paying so much to release the organization from the grip of ransomware be justified? According to the losses incurred by many organizations in the wake of sustained ransomware attacks, it can be. In a recent survey by SANS, more than 32 percent of financial firms said they've lost anywhere from $100,000 to a half-million dollars due to ransomware attacks on their organization.

Common threat scenarios

When it comes to business, ransomware extortion can take different shapes due to the variety of endpoints on the company's digital infrastructure. In their attacks on networks, ransomware operators look for the servers that keep the company running and encrypt those pivotal resources rather than encrypting endpoints across the entire company.

Contents

The point of entry is usually a phishing email with a malicious attachment, sent to an employee's email inbox. In most cases, the attachment is a Microsoft Office document that will prompt the victim to activate macros. Clicking the macros activation button often comes as second nature to users who just want to make the alert at the top of the document disappear. The malware executes as soon as the user allows the macros to run. Ransomware can also come through any other attachment, or via exploit kits that facilitate infection without any special action by the user.

Ransomware in an enterprise environment would typically take the following paths:

- Encrypt all files on company endpoints, disabling access to networks:

  Ransomware can scan target enterprise endpoints, find the locations where all files are saved, and rapidly encrypt all folders, rendering all data inaccessible. In 2016, a number of hospitals in the US fell victim to ransomware attacks of this type.

  Another case involving ransomware affected San Francisco's Municipal Transportation Agency in late November 2016, causing its light rail system to enable free trips on one of the busiest days of the year, Black Friday.

- Find and encrypt data and backups on and via company servers:

  The Samas ransomware was launched by hackers who studied and targeted specific companies then penetrated their networks with pen-testing tools to ultimately encrypt files and backups.

  In another example, the Bucbi ransomware was delivered via brute-forced RDP (Remote Desktop Protocol) accounts on Internet-facing Windows servers, infiltrated company networks, and infected employee endpoints, locking files to prevent access.

- Find and exfiltrate data from the organization, then threaten to publicly release it unless paid.

  Ransomware is a crime like any other. If companies shift to restoring data from adequate backups and refuse to pay ransom for encrypted files, cybercriminals may attempt to shift tactics and demand payment for not releasing stolen data. This cyber extortion technique is not a ransomware attack per se, but rather a targeted attack that demands ransom for seized company assets.

Contents

Businesses rely on data to be available on demand, and ransomware attacks can easily disrupt operations, temporarily or permanently restrict access to data, corrupt or cause loss of data, and inflict monetary and reputational damage on the organization. An example of a case where ransomware caused immediate impact to operations was the hack of the San Francisco light rail transit system where an opportunistic ransomware operator disabled the rail's agents' endpoints, taking them offline for an entire day. The SFMTA recovered from the ransomware attack by using its own backups and never paid the cybercriminal.

Most meaningful data: the business take

Two-thirds of business respondents in the IBM ransomware survey are generally worried about corporate data being compromised by hackers, be it via ransomware or other types of attacks, while being less concerned about a hack actually taking place on their protected networks.

The real pain point? Protecting employee-owned devices used for work (BYOD, or "bring your own device"), such as tablets and smartphones. Leaders are most afraid those devices will be hacked, thereby putting the organization at risk:

- Business executives are less confident in their organization's ability to protect data on personal BYOD devices used for work versus company owned devices.
- They place higher confidence in the ability to protect company owned devices (83 percent versus 70 percent average confidence for BYOD personal devices).
- Personal computers are the device business executives most fear getting hacked, with about half feeling this way (48 percent). Others were concerned about BYOD smartphones and company-issued equipment getting hacked.

Financial and sales records topped the list of types of data for which executives would most likely pay ransom, although generally there was very little difference from one type to another.

