In Partnership with

TREND MICRO™

mti™

Managing Data Securely

How to COMBAT the Rising RANSOMWARE THREAT

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

A message from the author...

Ransomware is a form of malware, and no organisation or individual is immune to it. As purely profit-driven attacks, the perpetrators of ransomware attacks do not care who they extort money from (usually in Bitcoin), with attacks involving targeted devices (such as laptops, smartphones, wearables or tablets), being locked until payment is received for an 'unlock' key.

As ransomware threats continue to evolve, the defences of enterprises need to catch up, and with the rapid expansion of the ransomware threat landscape (in part, thanks to the development of the IoT), defenders are scrambling to find ways to fight back.

While the threat of ransomware is not strictly new, the expansion of the threat over the past year was deemed enough to warrant a full-day seminar at the 2017 RSA Conference, with a dozen global experts examining the latest malicious-attack phenomenon.

Sourced from 245 IT decision makers in UK organisations larger than 1000 employees, this eBook is aimed at shedding light on the awareness and readiness of IT departments to deal with the growing threat of ransomware.

We hope that you find the eBook useful, and that it assists you in your efforts to combat one of the most prolific forms of global malware.

MTI Security Team

The ransomware landscape

Recently, there have been cyber-attacks on the US Democratic Party, the Ukrainian power grid and the central bank of Bangladesh, highlighting a scale and boldness of cyber threat previously unseen.

Ransomware is one of the most ‘en vogue’ threats of the last 18 months and is essentially malware for data kidnapping; an exploit in which the attacker encrypts a victim’s data and demands payment for the decryption via a key.

> *Cyber-attacks will continue to evolve and the rise of internet connected devices gives attackers more opportunity to use threats like ransomware. The public and private sectors must continue to work at pace to deliver real-world outcomes and reduce the threat to organisations, the public and critical services.*

Ransomware can spread through e-mail attachments, infected programs and compromised websites, and is often also referred to as a cryptovirus, cryptotrojan or cryptoworm.

There are two commonly accepted types of ransomware: lockscreen ransomware and encryption ransomware. Lockscreen ransomware shows a full-screen message that prevents you from accessing your PC, mobile device or files, requesting you to pay money (usually bitcoin) as a ransom to gain access to your device or files.

Encryption ransomware (as the name suggests) changes your files so you can’t open them. It does this by encrypting the files, before making the same demands for giving up access to the files.

Statistic

Almost three quarters of IT decision Makers (73%) say their organisation has been infected by ransomware in the last 24 months.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

Responding to ransomware

Although it is at the forefront of any discussion about security today, ransomware has only been a major part of the malware scene since around 2014. The threat however, is still evolving, and IT professionals are sure to encounter even more advanced ransomware in 2017.

While a return to security basics can help avoid infection and alleviate recovery from such an attack, the question remains; how prepared are businesses for ransomware attacks?

Attacker exploits are more likely to be successful if security teams are unprepared, so cybersecurity executives and organisations must respond to the challenge with an effective mix of strategy and technology.

The key message for cybersecurity executives is to use increased business awareness of the risk posed by ransomware to support a new, targeted approach that draws on the expert resources of trusted technology partners.

The challenge now is for IT and security professionals to turn the threat posed by the ransomware epidemic into an opportunity to establish better security and business practices across wider organisational structures.

> *One in three infected organisations pay hackers to get data back. Losing data is the most common worry affecting organisations; but fear of the loss of productivity, and reputational damage, recovery costs and lost revenues are also pressing concerns.*

Statistic

66% of organisations infected by ransomware paid the ransom.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

Ways to combat ransomware

Ransomware is a profitable market. For victims (individuals and organisations alike), even those who decide to pay the ransom, the consequences can be expensive; with indirect costs like downtime and system recovery, incident analysis and response, and significant impact to brand reputation costs and auditing.

IT managers who want to avoid the pain of ransomware need to have a 'start-to-finish' strategy for protection that includes a full menu of ransomware prevention tools.

Reducing the attack surface, blocking malware on desktops and keeping out phishing attacks are areas that IT decision makers must consider. However, systems management and patching tools, endpoint security suites and email security gateways are equally important too.

IT managers should evaluate each of these tools to be sure that they're getting maximum benefit out of these types of protection.

If patching isn't happening and excess software is installed, use system management tools to remediate. And, if malware is still getting onto end-user desktops, find out whether it's because your ransomware prevention tool needs replacing or if a configuration needs updating.

Similarly, if phishing attacks and unwanted attachments are getting through the email security gateway, look at what can be done using existing tools to increase protection and keep ransomware from actually making its way into the enterprise.

> *Recovering data encrypted by a ransomware attack is next to impossible. Having a robust data backup process, email filtering and antivirus software can go a long way in blunting the threat posed by ransomware. In fact, it is often the only way to recover data if you are unwilling to pay the ransom demanded by cyber-criminals.*

Statistic

66% of organisations provide company-wide training on IT security that covers the dangers of ransomware, whilst 26% provide information on ransomware in their employee handbook and discuss it at staff inductions.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

Planning your response

There is an old phrase, often attributed to Benjamin Franklin: “an ounce of prevention is worth a pound of cure.” And this is applicable to the ransomware threat.

