Curo

Mini White Paper:

Ransomware: How to protect your business against this growing threat

CURO SUPPORT SERVICES
68 Lombard Street,
London, EC3V 9LJ

TEL: 0207 177 7111
EMAIL: info@curosupport.co.uk
WEB: www.curosupport.co.uk

MINI WHITE PAPER

Ransomware: How to protect your business against this growing threat

Sponsored by: Curo Support Services
Stuart Lang, May 2017

Situation overview

Ransomware is an increasingly prevalent form of cybercrime, which is allowing both traditional hackers and some not-so-technical newcomers to extort great sums of money in a very short space of time. Though this practice is a relatively new concern for anyone with digital data, ransomware has actually been around for longer than you may realise – in fact some reports put the first known case as far back as 1989.

In the intervening years, it has become a quick and relatively easy way for cybercriminals to make money from unwilling victims – everyone from huge international corporations to unsuspecting individuals using their home devices.

So what exactly is ransomware, why is it so hard to detect and what practical measures can you take to avoid becoming the next victim?

What is ransomware?

Ransomware is the relatively new term being applied to any method of encrypting and withholding a user's own data, before charging them for it to be unlocked and released back.

For example, ransomware might typically encrypt a company's digital records, so that no client data could be read or accessed. A sum of money would then be requested for its safe release, often with the threat of it being completely destroyed if payment is not made within a certain number of days or even hours.

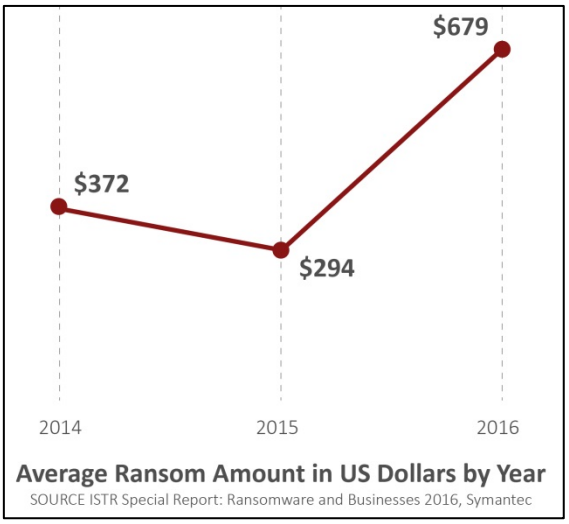
But it is not just businesses that are at risk. Individuals have also been targeted in recent years, with such things as their music collection (on iTunes, for example) being placed under lock and key until a ransom is paid for its safe release.

Ransomware is a devastatingly effective form of cybercrime as it plays on the fear of losing digital assets – as well as all the fallout and negative press that will come from such a loss.

Just as in any hostage situation, the prospect of paying up is not the only problem facing a victim because the outcome – even after the money has been paid – is never guaranteed. Frequently, the hackers will have scrambled the data to such an extent that, even after files have been released back, they can sometimes be largely useless anyway.

Curo

One of the most common strains of ransomware software goes by the name 'CryptoLocker'. First released in 2013, this trojan can lock certain files on local and mounted network drives using public-key cryptography (a process involving two keys, one public and one private, so that only the holder of the private key has access to the data). In CryptoLocker's case, the private key is held on its own secure servers.



Average Ransom Amount in US Dollars by Year
SOURCE ISTR Special Report: Ransomware and Businesses 2016, Symantec

CryptoLocker is most often propagated through infected email attachments. Once it is downloaded and has encrypted the files (often in a matter of seconds), a message is presented to the user offering the safe release of their data - provided a fine is paid. If the money (generally via bitcoin) isn't paid up by the typically short deadline, the private key is then destroyed, leaving the data forever encrypted.

CryptoLocker itself is relatively easy to remove from a computer although, unfortunately for those affected by this trojan, doing so will not decrypt the files – meaning that deleting it has little to no effect on the eventual outcome.

DIY code appeals to non-technical hackers

The ransomware threat has increased significantly in recent years – thanks in no small part to the emergence of so-called RaaS, or Ransomware as a Service.

This is when hackers, with various modified versions of CryptoLocker (and the like), effectively lease their software to any would-be cybercriminals. Those renting the software can then set about trying to extort money out of companies or individuals – without having to embark on the long and technical process of learning how to create these programs from scratch. Once a ransom is paid for data, the RaaS providers often take a percentage of the profits, in addition to the small fee they are paid by the individuals who seek access to their malware in the first place.

