Root Out Ransomware

Like dandelions taking over your lawn, ransomware is spreading. It's time to get up on the latest prevention strategies and recovery tactics.

"If You Ever Want to See Your Data Again …"

Information security never gets boring, but don't you sometimes wish it did? Now we've got ransomware to grapple with, that "new and improved" form of malware that holds your data hostage, demanding payment in exchange for its life. Hackers' use of ransomware is growing and getting more sophisticated. (There's even talk now about the ransomware business model.)

As this guide shows, there are no shortages of alarming reports about the rise of ransomware. Certainly, one key purpose of this Tech-Guide is to clarify the nature of the threat. Locky, Teslacrypt, CTB-Locker and Petya—our experts examine these and more. To paraphrase ancient Chinese military mastermind Sun Tzu, the first step in any security strategy is to know thy enemy.

There's a larger purpose, though: preparation. This guide provides you with concrete actions to take now to harden defenses and protect your enterprise from being a ransomware victim. And yet, as any experienced security pro knows, successful breaches do happen. That's why our closing chapter outlines steps you can take to recover from a ransomware attack, including how to contain the attack so it doesn't spread through your system. That's good information to have under your belt, before the worst happens.

Hackers love nothing more than an easy victim. This guide will help your organization avoid being one. ■

Brenda L. Horrigan, Ph.D
Managing Editor, Security Media Group

Why You Must Make Ransomware a Security Priority

Malware that encrypts key data and demands a ransom for its release has emerged as a top threat to business, according to researchers at security firms Kaspersky Lab and FireEye. A report from Kaspersky Lab revealed that the first quarter of 2016 saw a spike in the use of so-called *ransomware attacks*, which researchers said could become the main problem of 2016.

According to Kaspersky Lab, the company's database includes around 15,000 ransomware modifications, and the number continues to grow.

Of the 345,900 ransomware attacks blocked in the first quarter, the security firm said 17% targeted the corporate sector. The number of new pieces of mobile ransomware increased to 2,895, up 46% compared with the previous quarter. One of the most widespread attacks in the first quarter of the year was Locky, which Kaspersky Lab detected in 114 countries.

The top three ransomware families were Teslacrypt (58%), CTB-Locker (24%) and Cryptowall (3%), which all spread mainly through spam email with malicious attachments or links to infected webpages.

TECHNOLOGICAL INNOVATION IN RANSOMWARE

A ransomware called Petya was interesting from a technical perspective, the Kaspersky Labs report noted. Petya can not only encrypt data stored on the computer, but can overwrite the hard disk drive's master boot record, leaving infected computers unable to boot into the operating system. This represents significant technological innovation in ransomware, the researchers said.

"One of the reasons why ransomware has become so popular lies in the simplicity of the business model used by cybercriminals," said

Aleks Gostev, chief security expert in Kaspersky Lab's Global Research and Analysis team.

"Once the ransomware gets into the users' system, there is almost no chance of getting rid of it without losing personal data. The demand to pay the ransom in Bitcoins makes the payment process anonymous and almost untraceable, which is very attractive to fraudsters," he said.

RANSOMWARE TRENDS, THREATS

Another reason for the rise in ransomware attacks, according to Kaspersky Lab, is that those they target believe the threat is unbeatable.

"Businesses and individuals are unaware of the technological countermeasures that can help to prevent infection and files being locked up. By ignoring basic IT security rules, they allow cybercriminals to profit," Gostev said.

A threatening trend, Gostev said, is the ransomware-as-a-service business model, where cybercriminals pay a fee for the propagation of malware or promise a percentage of the ransom an infected user pays, making it easier than ever to carry out this type of attack.

Kaspersky Lab researchers said there are also services that work the other way round, offering a complete set of tools to the encrypter, who takes responsibility for distributing the Trojan and takes 10% of the ransom as commission.

The Kaspersky researchers also reported instances of well-known Chinese and other attack groups using ransomware. "If these incidents become a trend, the threat will move to a new level because the damage caused by ransomware is not much different from that caused by Wiper-type Trojans. In both cases, user data becomes inaccessible," the report said.

Another worrying trend, the Kaspersky Lab researchers said, is that ransomware Trojans

"Once ransomware gets into the users' system, there is almost no chance of getting rid of it without losing personal data." —**ALEKS GOSTEV,** Kaspersky Lab are expanding their sphere of activity, with CTB-Locker targeting web servers.

RISE OF RANSOMWARE

According to the data gathered by FireEye, the upward spiral of ransomware began accelerating in the second half of 2015.

The development of families with new anti-detection or encryption methods suggests enough victims are paying consistently enough to motivate cybercriminals to constantly improve their malicious code, FireEye researchers said.