Contents

About 60 percent of respondents indicate that their organization would be willing to pay some sort of ransom in order to recover stolen data:

- Financial records – 62 percent
- Customer and sales records – 62 percent
- Corporate email system/server – 61 percent
- Intellectual property – 60 percent
- Human resource records – 60 percent
- Corporate cloud system access – 60 percent
- Business plans – 58 percent
- R&D plans – 58 percent
- Source code – 58 percent

The incident response factor

After determining the scope and malware type with which they have been hit, businesses responding to a ransomware attack have a few options:

- Restoring their data and server configurations from the most recent backup
- Attempting to decrypt the malware themselves, which is possible in some cases, but usually not an option
- Paying the ransom or entering into negotiation with the cybercriminals, with or without police intervention
- Not responding and losing the data/access, then reimaging affected endpoints; this option entails considering the possibility of public exposure of stolen data

Law enforcement's recommendation is to avoid paying cybercriminals, putting more effort into prevention and lowering the risk of ransomware attacks and having a solid business continuity plan in place, including backup, redundancy and remediation capabilities.

The IBM ransomware survey reveals that while many companies have taken protective measures, most know they would benefit from expert consultation on this matter:

- Sixty-nine percent of respondents stated that their company has taken action (in the past three months) to protect its electronic data from being hacked.
- The most useful resources in preventing a hack are best practices in data security (58 percent) and security expert consultations (56 percent).

Contents

Businesses' attitude toward paying to recover data

The perception of the value of data, and the corresponding willingness to pay to retrieve it, increases with company size. Sixty percent of all respondents say their businesses would pay some ransom and they're most willing to pay for financial (62 percent) and customer/sales records (62 percent). Larger firms are notably the most willing to pay substantial amounts of money to get data back.

What do executives believe they will pay to recover company data? The reply varies according to the business's size and type of data. The amounts executives believed they would pay are expressed here as the percentage out of the business's IT security budget.

To understand business executives' attitude regarding how much ransom they would consider paying, IBM's ransomware survey looked at ransom amounts as part of the overall IT budget. According to a recent SANS survey, in 2016 most companies' projected median IT budget is $500,000 to $1,000,000, and most spend seven to nine percent of it on security. We asked executives how much their organizations would be willing to pay in case of a serious ransomware attack:

- **For financial records:** would pay over $50,000:
  - Large business – 29 percent
  - Medium business – 12 percent
  - Small business – 5 percent
- **For sales records:** would pay over $50,000:
  - Large business – 24 percent
  - Medium business – 8 percent
  - Small business – 5 percent
- Those working for small-sized businesses were far less likely to pay a ransom at all.

The size of the business and the type of data held for ransom are the most significant predictors of whether or not the company would pay and how much.

Contents

Law enforcement advises: Don't pay!

With ransomware, the question is still what it's always been: to pay, or not to pay?

The FBI and other law enforcement agencies advise victims to avoid paying a ransom. That only encourages cybercriminals to continue spreading their malware and raking in the cash. According to FBI Cyber Division Assistant Director James Trainor:

"Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cybercriminals to target more organizations; it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."

As Will Bales, supervisory special agent for the FBI's Cyber Division, said to the Federal Trade Commission (FTC):

"People have to remember that ransomware does not affect just one person or one business. It will more than likely move on and affect somebody else. And for those who pay the ransom, it only encourages [cybercriminals] to extort the next person."

The more outspoken law enforcement is about ransomware, the less organizations are likely to pay cybercriminals without a fight. Refusing to pay cybercriminals is the only way to reduce the allure of ransomware, the ROI and the profits that keep this type of crime going now and in the future.

Contents

What can consumers do to lower the ransomware risk?

Most cases of ransomware infections begin with unsolicited email that tricks victims into opening a malicious attachment or clicking on a spoofed URL. If you are not expecting a document, such as an invoice, package tracking link or fax, your best bet is to immediately and permanently delete the unsolicited message and alert your service provider if an email purported to come from them.

Banish unsolicited email: Sending a poisoned attachment is one of the most popular infection methods used by ransomware operators. Be very discerning when it comes to what attachments you open and what links you click in emails.

No macros: Office document macros have been a top choice for ransomware operators in 2016. Opening a document and that then requires enabling macros to see its content is a very common sign of malware, and macros from email should be disabled altogether.

No ads: Disable ads in your browser to prevent pop-ups and banners. Those can often deliver exploit kits that in turn scan endpoints for vulnerabilities and silently infect them without the user's knowledge. This is important because any website, even very reputable ones, can be plagued by dubious third party ads.

Update and patch: Always update your operating system, and ideally have automatic updates enabled. Opt to update any software you use often, and delete applications you rarely access.

