RANSOMWARE

While many cybercriminals use stealth and theft as their weapons of choice, ransomware perpetrators use neither.

ebook
An SC Magazine publication

Sponsored by
SOPHOS

The business case for ransomware

With sophisticated attack plans and technical support in place, ransomware criminals are banging on corporate and personal networks. Stephen Lawton investigates.

Ransomware is hardly new. In fact, the sci-fi TV series *Star Trek: The Next Generation* did an entire episode that clearly showed how a bit of social engineering can turn malware into a most dangerous form of ransomware. In the 1993 episode "Ship in a Bottle," a computer program recreates Sherlock Holmes's nemesis Professor Moriarty, who tricks Captain Picard into believing the computer program had become a sentient being. The program takes control of the Starship *Enterprise* and threatens to destroy it unless a ransom of services is paid. The demands are: a Shuttlecraft to transport the criminals off the *Enterprise* and taking another computer character off the holodeck and have her come to life. Once the malware is detected, the crew uses intrusion detection to essentially create a honeypot where the malware is able to reside and cause no more damage to the ship's computers.

OUR EXPERTS

Cheryl Biswas, threat intelligence consultant for cybersecurity, KPMG
Vikas Bhatia, CEO, Kalki Consulting
Brian Honan, CEO, BH Consulting
Lance James, chief scientist, Flashpoint; co-founder, Unit 221b
Chad Loder, strategic adviser, cybersecurity and privacy governance
James Scott, senior fellow and co-founder, Institute for Critical Infrastructure Technology

While that 1993 TV show was designed as entertainment, there is nothing amusing about malware that takes complete control of a corporate network, putting all corporate data at risk. In *Star Trek*, the fictitious ship was in danger. Today, financial demands, the potential for demands of services and the possibility that data will be lost – even if the ransom is paid – puts corporations and individuals at very real risk.

What distinguishes ransomware today are the brazen approaches attackers are using, along with the highly publicized payments that are being made by hospitals, businesses and even police departments. Rather than a criminal conducting a traditional stealth attack that drains data later put up for sale to third parties on underground markets on the dark web, today's ransomware attack goes for the immediate payoff in bitcoin or some other cyber currency. While the technology is basically the same, the business model, and thus the attackers' raison d'être, is significantly different.

"While ransomware is fundamentally another piece of malware, the main difference with ransomware from other forms of malware is its impact," says Brian Honan, owner and CEO of Dublin-based BH Consulting, an information security firm. Once ransomware infects a system, he explains, it can encrypt all data held on the victim's computer and all its drives, networked or otherwise, to which that machine is connected.

"This results in an immediate and impactful event that leaves the victim with the choices of hoping their backup strategy works, losing all their data, or [paying] the ransom," Honan says.

Ransomware's earliest occurrence dates back to 1989 when biologist Joseph Popp at an international AIDS conference distributed to attendees some 20,000 floppies infected with the AIDS trojan, aka the PC Cyborg virus. After a period of time, the recipients' infected machines would shut down and the

89%

Percentages of breaches that had a financial or espionage motive.

– 2016 Verizon Data Breach Investigations Report

owner was instructed to send $189 to a post office box in Panama.

In the past 25-plus years there have been a variety of attacks, including traditional logic bombs to the 2005 GPCPDER, a file-encrypting malware, and the 2010 WinLock, which attacked premium users of short message service (SMS). However, 2013 marked a major change in ransomware with the advent of CryptoWall, the first malware to demand bitcoin payments. Since then there have been numerous ransomware attacks on Windows- and Android-based systems, with KeRanger being the first to target Apple's OS X earlier this year. One enterprise firewall vendor estimates that today there are 30 active families of ransomware in the wild.

Vikas Bhatia, CEO, Kalki Consulting

It is this transition to immediate payoffs via anonymous cybercurrencies that makes today's malware attacks different from those in the past, says Vikas Bhatia, CEO of New York-based cybersecurity consultancy Kalki Consulting. Twenty years ago cybercurrencies didn't exist, "so you had to pay the guy with the carnation standing under the clock at Waterloo Station," he says, referencing a train station in London popular in spy novels. Today, ransomware writers can be anywhere in the world and quickly transfer the bitcoin payment into their local currency, he notes.

But corporate security staff should not become complacent and assume that a ransomware attack is what it seems to be – simply a demand for money or an overt attack, cautions James Scott, a senior fellow and co-founder of the Washington, D.C.-based Institute for Critical Infrastructure Technology, a cybersecurity think tank that focuses on critical infrastructure.

Historically, Scott says, distributed denial-of-service (DDoS) attacks were used by experienced attackers to shut down corporate servers and to plant malicious code. Today, he says, "ransomware is almost the new DDoS for experienced mercenaries."

Rather than simply using ransomware to extort money, today's attackers are using it as a diversionary tactic to misdirect and confuse IT departments, he says. While the victim is running around trying to stop the ransomware from spreading to other corporate systems, an entirely separate malware attack is being injected into the target network to map it and identify potential high-value targets.

In fact, sometimes the initial attack is outsourced to what is now referred to as ransomware-as-a service providers – so-called script kiddies who get paid, based on a fee structure, for mucking up the corporate works while the mercenaries focus on their prime attack, Scott says.

Ransomware as a business model

With traditional malware it's a binary response by the information security team or IT, Bhatia says. "You either have been attacked or haven't." With ransomware, the burden of responsibility to end the attack falls on the business and, therefore, it's a business decision to pay or not to pay, he says.

Some recent news stories in the consumer press tout very high ransoms being paid by victims. Hollywood Presbyterian Medical Center, for example, paid $17, 000 in bitcoin, according to the *Los Angeles Times*, and the University of Calgary paid $20,000, as reported by the Canadian Broadcasting Corp.

But Scott says the business model for ransomware is fraught with challenges and risk for attackers as well. First, he says, the attacker needs to have valid email addresses

2

Ransomware was the second-most popular crimeware attack from malware.

– 2016 Verizon Data Breach Investigations Report

for its targets. While mass email address purchases are common on the dark web, often those addresses are invalid. Next, the attacker needs a delivery method that will bypass the corporate data security tools. Infected emails can get picked up by one of the multiple layers of corporate email security and never reach the potential victim, so the recipient might never know they were attacked or by whom. While targeted spear-phishing emails can be more effective, they also take more time to research the potential victim and more effort on the attacker's part, Scott notes.

Third, he says, the attacker needs an effective delivery mechanism, which often requires ISP capabilities of modifying outgoing IP addresses and managing the massive mailings. Finally, he says, if someone is not an expert at spam, chances are they will not make money at ransomware.

Cheryl Biswas, threat intelligence consultant for cybersecurity, KPMG

If an attacker sends out one million ransomware attack emails and gets 50 responses, it's "an act of god," Scott says. Ransomware attackers are generally lucky to make a few hundred dollars on such an attack, not the millions that the consumer news media says attackers generally earn.

By layering defenses and having different types of email security built into the corporate defenses, companies can be "vigilant without being Orwellian," Scott says.

Now with tech support

Interestingly, one aspect of ransomware that differentiates itself from all other types of cyberattacks is that many cybercriminals using the approach also offer technical support. "One can assume that a large number of organizations that are either victims of ransomware or are called on to remediate ransomware do not have a dedicated information security team or are lacking in their capabilities," Scott notes. "If that is the case, then it makes sense for these individuals to have the support they need to restore business as usual as quickly as possible."

However, Bhatia cautions: "I really hope that this doesn't turn into an 'Oh, we got hit by XYZ and they had great support so we'll continue to pay!'"

Too often, companies will look at the costs of downtime versus the costs of hiring a forensics firm, making the effort to identify the breach, searching for a way to overcome the malware and then paying someone to come up with the right code to unlock the encrypted data, says Cheryl Biswas, threat intelligence consultant in cybersecurity in the Toronto office of the consultancy KPMG. Often the cost of paying the ransom is far lower than the cost of continuing business without paying the ransom. That said, paying the ransom is not the recommended response to an attack, she says.

Rather, the goal is to mitigate the damage as quickly as possible, she says. One approach to reducing the risk is to be educated about potential attacks before they happen. Sharing information about potential attacks through Information Sharing and Analysis Centers (ISACs) for a given industry is a good start, she says. "Bad guys collaborate," she insists, and so should the good guys.

Despite the availability of ISACs and Fusion Centers run by the Department of Homeland Security (DHS), many companies and agencies still are shy about acknowledging breaches and using these resources. (Fusion Centers operate as state and major urban area focal points for the receipt, analysis, gathering and sharing of threat-related information between federal, state, local, tribal, territorial and

42K

In the first year that CryptoLocker was in the wild, it generated roughly $27 million, or 42,000 bitcoin, in revenue for attackers.