"The threat landscape is changing every day, and organizations need to seek any advantage they can find to try and stay one step ahead of the attackers," said Richard Turner, regional president at FireEye. "The evidence highlighted in this report demonstrates that geopolitical, financial and economic changes happening in the region are increasingly mirrored in the cybersecurity world."

It's critical that all organizations prepare now for the reality of ransomware. They need to secure their systems wherever possible and know what to do in the event of a breach. As Turner noted, organizations "are only as strong as their ability to adapt."

—*Warwick Ashford*

Five Steps to Raising Ransomware Resistance

RANSOMWARE ATTACKS ARE not only becoming more common—they're becoming more creative. This advanced malware that once targeted users directly is now being deployed via remote exploits of unsecured web servers running WordPress and, now, JBoss. According to Cisco's Talos threat intelligence organization, a new type of ransomware called SamSam is targeting enterprises running vulnerable versions of JBoss. Rather than the ransomware infection spreading through phishing attacks or drive-by downloads, it attacks a compromised server and spreads throughout the internal corporate network. This is just one example of a myriad of highly complex threats targeting corporate assets and resources every day. Ransomware appears to be coming of age.

So, what can enterprises do to protect themselves from an initial ransomware infection? If ransomware gets into one system, how can enterprises stop it from spreading to others? It all comes down to common sense. The ransomware threat is no different than any other threat; there's a vulnerability, and the criminals want to exploit it for ill-gotten gains. The method and underlying technologies evolve, but the threat itself needs to be handled in the same manner as any other threat. Here's how enterprises can approach this security challenge:

1. Acknowledge that you don't know what you don't know. The sign of a truly wise security professional is admitting that many things on the network are unknown. Systems, applications, users, information and the like all make up a group of assets that are often unaccounted for and, therefore, under-secured and currently at risk to ransomware. Another key indicator of a smart security pro is the presence of a plan to make things better.

2. Acquire support from management and users. Before anything can get off the ground in security, management needs to politically and financially back it, and they need to do so on an ongoing basis. Assuming the security team is able to get management on board with their plan for fighting ransomware, they'll also need to get the users on board with policies, ramifications of bad choices and the overall setting of expectations.

3. Deploy the proper technologies or tweak your existing setup. The heart of a strong malware defense is well-designed and properly implemented technologies. If a network is to stand up against a modern-day ransomware infection, it needs to have a few things.

- First and foremost, patching needs to be under control. Many businesses struggle with this, especially with third-party patches for Java and Adobe products, and hackers love this. Until software updates are deployed in a timely fashion, the organization is a sitting duck. A network is just one click away from compromise.

- Effective malware protection is also a necessity. Steer away from the traditional, and look more toward advanced malware tools, including non-signature or cloud-based antivirus, whitelisting, and network traffic monitoring and blocking technologies.

- Data backups are critical. Organizations' systems are only as good as their last backup. Discussions around backups are boring, but they need to be well-thought-out to minimize the impact of the ransomware that does get through and encrypts critical assets.

  Network segmentation is another important part of ransomware protection, but it's only sometimes deployed properly. Just keep in mind that virtual LANs—the most common segmentation technique—aren't secure if an internal user can guess the IP addressing scheme that's likely a mere digit increment or decrement away.

- Finally, security assessments can help protect enterprise networks. Stop pen testing for the sake of the Payment Card Industry Data Security Standard, and start performing comprehensive security vulnerability assessments that look at the bigger picture. If the security team keeps malware in mind when it looks at its internal network from the internet, it'll find a slew of weaknesses that are currently facilitating the ransomware infection threat. Document these findings and present them to management for the necessary support.

4. Monitor and respond. Security teams can't secure—or respond to—things they don't acknowledge. Most enterprises have a half-baked monitoring, alerting and incident response program. Security teams need to do what needs to be done: monitor servers, workstations and networks for anomalies; take quick action; and do what's necessary to respond to the current event and prevent it from reoccurring.

5. Fine-tune to get better. Many people—both in management as well as IT and security—view security as a one-time deal: You invest, you deploy, you assess and everything else will take care of itself. But this is hardly the case. IT and security teams are pressed for time because they're constantly having more projects layered on top of what is still left undone. Figure out a way to fix that. It may be in terms of time management, different processes or hiring new employees. Whatever it is, fix it.

The security solutions to a ransomware infection are not endpoint-centric, as Cisco's Talos report showed, nor are they network-centric. They're holistic. It's a little bit of everything—in various parts of the organization—working together to create barriers to entry and exploit. Sound familiar? It's the same tried-and-true approach to information security that's been known for decades, yet organizations continue to struggle with it. The technical understanding is there, but security is impeded by politics and special interests. From the CIO to the chief learning officer to the CEO and a lot of people in between, everyone involved has his or her own agenda that keeps what needs to be done from getting done.