Protect: Have up-to-date antivirus and malware detection software on your endpoint. Allow scans to run completely, and update the software as needed. Enable the security offered by default through your operating system, like firewall or spyware detection.

Junk it: Instead of unsubscribing from spam emails, which will confirm to your spammer that your address is alive, mark it as junk and set up automatic emptying of the junk folder.

With threats crossing to the mobile platform, ransomware has been a growing problem to Android-based handsets. These tips apply to your mobile as well, except unsolicited messages can also come in the shape of SMS messages or fake notifications. To learn more about protecting your mobile device visit our online mobile security tips page.

Contents

What can businesses do to lower the ransomware risk?

In addition to user education for employees to emphasize the consumer tips mentioned, businesses can also enact formal policies to address the ransomware risk.

- **Awareness:** Plan and carry out periodical employee awareness campaigns about threats in general and ransomware in particular. It's vital for employees to understand their critical role in preventing the success of ransomware attacks.
- **Hygiene:** Have and carefully maintain security hygiene plans that include operating system updates, patching software and updating firmware. Consider using a centralized solution to handle efficient security hygiene routines.
- **Backups:** Plan and maintain regular backup routines. Ensure that backups are secure and not constantly connected or mapped to the live network. Test backups periodically to verify their integrity and usability in case of emergency.
- **Security software:** Have up-to-date antivirus and malware detection software installed on employee endpoints. Set up regular scans and automatic updates for those solutions.
- **Safer browsing:** Disable Internet ads on employee endpoints and modify browser security settings to restrict unauthorized downloads.
- **Safer email:** Disable Office file macros when those are launched through email attachments.
- **Plan:** Creating and maintaining an incident response plan is key to quick recovery from any security incident. Learn more about incident response planning and how to orchestrate the response.

Contents

Ransomware won't change until we do

Ransomware is one of today's most prominent online threats. It has risen 300 percent since 2015 alone, creating a rising source of illicit gains that is relatively easy for even lower-skilled cybercriminals to operate.

Geographic safe havens and the low probability of apprehension embolden those who carry out ransomware attacks. Cybercriminals using ransomware may fund multiple criminal enterprises, from cybercrime gangs to organized crime networks to terror organizations. Cybercriminal enterprises would prefer every ransomware attack to result in financial gain, and individual cybercriminals believe this will be the case.

A cybercriminal's reputation is at stake from the moment an enterprise hires the individual. Encountering resistance from a victim, he or she might shift tactics, perhaps blaming or shaming the victim into paying—tactics that may also serve to preserve or enhance the criminal's reputation with their peers and employer. This activity should be viewed as a lucrative extortion model ultimately serving criminal enterprise rather than a single individual.

For ransomware attacks to subside, what needs to happen is clear: There must be a substantial drop in profits, to the point where cybercrime gangs no longer find it lucrative to orchestrate ransomware operations.

The top three factors that will eventually shift the dial on ransomware are:

- User education and employee awareness
- Ongoing business continuity planning and regular data backup that is tested and secured
- Incident response and disaster recovery capabilities

Ultimately, the case of ransomware is like that of an infectious disease before the discovery of penicillin. When the cure is known and properly implemented, the bug's successful infection campaigns subside, it can no longer cause damage, and eventually, treating it becomes routine.

Contents

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations, monitors billions of security events per day in more than 130 countries, and holds more than 3,500 security patents.

About the author

Limor Kessem is one of the top cyber intelligence experts at IBM Security. She is a seasoned security advocate, public speaker, and a regular blogger on the cutting-edge SecurityIntelligence.com blog. Limor comes to IBM from organizations like RSA Security, and ThetaRay. With her unique position at the intersection of multiple research teams at IBM, and her fingers on the pulse of current day threats, Limor covers the full spectrum of trends affecting consumers, corporations, and the industry as a whole.

Contributors

Kevin Albano, Global Lead for Threat Intelligence, IBM X-Force Incident Response & Intelligence Services

Ketchum Global Research and Analytics

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

For more information on IBM X-ForceForce, visit: **ibm.com**/security/xforce

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

Contents

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
December 2016

IBM

WGL03135-USEN-00