– Ransomware: Unlocking the Lucrative Criminal Business Model, Unit 42

private sector partners, according to DHS.) Acknowledging a breach and discussing how it happened often appears as a sign of weakness for a company and could be used by a competitor, Biswas says.

There is a stigma following a breach, Biswas adds. “Companies don’t want to talk about it unless it’s plastered all over the news.” At that point, she muses, the companies don’t have the option of glossing over the attack.

The primary defense to a ransomware attack is to have business continuity and disaster recovery plans in place before the attack, experts say. Dealing with the potential of a loss before it happens helps minimize the damage after the attack is identified.

“Your backup will be your lifeline,” Biswas says, but adds that the backup must not be connected to the same network that it protects. The backup could be stored physically offsite in vaults or on cloud-based servers. However, she says, the cloud is not necessarily a “saving grace.” It is only as good as the people who operate it and the technology in place, neither of which the company that owns the backup can control.

> “Your backup will be your lifeline.”
>
> – *Cheryl Biswas, threat intelligence consultant for cybersecurity, KPMG*

The concept of stopping ransomware by having a strong business continuity and disaster recovery (DR) plan in place is sound, says Lance James, chief scientist at Flashpoint, a firm that offers tools and consulting for pulling data off the dark web. Make sure the company is making regular backups stored to multiple, off-premises locations, he says. Companies need to test their DR plans to ensure that an infected server can be taken offline quickly and an offsite server that is clean and untainted by a malware attack is able to fire up and replace infected server. It is not so different from a backup of a server that might be subject to a natural disaster, such as an earthquake, flood or tornado.

James, also cofounder of security consultancy Unit 221b, recommends that companies do regular scans of backups. While a piece of malware might have been able to bypass a scan in the past, updates to scanning software might be able to identify and stop the malware on a backup before it has a chance to relaunch.

From a practical perspective, the cybercriminals need to have high-quality customer support if they expect to receive payment, James adds. The problem attackers have with most of their victims is that they cannot pay the ransom in the proverbial coin of the realm – bitcoin. Most companies and individuals do not have personal or corporate bitcoin wallets, nor are many of the victims familiar with processing data via Tor.

As a result, in order for the ransomware scam to work, the attackers need to provide victims with the technical support to obtain a bitcoin wallet and then walk them through the procedures to obtain and then transfer the cryptocurrency.

Often the victim is feeling coerced or fearful for their jobs if they acknowledge they clicked on a bad link, James says, so they might pay the ransom in return for the attacker not disclosing the attack. However, if the victim does not report the attack to the corporate security team, they might be paying a ransom for data that is not actually compromised.

But James sees much more dire possibilities ahead. Rather than asking the victims to pay some bitcoin (the exchange rate for the dollar today is roughly $400 per bitcoin), James fears the attackers might begin asking victims to take specific actions rather than pay a fee. These actions could be anything from leaving an infected computer running overnight to

30%

Increase in ransomware attack victims in first quarter of 2016 over the fourth quarter of 2015.

– Kaspersky Lab

changing a setting to committing an act of industrial sabotage or theft.

If this occurs, he says, it takes ransomware from just a financial or data loss attack to potentially sabotage or espionage. That would be a significant change from today’s cybertheft.

To date, ransomware has become the bane of what Chad Loder, a Los Angeles-based security consultant refers to as legacy technology – in this case on-premises storage. “As we transition away from ‘docs on my laptop’ or ‘docs on a fileshare’ to doing more work in SaaS apps and cloud collaboration tools, ransomware won’t work as well,” he says. “Ransomware takes advantage of the fact that people generally are [poor at] backup hygiene. When getting your docs back becomes a push-button request in Office 365 or Salesforce, ransomware doesn’t work.” Loder is former vice president of security solutions and co-founder of the security software firm Rapid7.

Many types of malware are borne by spoofed email and these can and could be blocked at the perimeter using graylisting and DNS lookups. Subscribing to an effective threat feed that identifies known malicious email addresses, subject matter headings, keywords and known malicious IP addresses also could be included as part of a company’s defense.

Brian Honan, CEO, BH Consulting

However, Honan believes that ransomware is a very lucrative source for criminals and they will work hard to ensure this continues to be the case. By encrypting the data with the criminals’ own form of crypto, they ensure only they can have access to it. While the security companies are discovering the various keys used by the criminals to decrypt the ransomed data, the criminals are constantly updating their ransomware with new keys. “So, in effect it is a race between both sides,” he says.

