Ten ways to protect your organisation from ransomware

By Paul Williams

28 Apr 2016

If you've been listening to the news lately, you would have heard of a number of companies being affected by ransomware. Organisations and users are concerned about the recent surge in this form of cyber attack and they should be. Ransomware is nasty stuff.

Paul Williams

But with some careful preparation, you can significantly lower your risk of being infected, and reduce the impact on you or your organisation should you get hit.

Ransomware is a form of malware that infects devices, networks, and data centres and prevents them from being used until the user or organisation pays a ransom to have the system unlocked. Ransomware has been around since at least 1989, when the 'PC Cyborg' trojan encrypted file names on a hard drive and insisted users pay $189 to have them unlocked. In the interim, ransomware attacks have become increasingly sophisticated, targeted, and lucrative.

The impact of ransomware is difficult to calculate since many organisations opt to simply pay to have their files unlocked - an approach that doesn't always work. But a report on the Cryptowall v3 ransomware campaign, issued in October of 2015 by the Cyber Threat Alliance, estimated that the cost of that single attack was $325m.

Crypto ransomware

Ransomware generally works in one of several ways. Crypto ransomware can infect an operating system so that a device is unable to boot up. Other ransomware will encrypt a drive or a set of files or file names. Some malicious versions have a timer and begin deleting files until a ransom has been paid. All demand that a ransom has to be paid in order to unlock or release the blocked or encrypted system, files, or data.

On 31 March 2016, the US Cyber Emergency Response Team and the Canadian Cyber Incident Response Centre issued a joint warning about ransomware following several high-profile infections at hospitals.

According to this alert, infected users often get a message displayed on their device's screen saying something like:

- Your computer has been infected with a virus. Click here to resolve the issue.
- Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine.
- All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data.

©ginasanders via 123RF

In some circumstances, this warning is displayed with embarrassing or pornographic images in order to motivate the user to get it off their system as fast as possible. But in every situation, systems are taken offline, critical data becomes unavailable, productivity is halted, and business operations are harmed.

Ransomware can be delivered in a number of ways, but the most common is as an infected file attached to an email. For example, today I received an email claiming to be from my bank. It had the right logo, links to real bank URLs, and my name. The body of the message explained that they have detected suspicious activity on my account and that I needed to install an attached file in order to verify my credentials. This seemed like a legitimate issue. But it wasn't. It was a phishing attack.

The giveaway to me, of course, was that no bank should ever send a file and ask you to install it - certainly not to validate your credentials. Instead, the attached file was infected with ransomware, which would have loaded onto my system if I had clicked on it.

Drive-by downloading

But email attachments aren't the only mechanism for infection. Drive-by downloading is another, where a user visits an infected website and malware is downloaded and installed without the user's knowledge. Ransomware has also been spread through social media, such as web-based instant messaging applications. And recently, vulnerable Web servers have been exploited as an entry point to gain access to an organisation's network.

Here are ten things you need to do to protect yourself and your organisation from the effects of ransomware:

1. Develop a backup and recovery plan. Back up your systems regularly, and store that backup offline on a separate device.

2. Use professional email and web security tools that analyse email attachments, websites, and files for malware, and can block potentially compromised advertisements and social media sites that have no business relevance. These tools should include sandbox functionality so that new or unrecognised files can be executed and analysed in a safe environment.

3. Keep your operating systems, devices, and software patched and updated.

4. Make sure that your device and network anti-virus, IPS, and anti-malware tools are running the latest updates.

5. Where possible, use application whitelisting, which prevents unauthorised applications to be downloaded or run.

6. Segment your network into security zones, so that an infection in one area cannot easily spread to another.

7. Establish and enforce permission and privilege, so that the fewest number of users have the potential to infect business-critical applications, data or services.

8. Establish and enforce a BYOD security policy which can inspect and block devices which do not meet your standards for security (no client or anti-malware installed, anti-virus files are out of date, operating systems need critical patches, etc.)

9. Deploy forensic analysis tools so that after an attack you can identify a) where the infection came from; b) how long it has been in your environment; c) that you have removed all of it from every device and d) that you can ensure it doesn't come back.

10. This is critical: **Do not** count on your employees to keep you safe. While it is still important to up-level your user awareness training so employees are taught to not download files, click on email attachments, or follow unsolicited web links in emails, human beings are the most vulnerable link in your security chain, and you need to plan around them.

Here's why: for many of your employees, clicking on attachments and searching the internet is part of their job. It is difficult to maintain the appropriate level of scepticism. Second, phishing attacks have become very convincing. A targeted phishing attack uses things like online data and social media profiles to customise an approach. Third, it is simply human nature to click on an unexpected invoice or critical message from your bank. And finally, in survey after survey, users feel that security is someone else's job, not theirs.

Hopefully, you have a recent backup and you can wipe your device and reload it with an uninfected version. Here are some other things you need to do:

• Report the crime.
• Paying the ransom is no guarantee.
• Contact experts.
• Have a Plan B.

Rise in sophistication

Cybercrime is a for-profit business generating billions in revenue. Like most businesses, cybercriminals are highly motivated to find ways to generate revenue. They use subterfuge, extortion, assault, threats, and enticements to gain access to your critical data and resources. Ransomware is not new. But its recent rise in sophistication and distribution is the latest in an escalating trend to find new and unexpected ways to exploit individuals and businesses that operate online.

Now, more than ever, security is not something you add to your business. It is integral to doing business. Make sure you are partnering with security experts who understand that security is more than a device. It is a system of highly integrated and collaborative technologies, combined with an effective policy and a life-cycle approach of preparing, protecting, detecting, responding, and learning.

Security solutions need to share threat intelligence in order to detect and respond efficiently to threats anywhere across your distributed environment. They need to be woven into your network fabric so they can protect you seamlessly as your networked environment evolves and expands. They need to be able to adapt dynamically as new threats are discovered. And they need to never get in the way of you doing business the way you need to do business.

ABOUT PAUL WILLIAMS

Paul Williams is the country manager SADC for Fortinet.
- Digital trust: the currency of the future - 21 Jul 2017
- Managing the attack surface of a smart city - 29 Dec 2016
- Four key strategies to secure cloud migration - 21 Nov 2016
- Ten ways to protect your organisation from ransomware - 28 Apr 2016
- Layer 7: Data centre security and traffic challenged from all fronts - 29 Oct 2015

View my profile and articles...