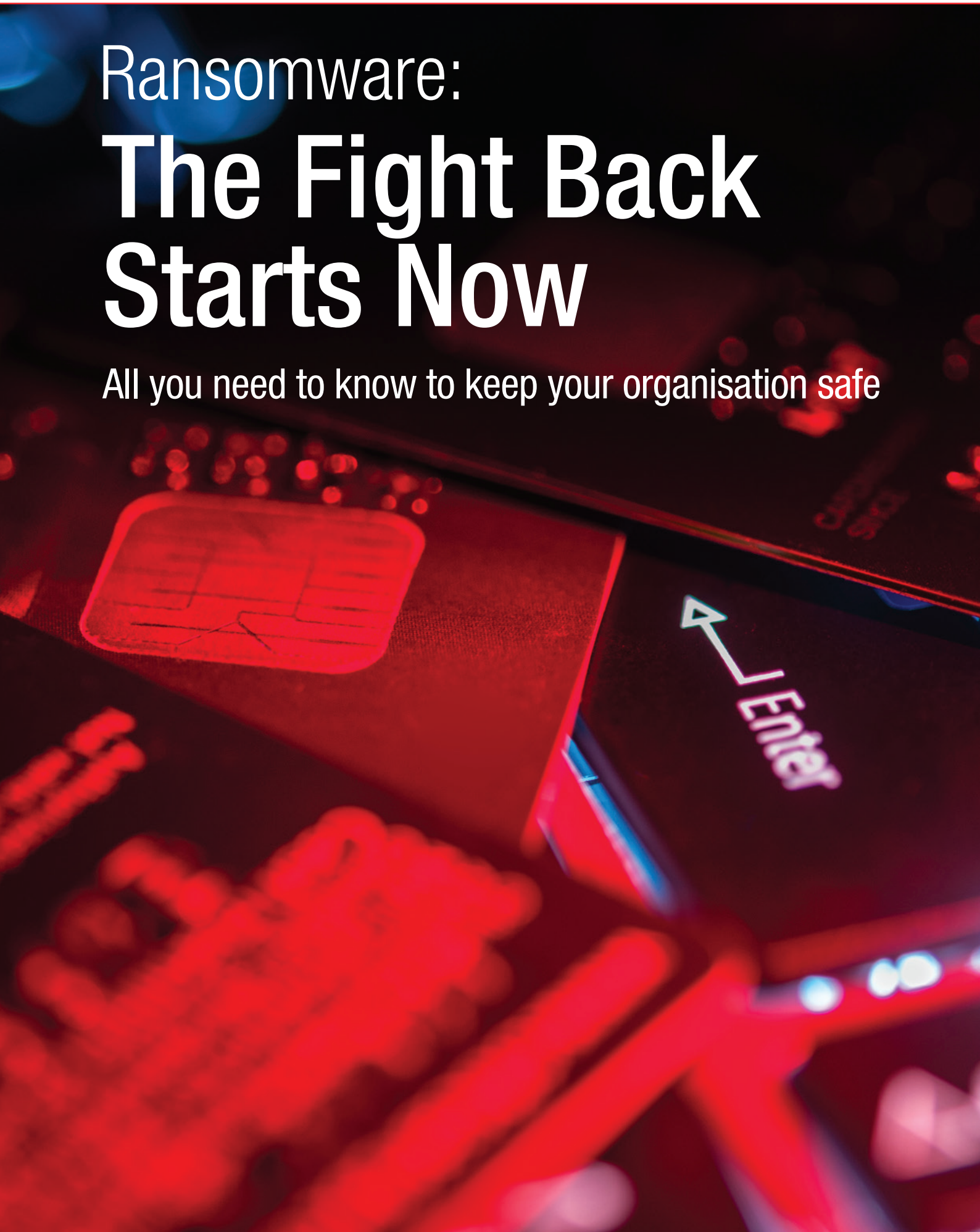
HEAT® software

Ransomware: The Fight Back Starts Now

All you need to know to keep your organisation safe



Introduction

If any modern cyber threat could be described as having reached epidemic proportions, it's ransomware. The combination of intimidation, extortion and technology has proved a winning formula for the cybercriminals, and a major headache for organisations locked out of their mission critical data.

The truth is, ransomware has been around for over a decade, but it's only in the past 12-24 months that infections have really taken hold. Off-the-shelf toolkits have democratised the means to launch attacks and cybercriminals have shifted their focus from consumers to organisations.

