Ransomware–Mitigating the Threat of Cyber Security Attacks

OTAVA POWERED BY Zerto

What is Ransomware?

In the last few years more organizations have witnessed the increasing trend of hackers attempting to extort money via the proliferation of various Ransomware Trojans such as WannaCry. In fact, according to Cybersecurity Ventures, Ransomware damages expected to reach $20b by 2021-- 57 times more than it was in 2015.

Malicious software is designed to gain access to files and encrypt data by generating a private-public pair of keys. The data is impossible to decrypt without the private key which is stored on the attacker's server until the ransom is paid. Unfortunately, in many cases even after a company pays the ransom the attackers never provide the decryption key leaving victims without their money or their files.

Recent advancements in encryption technologies coupled with the ease with which hackers can conceal their identities has resulted in an increase in the number of them adopting a ransomware strategy.

Ransomware—The story so far

The first largescale ransomware threats began in late 2013 with the emergence of what is probably the most well-known family of Ransomware, CryptoLocker. In May 2014, as a result of a joint operation by law enforcement and security agencies the CryptoLocker Trojan was shut down, thanks largely to the disruption of distribution over the GameOver Zeus network used by hackers.

Although the original CryptoLocker Trojan has been shut down, many imitations of it are still circulating, while at the same time other families of Ransomware have since sprung up. The most prolific of these families are CTB- Locker, TorrentLocker, WannaCry and more recently, MegaCortex. Regardless of the name, their aim is the same – extort money from victims in return for decrypting their data and files.

Why is ransomware such a big threat?

These attacks pose a considerable danger for several reasons:

- Clever and evasive techniques circumvent security software, resulting in the creation of "Zero-Day Malware", meaning the Trojan will be unknown to security experts as a risk in any security software.
- Security experts consider encrypted data to be unrecoverable. Many victims report that the decryption key is not provided by the attacker, even if the ransom has been paid. Therefore, giving in to the hacker's demands is pointless.
- Through the use of the Tor network and virtual currencies such as Bitcoin, hackers are largely untraceable by security agencies.
- Attacks are directed mostly at users in more affluent countries. According to MalwareBytes 47% of attacks in the first quarter of 2019 occurred in the US.
- Specific to businesses, in mid-2019, eCh0raix started appearing. This specifically targets mass-storage and network attached storage (NAS) disks. This trend of targeting "high-value" victims already has and is likely to continue increasing.

"Most ransomware attacks can be avoided through good cyber hygiene and effective, regular data backups that are continually tested to ensure they can be restored if needed. Our recommendation is that businesses need to be proactive because the decryption keys are not always provided when ransoms are paid and being proactive is often easier and less costly than a reactive approach."

Raj Samani
CTO for Europe at Intel Security

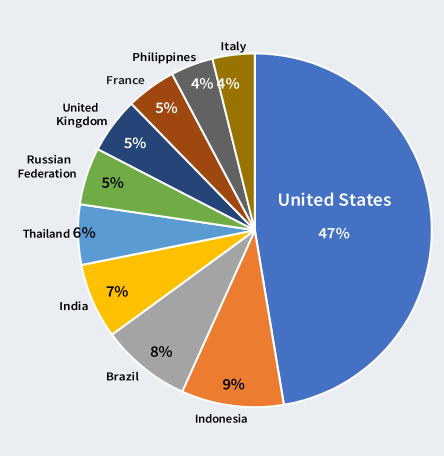

Figure 1: Q1 2019 Ransomware Attacks per Country - MalwareBytes

What are we likely to see in the year to come?

Unfortunately, Ransomware is on a steady rise. With over 850 million ransomware infections detected in 2018, recent studies show that attacks are increasing more than 300% year over year.

Numerous articles in the global news report organizations across the public sector, healthcare, transport and logistics, and financial services industries among others, are all suffering from increased ransomware attacks.

Use of the Tor Network has also enabled cybercriminals to begin offering Ransomware-as-a- Service (RaaS) models, meaning less experienced cybercriminals can leverage these attacks as well.

Cybercriminals are also becoming more corporate focused as they know that businesses rely on their critical systems to survive and therefore are more likely to pay a significantly higher amount to have their data decrypted.

So how do we protect ourselves from this threat?

As cybercriminals leverage more intelligent methods of attack, the need for protection becomes more crucial. An obvious starting point is ensuring you have suitable anti-virus and security software that is kept up to date. As seen in many cases, however, Zero-Day Malware is becoming more common so anti-virus software does not necessarily provide any guarantee of protection against this threat.

User education is also key, as many Trojans gain initial system access through links contained in phishing emails that are often very official looking. Human error can happen though, so extra layers of protection are still required.

Backing up your data is crucial, but the key to effectively recovering from ransomware is granularity. However, because traditional backup methods don't provide this granularity, most organizations with infrequent backups are at risk should their systems become infected. They will potentially stand to lose days' worth of data.

The Answer? Threat Mitigation

Accepting that prevention isn't always possible, mitigating the threat certainly is. Let's say you're the unfortunate victim of a ransomware attack. Your files are locked down and you start to realize that your last backup might have been from last night, last week, or maybe last month. How much data do you stand to lose? What's the cost to the business going to be? How will the public perceive your inability to counter this threat? What happens when all your public-facing services are down while you try to fix the problem? How much time is it going to take to get back up and running?

Otava DRaaS—Powered by Zerto

- Rewind your systems to the last point-in-time before the infection struck, to within a matter of seconds.
- Recover all your critical systems within the space of a few minutes, with only a few clicks of a button.
- Perform non-disruptive failover tests at any time, so you have confidence you can bring the business back online immediately.
- Fully managed solution so if you're under attack, simply call us to start the failover process
- Customized DR playbook tailored to your organization's specific RPO and RTO requirements.
- Recovery environment hosted inside secure, compliant data centers independently audited against HIPAA, PCI, SOC 2 and more