CODE42

Ransomware roadmap: where cybercriminals will attack next

In the first quarter of 2016, $209 million in ransom was paid to cybercriminals. The FBI estimates that losses incurred in 2016 due to ransomware will top $1 billion. Unfortunately, that looks to be just the beginning, as many attacks go unreported. Without a recent and reliable backup, victims have little choice but to pay to recover their files. By doing so, however, victims inadvertently fund cybercriminals’ research and development activities and the rapid evolution of attacks.

This white paper examines the evolution of ransomware proliferation techniques and what organizations can expect in the future.

Current ransomware trends

According to research by **Malwarebytes**, nearly 40 percent of businesses experienced a ransomware attack in the prior year. As a result of these attacks, more than one-third lost revenue, and 20 percent had to cease business completely. Malwarebytes also found that UK CIOs, CISOs and IT directors are most likely to pay a ransom to get their data back. Not only is it embarrassing to fall prey to extortion, their jobs could be at risk if others became aware that the organization failed to prevent this threat.

Cybercriminals focus their efforts on industries where large amounts of money are made, data is highly valued and downtime has a significant impact. Malwarebytes found that healthcare and financial services were the leading industries attacked with ransomware globally. Both industries were targeted well above the average ransomware penetration rate of 39 percent.

A short history of ransomware

1989	**First appearance of cryptoviral extortion was in 1989 via floppy disk, created by Dr. Joseph L. Popp**
2005–06	**Apps posed as spyware removal tools and computer performance enhancement tools**
2008–09	**Apps posed as fake antivirus programs**
2011–12	**Drive-by downloads. Mimic law enforcement notices and Windows error messages**
2012–16	**Attackers add phishing and direct attacks to their arsenal**

Ransomware characteristics

Ransomware attacks evolve quickly. Cybercriminals use a specific strain of ransomware and backend servers once or twice, then change them substantially to avoid detection. Attacks tend to be automated, well-orchestrated and fast. Victims don't know that they have been attacked until after their data has been encrypted and the ransomware triggers a notification, informing the user to pay a sum of money in untraceable Bitcoin to regain access to data.

Proliferation methods have also evolved. What began on a floppy disk (see timeline), has spread to nearly every possible attack vector used by malware. However, the majority enters through an endpoint, often originating from email. These attacks require the user to take an action and include:

Phishing
Emails with .ZIP-like attachments trick users into opening an attachment or clicking on a link that allows the system to run the ransomware locally. MakTub is one such example.

Spam
Emails with corrupted attachments, such as a Microsoft Office document with malicious macros. Locky is an example of ransomware sent via spam.

Drive-by downloads
A compromised website hosts an exploit kit, which attacks a security vulnerability on the user's machine. The exploit kit then delivers the payload—the actual ransomware—which is then executed. Mobef is one example of ransomware delivered via a drive-by download.

Malicious applications (aka Trojans)
Ransomware can also pose as legitimate software that is downloaded by the user. The ransomware Fantom poses as a legitimate Windows update.

External drives
Ransomware stored on a USB flash drive automatically encrypts the machine when the flash drive is attached. The ransomware CryptoLocker was modified from a Trojan to a worm spread via USB.

Cybercriminals can also attack users directly with ransomware by penetrating the environment via social engineering or by exploiting a vulnerability. Once in the system, the attacker manually executes the ransomware.

Still other strains of ransomware are self-propagating. It only takes one user to run it, and the ransomware infects a series of shared files. When an infected shared file is opened by another user, the ransomware executes in that user's machine, encrypting every file to which the user has write access—including those on shared infrastructure.

Russian Roulette ransomware.

Cybercriminals have added other “features” to their ransomware to convince victims to pay a ransom and to do so sooner rather than later. For example, a strain of ransomware dubbed Russian Roulette randomly deletes files until a ransom is paid. These files become effectively unrecoverable because the ransom only buys the victim decryption capability. One example of Russian Roulette ransomware is Stampado. Other ransomware will delete large chunks of files at once if the user reboots or continue to encrypt new data until the ransom is paid.

