LogRhythm®
The Security Intelligence Company

Next-generation ransomware

A threat that has never stopped evolving

In recent years, ransomware has grown very quickly from relative obscurity to become one of the greatest cybersecurity risks facing organisations today.

Ransomware is not a new type of threat: it's been around in its current form for over a decade. However, in the last few years, it has risen to prominence as an increasing number of variants were released into the wild – and several high-profile organisations fell victim to them. In the first half of 2017 in particular, the WannaCry and Petya/NotPetya outbreaks raised awareness of ransomware by causing damage to corporate systems that took some companies and parts of the public sector many months to recover from.

Organisations are now familiar with the threat ransomware poses, and are aware they need to protect their systems from emails and compromised sites that attempt to spread the malware, which can lock down systems and encrypt their files.

While the number of ransomware strains has been steadily growing in recent years, most variants still find their mark by exploiting unpatched systems. Ransomware may be hard to recover from but often it's relatively easy for IT departments to defend against, using good software hygiene and staff education. But just because organisations are becoming more accustomed to dealing with ransomware, it doesn't mean they can afford to take it any less seriously. As enterprises have become conversant with cybercriminals' conventional attacks, so the cybercriminals are evolving their tactics to stay one step ahead of their intended victims.

Ransomware groups are now using a number of new strategies to catch organisations out.

Losses due to ransomware are thought to have hit $1bn in 2016[1]

How ransomware is changing

Targeted ransomware attacks:
Ransomware gangs are refining how they distribute their products, going after enterprises that offer the biggest payday, such as financial institutions. In the past, ransomware groups have been using a 'fire and forget' strategy, hoping to make their money by tricking as many people as possible into accidentally encrypting their files. Now, they are identifying organisations that simply can't afford for mission-critical files to be out of action for any length of time, in the hope of extorting a bigger ransom from them.

Mobile ransomware:
Like most cybercrime trends, what starts on the desktop will eventually spread to the smartphone and tablet. Mobile ransomware works differently to its desktop counterpart but the aim is the same – to prevent users being able to access their files. Mobile ransomware is still a relatively low-profile threat but a growing number of variants targeting mobile platforms are being detected.

Zombie ransomware:
Ransomware strains once thought to be extinct are being revived and equipped with new methods of attack. In an effort to attract more victims with minimum effort, ransomware groups are reusing and updating their existing malware variants with different cryptography or malicious extensions to help them spread more effectively and prevent files being decrypted without a ransom being paid.

Democratisation of ransomware:
Once the province of skilled practitioners, distributing ransomware is now open to everyone regardless of their technical ability. Would-be criminals can invest in ransomware-as-a-service, buying access to an existing ransomware set-up which they can then tailor according to their preferences. Commercial ransomware-as-a-service providers offer similar services to other legitimate online businesses, such as live customer support. In return, they receive a share of the profits their customers generate.

17 per cent of businesses have fallen victim to ransomware[2]

Anatomy of a ransomware attack

Ransomware typically finds its way into corporate networks when users open malicious email attachments or visit compromised sites, known as watering holes. Recently, however, some ransomware variants have been designed to spread laterally through networks.

The malware will try to evade antivirus software and, if successfully installed, will encrypt a user's files, preventing the user accessing them.

The ransomware will then request a ransom, usually in the region of several hundred dollars, to release the files. If the victim decides to pay the ransom, they will have to transfer the fee to the ransomware writer in a cryptocurrency such as Bitcoin. Once the payment has been registered, the user will receive a cryptographic key allowing them to decrypt files and regain access to their system. Although in some cases the files aren't released even if the payment is made.

The wiper threat:
Although Petya/NotPetya looked a lot like traditional ransomware, it was something perhaps ultimately more dangerous: a wiper. Ransomware has always had profit as its goal but a subset of malware writers is just as happy wreaking havoc as making money. While Petya/NotPetya did have a ransomware component, it's thought that it was politically motivated and sought mainly to cause economic damage by disabling vital systems – leaving organisations caught in the crossfire.

Ransomware remains an issue for all organisations despite security teams' familiarity with the threat. But the evolution of new variants, technologies and social engineering techniques means that security operations should never become complacent. Ransomware is a quick win for cyber criminals. If defences against traditional attacks can be strengthened and staff better educated to be more resilient threat actors will change and adapt their approach. They won't be willing to give up their payday so easily.

About LogRhythm

LogRhythm is the pioneer in Threat Lifecycle Management™ (TLM) technology, empowering organisations on six continents to rapidly detect, respond to and neutralise damaging cyberthreats. LogRhythm's TLM platform unifies leading-edge data lake technology, artificial intelligence, security analytics and security automation and orchestration in a single end-to-end solution. LogRhythm serves as the foundation for the AI-enabled security operations centre, helping customers secure their cloud, physical and virtual infrastructures for both IT and OT environments. Among other accolades, LogRhythm is positioned as a Leader in Gartner's SIEM Magic Quadrant.

www.logrhythm.com

[1] Cyber-extortion losses skyrocket, says FBI http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[2] Cyber security breaches survey 2017 (Department for Culture, Media & Sport): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf