truenorth

Ransomware–Mitigating The Threat

WHAT IS RANSOMWARE?

Over the course of the last few years we have witnessed the increasing trend of hackers attempting to extort money from both private users, and more recently businesses, via the proliferation of various Ransomware Trojans such as CryptoLocker.

These malicious pieces of software are designed to gain access to and encrypt data and files by generating a private-public pair of keys. The data is impossible to decrypt without the private key which is usually stored on the attacker's server until the ransom is paid. Unfortunately, in many cases even once the ransom has been paid the attackers fail to provide the decryption key leaving victims without their money or their files.

Whilst Ransomware has been around for many years, the more 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 this strategy.

THE RISE AND FALL OF CRYPTOLOCKER

The current wave of Ransomware threats begun 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 enforcement and security agencies the CryptoLocker Trojan was shut down, thanks largely to the disruption of the GameOver Zeus network which was one of its major distribution agents.

Although the original CryptoLocker Trojan has been shut down we still see imitations of it circulating while at the same time many other families of Ransomware have since sprung up, the most prolific being CTB-Locker, CryptoWall, TorrentLocker and more recently, TeslaCrypt. Regardless of the name, they all aim to do the same thing – extort money from victims in return for decrypting their data and files.

WHY IS RANSOMWARE SUCH A BIG THREAT?

These types of attack pose a considerable danger for several reasons;

- They use very clever and evasive techniques to circumvent security software. This often results in the creation of "Zero-Day Malware", meaning the Trojan will be unknown to security experts so will not be have been identified as a risk in any security software.
- Security experts consider encrypted data to be unrecoverable. As many victims also report that the decryption key is not provided even if the ransom has been paid it, is not recommended to give in to the hacker's demands.
- Through the use of the Tor network and virtual currencies such as Bitcoin, hackers are largely untraceable by security agencies.
- The attacks are directed for the most part at users in more affluent countries – In 2015 50% of all CTB-Locker attacks detected were in the US and 35% in Europe.
- Specific to businesses, in late 2014 another Ransomware family to appear, SynoLocker, specifically targeted mass-storage and network attached storage (NAS) disks. This trend of targeting "high-value" victims already has and is likely to continue increasing.

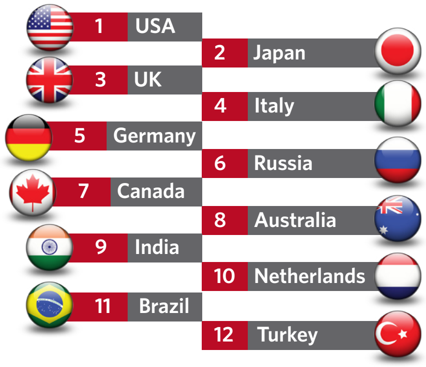

Figure 25. Top countries impacted by binary-based ransomware

WHAT ARE WE LIKELY TO SEE IN 2017?

Unfortunately the use of Ransomware seems only to be on the rise. 2014-2015 saw a 250% increase in the use of Ransomware and the first quarter of 2016 alone saw a 165% rise. McAfee Labs researchers then reported more than 4 million samples of ransomware in Q2, of which 1.2 million were new.

New focuses have been seen and are expected against, in particular, the financial industry and Public Sector organisations. You may have seen in a BBC News article a couple of weeks ago that Lincolnshire Council in England had their systems infected by a Ransomware Trojan which resulted in their network being shut down for over 4 days, affecting their public-facing services.

The use of the Tor Network has also enabled cybercriminals to begin offering Ransomware-as-a-Service (RaaS) models, meaning more inexperienced cybercriminals will be able to leverage these attacks as well.

Cybercriminals are also becoming more corporate focused as they understand that businesses rely on their critical systems to survive and so consider them more likely to pay – and pay a significantly higher amount - to have their data decrypted.

SO HOW DO WE PROTECT OURSELVES FROM THIS THREAT?

As cybercriminals leverage more and more intelligent methods of attack, the need to protect ourselves becomes ever-more crucial.

Ensuring you have suitable Anti-Virus and security software, as well as ensuring it is kept up-to-date, is the obvious starting point. As we have seen with the case of Lincolnshire Council however, Zero-Day Malware is becoming more and more common so AV software does not necessarily provide any guarantee of protection against this threat.

User-Education is also key, as many Trojans gain initial access to systems through links contained in (often very official looking) phishing emails. Human Error can and does happen though, so extra layers of protection are still required.

Backing-up your data is crucial, but many businesses either do not have a backup program in place, or have such infrequent backups that should their systems become infected they will potentially stand to lose months' worth of data.

> *"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*

THE ANSWER? THREAT MITIGATION

Sometimes you just have to accept that prevention isn't always possible, but mitigating the threat certainly is.

Let's say you've been the unfortunate victim of a Ransomware attack. Your files are locked down, you start to break a sweat... 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 you to get back up and running?

THE SOLUTION–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.
- Not only restore entire applications and databases with consistency, but with v4.5 gives you the granularity to restore individual files as well.
- Perform non-disruptive failover tests at any time, so you know you can bring the business back online straight away when needed.
- Create off-site backups for longer-term data retention in addition to giving you Continuous Data Protection for up to 14 days.

ABOUT True North ITG

With over 15 years providing IT services to healthcare providers, True North focuses on delivering the performance, security, and continuity you need to do what you do best: providing excellent care for your patients. True North converts your IT investment into drivers for improved business performance with our unique blend of people, process, and infrastructure. Take advantage of our IT expertise, including fully-redundant, HIPAA compliant data centers, end-to-end healthcare IT service and support, and exclusive partnership with GE Healthcare.

www.truenorthitg.com

16504 9th Ave SE Ste 203
Mill Creek, WA 98012

p: 480.482.1887
f: 425.743.3765
info@truenorthitg.com