Latest developments in ransomware

In addition to collecting ransoms directly from victims, cybercriminals are branching into new revenue models such as Ransomware as a Service. RaaS rents the infrastructure to bad actors who can’t create their own ransomware to attack others. The infrastructure often includes online support to help attackers—and their victims—through the decryption process.

Ransomware as a Service exists as two models. First, it exists on a per-person basis where individuals build out the infrastructure and provide services to others. In this model, the vendor takes a cut of the ransoms collected. In the other RaaS model, organized crime syndicates build a set of tools and infrastructure that are repurposed. This allows criminals to launch campaigns quickly. While Ransomware as a Service lowers the barrier of entry for would-be criminals and increases the number of attacks seen in the wild, it hasn’t become a huge factor due to the trust required between criminals.

Cybercriminals are also evolving their ransomware attacks to make the damage more difficult to undo without their involvement. For example, the security industry is beginning to see ransomware that targets executables. Previously, ransomware would encrypt all data in the home directory; it was very unusual for ransomware to go after binaries on the machine. However, now some strains of ransomware will break the software on the machine in addition to encrypting data.

Cybercriminals have also begun using **other forms of extortion**, such as Distributed Denial-of-Service (DDoS) and DNS attacks. These attacks bring down IT services or websites until a ransom is paid. Attackers recently launched a DDoS against Dyn, a U.S. company that provides directory services to online companies. This particular attack was not accompanied by an extortion demands, but it did bring down a number of high-profile sites, including Mashable, CNN and the Wall Street Journal.

What’s next from ransomware

Experts predict future “releases” of ransomware will require little or no user involvement and affect more of the organization’s data. For example, the security industry has already seen a crypto-worm, which behaves similarly to a traditional malware worm. A proxy looks for a vulnerability to exploit and runs the ransomware on behalf of the attacker with no user interaction. Instead of propagating through the network and creating a botnet, the crypto-worm escalates privileges on other machines and encrypts the data on them. By spreading throughout the network, a crypto-worm can encrypt greater quantities of data and demand higher ransoms.

Experts warn that ransomware attacks against high-value targets will increase. Organizations with critical data that can't afford downtime like hospitals and manufacturing plants will look for the fastest way to recover. Every minute they can't access data costs these organizations money and, in some cases, lives. Without backups in place, they are forced to pay the ransom. **Some hospitals have already paid out hefty sums to recover from ransomware attacks**. Financial services, B2B and supply chain organizations may also prove to be lucrative targets.

Similarly, the industrial Internet of Things will also become a target for ransomware. Rather than encrypting data, attackers could disrupt the control mechanisms of industrial equipment and connected machinery—a disruption that could have life-threatening consequences. These types of attacks are more complex and require that the attacker understands the machinery, intelligence that has not proven to be a deterrent in the past.

Conclusion

The proliferation of ransomware will stop when organizations stop paying out ransoms, and it ceases to be a lucrative business model. In the meantime, cybercriminals will continue to identify targets with higher payouts and increase ransom demands based on how much an organization values its data properties.

In order to say no to cybercriminals, organizations must protect themselves. The single most reliable way to shut down ransomware is to implement endpoint protection that assures and automates data redundancy. This technology can give organizations peace of mind in knowing that a copy of their data is safe and recoverable, regardless of what a ransom note tells them.

Learn how TaylorMade uses continuous and automatic endpoint data protection to not only fight ransomware, but streamline their IT processes. **Read more**

CONTACT CODE42 SALES:
code42.com/contact

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SO. | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM

Code42 is a global enterprise SaaS provider of endpoint data protection and security to more than 39,000 organizations, including the most recognized brands in business and education.
Our highly secure cloud solutions enable IT and security teams to limit risk, meet data privacy regulations and recover from data loss—no matter the cause.