But not all attackers use unique keys, Scott notes. Sometimes, attackers will use the same crypto key for multiple attacks. In some cases, victims are able to search the internet for ransomware crypto keys and decrypt their data without paying the ransom. In such cases, the attackers fall victim to the same poor security practices that hamper some victims – using the same password, or in this case, the same crypto key, for multiple accounts.

Curiously, not all releases of private keys for ransomware are published accidentally. In July, *SC Magazine UK* published a story about rival gangs posting the private Chimera decryption keys of the other gang. The goal, the story said, was to reduce competition.

Historically, during a malware incident, the CFO or business stakeholder would need to authorize the spend on resources to respond to an incident. Whether this now involves spending bitcoin to remediate or bringing in an external entity, it is the same decision process, Bhatia notes. “I really hope that infosecurity professionals are looping their legal and finance teams into the incident response planning for their organizations.”

Honan agrees that the business model for ransomware can be problematic. “Criminals are also business people and they realize victims will only pay out if they are confident they will get their data back once they pay the ransom,” he says. Hence, these victims will look to ensure that any web searches about paying the ransom results in data being restored will give positive results. “This increases the victim’s confidence that paying the ransom will get their data back,” he says.

Despite the large amount of airtime and online news about ransomware, the criminals seem intent on getting every bitcoin they

97%

Percentage of malware that is unique to a specific endpoint.

– Webroot

can. In July, *SC Magazine* reported on a Kaspersky Labs research report that showed that ransomware for mobile devices using the company's security software has increased by a factor of four – from 35,413 of its users in 2014 to 2015 to 136,532 a year later.

The company says it detected nearly 450,000 ransomware attacks in October 2015, with a brief reduction to fewer than 200,000 in January 2016, before another spike to more than 350,000 by March 2016. Overall, in the 12-month period from April 2014 to March 2015, ransomware increased from roughly two million to 2.3 million users worldwide, the company said. Of those who were hit by ransomware, the proportion who encountered cryptors rose from 6.6 percent to 31.6 percent.

> "...there is no real way of knowing whether there isn't another backdoor within your network..."
>
> *– Vikas Bhatia, CEO, Kalki Consulting*

Kaspersky's results for its users is similar to reports from other security software vendors that note a sharp increase in ransomware attacks during the first quarter of 2016. A report published in May from FireEye reported an increase of more than 40 percent in ransomware attacks in the Asia-Pacific and Japan region in March, with a smaller increase of just less than 25 percent in the North, Central and South American region.

The "2016 Data Breach Investigations Report" from Verizon describes ransomware as "Crimeware." According to the report, "The Crimeware pattern continues to be driven by external organized criminal groups that are financially motivated. Establishment of control over a device using [command and control] malware followed by ransomware, then the targeting of credentials or enrollment into a botnet accounts for the majority of the incidents."

In an October 2015 article on *The Security Ledger*, site founder Paul Roberts reported that at a Cyber Security Summit in Boston, Joseph Bonavolonta, assistant special agent in charge of the FBI's CYBER and Counterintelligence Program in its Boston office, said that in some cases it is often easiest for companies to simply pay the ransom for their data.

While even the FBI in some instances acknowledges that paying the ransom might be a valid business decision, Bhatia says that from an information security perspective it is generally not a good idea to pay the criminal. "If you have been compromised, there is no real way of knowing whether there isn't another backdoor within your network or the decryption key doesn't contain more malware."

Even if the criminals provide a valid code to unlock attacked data's crypto key, there's no knowing if the malware has already burrowed deep into the corporate data, Bhatia notes. The best way to ensure data is safe is to purge the attack from the system.

For more information about ebooks from SC Magazine, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

93%

of organizations surveyed are running applications or experimenting with infrastructure-as-a-service.

– RightScale, "2015 State of the Cloud Report"

Sponsor

SOPHOS

More than 100 million users in 150 countries rely on Sophos' complete security solutions as the best protection against complex threats and data loss. Simple to deploy, manage and use, Sophos' award-winning encryption, endpoint security, web, email, mobile and network security solutions are backed by SophosLabs – a global network of threat intelligence centers.

Learn more at www.sophos.com.

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
CUSTOM MANAGER Kelly Heismeyer
kelly.heismeyer @haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*