YOUR MONEY OR YOUR DATA – THE DANGER OF RANSOMWARE

Go beyond prevention with total endpoint protection

Next generation endpoint security solutions

Predict, prevent, detect and respond, at machine speed

SentinelOne's deep file inspection (dfi) engine prevents today's most sophisticated file-based malware.

SentinelOne is recommended for its combined total cost of ownership and security effectiveness in the first public test of its kind.

Ransomware Protection. Guaranteed. - SentinelOne is the only endpoint protection company to guarantee its technology; $1 Million (One Million Dollars) in Guaranteed **Ransomware** Protection.

Why guarantee a technology? You wouldn't purchase a car without a warranty, right? What assurance do you have that your security vendor's claims will hold true? By 2020 it's estimated that the global cybersecurity market will balloon to nearly $170 billion. This is up from the $60-70 billion that was spent in 2015. Despite this massive growth in spending, nearly 72% of respondents in a recent Black Hat attendee survey felt it was "likely their organization would have a major data breach in the next 12 months." This just doesn't add up.

It's time for security companies to back their technology and provide users with the financial assurance they deserve against **Ransomware** attacks. SentinelOne users now have that assurance.

If we are unable to block or remediate the effects of a **Ransomware** attack, we will reimburse your company or organization up to $1000 per endpoint, or $1,000,000 in protection overall for the company. Guaranteed.

Ransomware is here: What you can do about it?

WHAT IS RANSOMWARE?

Ransomware is a malicious software virus that infects a computer, network or data. During the infection, your computer will either be locked or your data encrypted, held hostage, and the only way you can regain access is by paying a "ransom". Ransom is typically demanded in Bitcoini, a largely anonymous currency, which is often used in cyber black markets. **Ransomware** is classified as a "denial of access" attack, denying the victim access to the electronic device or data stored on the device until a ransom is paid. Distributing **Ransomware** is a criminal activity, and even though the technology it utilises is quite sophisticated, the prevalence of **Ransomware** hinges on the exploitation of the human element – as do most criminal activities. Malware such as **Ransomware** is not a new phenomenon, but it has become increasingly widespread and invasive in recent years.

Block **Ransomware** before it touches your data. **Ransomware** gets past antivirus and backups fail constantly. You have a choice: leave your company's data at risk, or add another line of defence to prevent data loss and theft.

In a survey of **Ransomware** victims:

100% of respondents had up-to-date antivirus

58% did not fully recover their data

As of late, **Ransomware** has been getting a lot of press and the attention of the world, and for good reason. **Ransomware** attacks have been on the rise for the past few years and are not expected to go away any time soon.

We all know that **Ransomware** takes part of your system and doesn't give it back until the attackers have been paid, but what does that mean? How often does paying the ransom, actually pay off?

In this Whitepaper, we go into the details of what **Ransomware** means, where it comes from, how it acts and what you can do to stop it in its tracks.

Total endpoint protection, one powerful platform

Next Generation Endpoint Protection software – SentinelOne

Defend every desktop, laptop and critical server against today's most sophisticated attacks. Only SentinelOne gives you the layered protection you need across the entire threat lifecycle, in a single next-gen security solution.

WHO CREATES RANSOMWARE?

Ransomware is created by criminals with the intent to vandalise, swindle, blackmail or demand ransom from victims. These criminals violate technology in order to create a platform to engage in criminal activity, and are usually referred to as cybercriminals. **Ransomware** criminals use coercion tactics in order to ensure they get what they want. Some coercion tactics involve scaring victims into thinking they have committed a crime by visiting a restricted website, or threatening to delete some data every 30 minutes until the ransom is paid. What exactly is it that they want? **Ransomware** is inflicted for two main reasons: monetary gain and acquiring sensitive data to sell on online black markets.