The true scale of the problem is difficult to pinpoint, as many incidents continue to go unreported and in some countries there simply is no reporting infrastructure. But we can point to a huge uptick in incidents from various sources. The FBI might cover just the United States but it's a reliable indicator. According to them, there have been over 4,000 attacks per day since 1 January 2016. That's a 300% increase on the 1,000 daily attacks seen in 2015.

As long as ransomware campaigns continue to generate profits, there'll be no let up. So the onus must be on organisations, led by their IT security teams, to fortify systems against attack. This report will guide you through the basics: what ransomware is, how it works, how it has developed over recent months, and where the key threats lie today. Then we'll illustrate how a layered approach to security is the best strategy to mitigate the risk of infection.

All stats were correct at the time of publishing, but with a threat as fast-moving as ransomware, expect them to change as the weeks and months progress.

What is ransomware?

Ransomware has become the favourite way for cybercriminals to generate quick and easy profits. It's a type of malware which locks a user or organisation out of their computer system, demanding a fee to regain access.

It can be split into two main categories: screen lockers and those using encryption, or crypto-ransomware. Historically the former was more common, with the black hats requesting payment via premium rate SMS, money transfers and even snail mail cheques. Some of these variants tried to scare victims into paying by flashing up messages claiming that they had accessed illegal content such as child pornography, and that only a payment would halt criminal proceedings.

Then in 2013, everything changed as CryptoLocker burst onto the scene. It was the first major ransomware family to use encryption to lock users out of their files. Payment is demanded in order to receive the decryption key, with users warned that if they fail to meet the deadline their data will be gone forever. The rise of this crypto-ransomware also coincided with the use of Bitcoin and other virtual currencies for payment, and Tor and other anonymising networks to hide communications, making it harder to trace the black hats behind the scams.

Ransomware is also prevalent in the mobile space. Unlike in the PC world, most variants are simple screen blockers because Android automatically backs up to the cloud, so encryption is less impactful. Also, the OS has built-in security which makes it tricky to access all files on the device.

Today, crypto-ransomware is by far the most popular type, accounting for around 95% of all ransomware.

How does it work?

No ransomware variant is alike, but there are some commonalities in attacks which we can study:

1) The first stage involves getting the ransomware onto a victim's machine. Most common is a phishing email loaded with a malicious attachment. Sometimes users will be prompted to enable macros on opening the doc. Other vectors include malicious links, taking the user to a compromised site which will trigger a drive-by-download in the background.

2) Once on the machine, the ransomware can exploit a vulnerability to install and gain system access. Exploit kits such as Angler are frequently used by cybercriminals here. Vulnerabilities could be exploited in the OS, third party apps, web browsers, servers etc.

3) Ransomware will then employ anti-detection techniques such as disguising itself as legitimate processes, in order to evade security tools. Some versions will go further and disable anti-malware processes and configure themselves to load on boot even in Safe Mode.

4) The ransomware will then connect to a command and control (C&C) server, potentially downloading additional code, and uniquely identify the individual machine. The C&C will relay the text to be used in the ransom demand. Most C&C servers today are hidden from investigators on the TOR or I2P networks.

5) The malware will remove any back-up files and then perform a secure key exchange with the C&C before encrypting a pre-selected range of file types, which could run into the hundreds. Original files are overwritten with encrypted versions and strong, virtually uncrackable encryption is used. The ransomware will move through the machine and, if it can, the organisation's network, encrypting as it goes.

6) The final step is to demand the ransom, in the user's native language, including strict instructions about the time limit imposed and payment details. Bitcoin is the preferred method, for anonymity reasons.

If the victim does decide to pay the ransom, they would expect to receive a unique decryption key. Even though the cybercriminals' business model depends upon the assumption that decryption keys will be produced, it is not a given that one will be forthcoming, or even work. That's why organisations are always recommended NEVER to pay the ransom.

Who does it affect?

The short answer to this is: everyone. Seeing bigger returns and more potential victims, the black hats have over the past two years focused their attention increasingly on organisations rather than consumers. The share of corporate users attacked virtually doubled from 2014/15 to 2015/16 – from 6.8% to 13%.
They do not discriminate. From hospitals to schools, utilities providers to local government – every type of organisation in every sector in every country is potentially at risk. For example, universities and NHS Trusts in the UK have been hit hard by ransomware in the last year according to latest FoI requests and according to the US Government, ransomware attacks in the US have increased in frequency by 300% year on year with 4,000 incidents a day being reported.

This is now a cyber pandemic.