While ransomware threats can cause serious damage to an enterprise, there are some security measures that can reduce the risk of such an attack and improve overall company-wide security practices.

There are some key steps organisations should consider in terms of gauging their readiness for a potential attack before implementing preventative measures:

- How prepared are you?
- What does detection and analysis look like?
- Containment, eradication and recovery
- What does post-incident activity and communications look like?

Prevention measures include:

1. Making sure your data is backed up
2. Train employees to be alert to, and avoiding opening phishing emails
3. Install a security software that can detect websites where ransomware goes for encryption keys
4. Use a good antivirus program which will detect older versions of the virus

> *Outright prevention of ransomware attacks is practically impossible and anti-virus software alone cannot guarantee protection. However, there are some essential steps organisations can take to reduce the risk and impact of ransomware attacks.*

Statistic

Just over one in ten (12%) of organisations leave themselves vulnerable to being infected with no response plan in place.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

What's on the horizon for 2017?

Ransomware does not discriminate and there have been a number of high-profile examples of hospitals and government agencies essentially being held hostage for bitcoin payments after ransomware has encrypted business-critical files over the last 12 months.

At the same time, ransomware has also plagued consumers by encrypting information and data of sentimental value, such as family photos, videos and other information.

Ransomware attacks grew markedly in 2016 and cyber-attacks (particularly ransomware and DDOS) exploiting the insecurity of the Internet of Things are expected to rapidly increase this year too.

Affirming the very real threat, recent findings from the National Cyber Security Centre highlighted that hackers attempting to compromise Industrial Internet of Things (as well as personal) connected devices through malware like ransomware, are among the biggest threats to the security of UK companies and citizens in 2017.

> *Ransomware has become prevalent in the last year. The explosion of smartphones, connected watches, televisions and fitness trackers could mean that ransomware is set for a big increase in 2017 too.*

Statistic

Just over nine in ten (92%) of IT Decision makers think the number of ransomware attacks will continue to grow in frequency and severity in 2017.

Ransomware through a GDPR filter

The Data Protection Act of 1998 compelled businesses to ensure that appropriate technical and organisational measures were in place to secure personal data held, and the Information Commissioners Office (ICO) guidance clearly states that disruption due to ransomware incidents should be avoided through additional security protocols being in place. And, as it stands, a breach of the Data Protection Act 1998 can lead to a monetary penalty being imposed of up to £500,000.

We are however, presently in the midst of wide reaching and extensive data protection reforms, largely in the guise of the General Data Protection Regulation (GDPR).

Organisations in the EU and outside that are considered controllers and/or processors of EU citizen data will be required to achieve compliance with the General Data Protection Regulation (GDPR) by May of 2018. The new legislation will focus on data protection from the initial identification and protection of PII through to the required prompt notification of a data breach incident to the relevant supervisory authority.

The GDPR requires companies to take far more detailed and extensive steps than the existing 1998 Act, and with the scope of PII set to increase dramatically, the threat represented by ransomware is a clear and present danger. GDPR will require companies to formulate new strategies and practical approaches to malware, like ransomware, if they are to ensure compliance with GPDR and avoid substantial monetary fines come May 2018.

> *With tighter and more regulated legislation coming into play across all sectors, it is important for organisations to consider the serious fiscal penalties of failing to prepare for cyber threats like ransomware.*

Statistic

Almost nine in ten (87%) organisations are planning, or taking steps to secure Personally Identifiable Information (PII) from ransomware and cyber threats and prevent fines from the incoming GDPR.

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

10 stats you didn't know about Ransomware...

1. **21% of ITDMs have been hit by ransomware twice in the last 24 months** & 1:10 have been infected 3 times
2. **On average, 40% of employees have been affected** by the most recent ransomware infection
3. The most common reasons for deciding to pay ransoms include: the worry of being fined for data loss (26%)
4. The most common reasons for deciding to pay ransoms include: impact on the corporate reputation (21%)
5. **Worryingly, almost 1:10 companies (8%)** do not have any IT training to cover the dangers of ransomware

6. **43% of organisations without ransomware protection** say they do not have enough resources within the team to manage it
7. Almost half (49%) of ITDMs think ransomware will grow more rapidly in 2017 than previous years

8. 13% of organisations are not taking any steps to prevent ransomware fines in relation to incoming GDPR legislation
9. **40% of organisations without ransomware protection** say they do not have enough available budget to support these plans
10. **Over half (51%) of organisations are currently reviewing their requirements** of GDPR and will take steps after

How to COMBAT the Rising RANSOMWARE THREAT

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

Contact MTI Today

Managing Data Securely

MTI engage with clients at every level, delivering a full consultancy service, to understand their business risks and vulnerabilities in an ever-changing threat landscape. MTI deliver a range of solutions that can be delivered on premise, as a managed service or in a cloud environment addressing issues such as, ransomware, GDPR, and Cyber Essentials compliance.

For more information on developing effective cyber security strategies to mitigate the threat of ransomware please contact us using the details below.

Call us on +44 (0)1483 520 200
Email us at ukinfo@mti.com

MTI Technology Limited, Riverview House, Catteshall Lane, Godalming GU7 1XE