These developments mean that virtually anyone has access to ransomware and can – with limited technical knowledge and very little outlay – begin trying their hand at digital extortion.

For this reason, as more information is stored online, and ransomware tools become more readily available, this threat is only likely to increase.

Why is ransomware so hard to detect?

Ransomware is well known by web hosts and law officials alike. However, recognising the problem and solving it are two very different challenges. Sophisticated cyber criminals have gone through numerous processes to ensure their software can evade detection – even by many of the big-name antivirus packages.

Curo

Firstly, communication between infected devices and the ransomware's command and control servers is itself encrypted – making it difficult to detect in network traffic. Additionally, the use of tor browsers and bitcoins for payment make it incredibly difficult for the authorities to trace any transactions back to the operator.

Most fascinating - and indeed alarming – is the malware's so-called polymorphic behaviour, which means it has the ability to mutate itself to create a new variant as required, but to not do it so much that the function is altered. It can also remain dormant on a system and wait to make an attack – in order to strike at the most opportune (and profitable) time.

Who are the top targets?

As described above, literally anyone can be targeted by ransomware, from global brands to individuals on their home PC. In fact, many cybercriminals actively target members of the general public, as they'll generally be less likely to know how they can fix the problem themselves – meaning a ransom payment (albeit smaller in value) is more likely to be forthcoming.

It's worth noting, however, that some companies, individuals or sectors are more at risk than others.

Small businesses are a popular target, as their systems are often less protected than much larger firms employing their own technical teams.

There is also a heightened risk for any companies who put a lot of stock in their public perception. Falling prey to such attacks is bad news and can decimate a company's credibility, so the pressure for these organisations to simply pay up – rather than reveal they have been compromised - is much greater.

Public institutions are also in danger, because they will often have huge databases of confidential information. With the threat of this data being deleted or exposed, the option of paying up for its safe return is a pervasive one. Not only that, public institutions often run outdated systems and have staff members who are not trained on the impact of ransomware – making it that bit easier to trick them into downloading it.

How was the NHS compromised in May 2017?

On Friday 12th May 2017, the news broke that a widespread cyberattack attack had claimed the National Health Service amongst one of its highest profile victims. The ransomware variant, which had reportedly affected over 40 NHS Trusts in England and some NHS bodies in Scotland, is known as WannaCryptor. This variant also goes by the name of WanaCrypt or Wcry.

WannaCryptor spreads via malicious email attachments sent to victims, which once opened, download the payload that encrypts a victim's data. However, once the encryption is underway, this specific ransomware also exploits a bug in file sharing protocol Windows Server Message Block (SMB) on unpatched or unsupported versions of Windows desktops and servers.

This highlights the importance of never opening an email attachment you do not recognise and ensuring that all windows operating systems are kept fully up-to-date.

Protecting your business

The increase in high-profile ransomware attacks, underlines the importance of protecting your own organisation's data. Though attackers are becoming more innovative with each passing day, and their techniques more sophisticated, there are three main ways that you can help to mitigate your own risk.

1. **Keep your antivirus and all system software up-to-date**

Though some ransomware uses ingenious techniques to bypass antivirus software, a full and up-to-date system can provide an effective first-line defence for your network. It is also vital to apply Windows patches and security updates on a regular basis, since certain forms of ransomware exploit known vulnerabilities in your operating system.

2. **Never click on a link you do not recognise**

Despite robust antivirus protection, it is often a user's action that results in an organisation falling victim to a ransomware attack. Clicking on links or opening attachments in spam emails is one of the surest ways to infect your system. Never open anything unless it's from a trusted source. If you're not sure, call the sender first to check on its authenticity.

3. **Ensure you have a watertight backup**

A secure, offsite backup can render even the most malicious ransomware completely impotent. Indeed very often, the only sure-fire way to help a victim recover from a major ransomware attack is to restore files from an alternative location. But remember, some malware can access data saved in the cloud, so it is important that your backup solution is designed and managed by a professional.

By following all these guidelines, and educating users about the threat ransomware poses, you and your data should be at significantly less risk.

Further Information

For more information on ransomware or any other cyber security threat to your business network, please contact our technical team using the following details:

CURO SUPPORT SERVICES
68 LOMBARD STREET
LONDON, EC3V 9LJ
0207 177 7111
info@curosupport.co.uk

Curo