It's all about the money. Ransomware is expected to become a billion-dollar enterprise this year, having already generated $209 million in the first quarter, according to the FBI and until organisations better protect themselves and/or stop paying the ransom, it will continue.

The cost to your business

It's no coincidence that ransomware is increasingly focused on organisations. The black hats know that these victims have the money to pay up and will be more desperate to do so to avoid any adverse repercussions. There are also more potential points of weakness to exploit. It takes just one user to click on a malicious link, visit a compromised site or open a malicious attachment and the entire organisation could be brought to a standstill.

So how do attacks affect the organisations they're aimed at?

First there's the cost of paying the ransom itself – which is what around two-thirds of victims choose to do. Increasingly, the cybercriminals will raise their price if they think the organisation will be desperate enough to get its data back. The Hollywood Presbyterian Medical Center famously admitted to handing over around $17,000 in Bitcoins as it was the "quickest and most efficient way" to gain access back to key systems.

But the cost of paying the ransom can pale in comparison to the other knock-on effects of an attack. Lost productivity, service disruption, remediation and clean-up costs, damage to reputation and even potential legal costs can all have a major adverse effect on the victim organisation. There could even be life-threatening repercussions if systems are taken offline in, say, a medical/healthcare environment.

When it hits, an infection can quickly spread through an organisation, especially if there are limited controls in place to isolate it. And the downtime that follows can be a far bigger burden than the financial cost of the ransom. CryptoLocker, for instance, can take down multiple offices in one sweep, should it infect a shared server. A business that tries to restore from a ransomware attack from a traditional backup can often lose weeks of work due to lost files, plus a day or more of downtime while computers are wiped and reloaded. Given the commercial and financial pressures facing organisations today, even a few hours is a long time to be offline, let alone a week.

The arms race

Ransomware may be serving its masters well, but that hasn't stopped them from developing new strains and continually adding functionality. Researchers disagree over the most common variants in 2016. The likes of TeslaCrypt, Locky, Petya, Cerber, CTB-Locker and CryptXXX have all been mentioned as causing widespread disruption, but there are likely hundreds of variants out there.

Here are a few new trends to be aware of that illustrate the ever-evolving nature of the threat landscape, and the importance of effective, layered protection:

Off-the-shelf cryptoware: strains like Cerber now offer cybercriminals with little technical expertise a means of jumping on the ransomware bandwagon. It operates on an affiliate model, with new recruits offered up to 60% of profits in return for disseminating the malware. It's pre-packaged, simple to use and even comes with online help.

Information-stealers: variants like the latest version of CryptXXX now come with a new module designed to steal the victim's passwords. So the cybercriminals can extort you by encrypting your files, and access to your online accounts.

Anti-security tools: ransomware is increasingly being designed to evade the unwanted attention of security tools. The Locky family features encryption of the payload, preventing any analysis of the executable. The malware also requires a command-line parameter to run properly, which confuses and disrupts sandbox tools.

Backdoor access: one recently discovered piece of ransomware, disguised as a Pokemon Go app, even creates a backdoor on the victim's machine. This would allow an attacker to return to the machine, potentially to steal data or commit other malicious actions.

How to protect your organisation

To effectively mitigate the risk of ransomware infection the most important thing to remember is defence-in-depth. Building up layers of protection provides the best antidote to the multitude of different types of malware and infection vectors out there. The following are all important elements:

Back-up: do this regularly and follow the 3-2-1 rule – three copies, on two different media and one offsite

Application control: intelligent whitelisting controls what can run in your environment and means unapproved programs like ransomware simply can't execute. Try to include Memory Injection Protection capabilities which protect against advanced in-memory exploits, including DLL Injection and Reflective Memory Injection attacks, which can evade standard endpoint security products

Regular patching and remediation: ransomware exploits vulnerabilities in order to work. Reduce these through effective, centralised patch management for all operating systems, native and third-party applications, plug-ins and add-ons.

User education: turn your staff from weakest link to first line of defence by educating them how to spot suspicious emails.

Anti-malware: effective anti-malware can stop many forms of ransomware. It should include advanced heuristics capabilities to spot zero day exploits that might evade traditional signature-based AV.

Device control: this will mitigate the risk of infection via attachable devices like USBs.

Incident response: update your IR plan to include ransomware and practice regularly from start to finish to ensure all stages work.

Security reporting: Leverage your IT Service Management system to create a way for your users to report and learn about phishing attempts that might lead to a ransomware attack.

HEAT Software
Website: www.heatsoftware.com
@HEAT_Software