An organization might not be able to overcome the human aspects of information security, but it can at least try to make the criminal hacker's job as difficult as possible.

—Kevin Beaver

Ransomware Recovery Starts With a Data Strategy

THE NATURE OF disaster recovery planning is changing, almost on a daily basis. What was once preparing for the loss of the data center caused by a natural or manmade event is now morphing into recovering from ransomware and other cyberattacks. The latest complications promise to be more problematic to an organization than any natural disaster could ever be.

Cyberattacks, like denial of service attacks and viruses, have been around since the internet has been connecting organizations. But there is a new assault that looks to be very difficult to keep out and extremely costly to defeat over time: ransomware attacks.

Ransomware typically enters a data center when users click on a link they shouldn't. The ransomware downloads a virus onto the user's device and then begins crawling into everything the user has access to, including network shares and other users' laptops, encrypting all the data it encounters.

Unlike other cyberattacks, the data is usually kept intact, but it is encrypted by the virus. The only way to gain access to your data is to buy the encryption key from the attacker using a service such as Bitcoin. This digital currency uses its own encryption techniques to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. Attackers use Bitcoin to get paid without revealing their identity or location.

QUICK RANSOMWARE-RECOVERY STEPS

A key facet to successfully recovering from ransomware is a solid data protection strategy:

Step 1: Continuous protection. Organizational shares need to be protected via replication, snapshots or frequent block-level incremental backups, with the understanding that data created or modified between protection events will be lost.

Step 2: Laptop protection. Mobile users create and modify data separate from the corporate network-attached storage (NAS) or file server. Protecting these devices should be standard operating procedure for most organizations, but that often isn't the reality. The threat of ransomware heightens the requirement. There are plenty of laptop data protection products available, but most only protect data on a scheduled basis.

A viable alternative is [enterprise file sync-and-share products]() that update a corporate NAS or file share as users change data. Data on these systems should be recoverable in the event of a ransomware attack. Some enterprise file sync-and-share offerings are adding the ability to detect a ransomware attack, turn off syncing and alert an administrator of a potentially infected laptop.

The real challenge with ransomware is that, unlike other types of attacks, it is almost impossible to keep out of an organization. A popular approach is to send an email that looks like it's from a popular online retailer and request that users click a link for an order status.

Because of the way an attack is triggered and how it infects data, recovering from ransomware is almost always the responsibility of the data protection team. The problem is that most of the infected data is only protected once per night through the backup process, as it is deemed not as critical as an organization's databases and applications. If, as is often the case, the attack happens during the middle of the day, then much of the infected data has either been created or changed since the last protection event. The result: The last good copy of data is solely in the possession of the attacker.

Stopping ransomware may be an almost impossible act for IT organizations. But recovering from ransomware should not be. A successful ransomware recovery can leverage existing data protection techniques, but the span between protection events needs to be shortened. —*George Crump*

ABOUT
THE
AUTHORS

HOME

EDITOR'S NOTE

WHY YOU MUST
MAKE RANSOMWARE
A SECURITY PRIORITY

FIVE STEPS TO
RAISING RANSOMWARE
RESISTANCE

RANSOMWARE
RECOVERY STARTS WITH
A DATA STRATEGY

WARWICK ASHFORD, *security editor at Computer Weekly since 2012, previously served for five years as the site's chief reporter. Before his career in IT journalism, Ashford worked as a course developer and technical writer for an IT training organization and also spent many years in radio news at the South African Broadcasting Corporation.*

KEVIN BEAVER *is an information security consultant, expert witness and professional speaker with Atlanta-based [Principle Logic LLC](). Beaver specializes in performing independent security assessments revolving around information risk management. He has authored or co-authored 12 books on information security, including* Hacking For Dummies *and* The Practical Guide to HIPAA Privacy and Security Compliance.

GEORGE CRUMP *is president of Storage Switzerland, an IT analyst firm focused on storage and virtualization. Prior to founding Storage Switzerland, Crump was chief technology officer at one of the nation's largest storage integrators, where he was in charge of technology testing, integration and product selection.*

STAY CONNECTED!

Follow @SearchSecurity today.

TechTarget

Root Out Ransomware
is a SearchSecurity.com e-publication.

Robert Richardson | *Editorial Director*

Kara Gattine | *Executive Managing Editor*

Brenda L. Horrigan | *Managing Editor*

Robert Wright | *Executive Editor*

Linda Koury | *Director of Online Design*

Megan Cassello | *Graphic Designer*

Moriah Sargent | *Managing Editor, E-Products*

Doug Olender | *Senior Vice President/Group Publisher*
dolender@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER: FOTOLIA