The **Ransomware** business model today is so mature that cybercriminals are going as far as working to provide a pleasant "customer" experience (strange as it may sound) in order to ensure that it is as easy as possible for victims to actually convert money into Bitcoin and pay the ransom in question. In some cases, this includes the provision of telephone support. Other **Ransomware** "professionals" have identified the opportunity to commoditise **Ransomware** and have begun offering "**Ransomware**-as-a-service". This means they actually offer the **Ransomware** virus for sale, or they offer to run and administrate the **Ransomware** operation on behalf of someone else for a fee or percentage of the ransom. The impact of which is that **Ransomware** attacks are increasing and becoming more prevalent as criminals don't even need to be able to write code to jump on the **Ransomware** bandwagon.

HOW DOES RANSOMWARE INFECT?

With the landscape of technology increasing and expanding – the prevalence of smart mobile devices, the internet of things expanding, and humans relying on technology for everyday operational activities – **Ransomware** is granted a rich playing field in which to populate. There are 4 most common ways that **Ransomware** can gain access to your computer

1. SPAM EMAILS AND UNSOLICITED EMAIL ATTACHMENTS

An easy and popular way for **Ransomware** to spread is via emails and unsolicited email attachments. The emails trick the user into opening it, or opening the attachments (usually by making the content appear enticing for the user, or using "spear phishing" techniques). Spear phishing is the newest version of phishing. Phishing is a method whereby cybercriminals and attackers attempt to obtain sensitive personal information from individuals via electronic communication in order to launch a malware attack. Phishing coaxes individuals to surrender personal information by presenting bait, or the promise of appealing incentives. Spear phishing depends on familiarity with the person targeted and can resort to measures as extreme as using a person's web presence (their online activity, favoured websites, social network interaction, etc.) against them.

This means cybercriminals will often monitor their victims, learning about them and then tailoring and personalising the content used in the attack before striking. By doing this, they increase the odds of succeeding in getting the victim to engage with the malware.

2. INFECTED REMOVABLE DRIVES

Malware can spread through removable drives (USB flash drives and external hard drives). It is usually created to automatically install on any machine that it is connected to. If a computer or any other type of device is connected to a network, the malware can spread through the network to other machines. When a digital device infected with **Ransomware** connects to wireless internet connections, this can also pose a huge threat to the rest of the devices connected to that wireless network, and infection can spread rather quickly. Some **Ransomware** creations can spread easily without being detected by anti-virus software.

3. BUNDLED WITH OTHER SOFTWARE

Ransomware can be bundled together with other software applications that are downloaded and installed. The victim may think they are only downloading a certain legitimate application, not knowing that it is a Trojan Horse designed to trick them into activating the malware on their device. For this reason, make sure that any software application that is downloaded is done so from a safe source and is secure and trustworthy to install. Most anti-virus and anti-malware software can verify the integrity of applications before they are installed.

4. COMPROMISED WEBPAGES

Ransomware can take advantage of software vulnerabilities in order to infect a computer. When the victim visits a compromised or hacked website the **Ransomware** can utilise pop-ups or other malicious tactics that mimic online advertisements in order to engage with the victim. Sometimes not even a click is needed for the **Ransomware** to covertly seize control of the computer. Simply viewing the page with an unpatched vulnerability on your device is all the **Ransomware** needs.

WHAT ARE THE DIFFERENT TYPES OF RANSOMWARE?

There are two main types of **Ransomware**: Locker **Ransomware** and Crypto **Ransomware**.

LOCKER RANSOMWARE:

Locker **Ransomware** typically locks access to the computer interface, only allowing the user to interact with the ransom demand. It generally doesn't attack the underlying operating system or data, only denies access to it.

CRYPTO RANSOMWARE:

Crypto **Ransomware** is the more malicious one of the two and is designed to encrypt all valuable data stored on the computer or network. It moves fast, it stays undetected until ransom demands are made and it is a bigger threat to data loss. For the different names and a list of the most common types of **Ransomware**, visit the Kaspersky Lab website for a detailed report.

HERE'S HOW RANSOMWARE HITS SA

Ransomware is increasingly becoming a problem in SA and local companies are not reporting incidents for fear of reputational damage, says a security company. "Statistics in South Africa remain vague as organisations are reluctant to reveal the extent to which they have been targeted by **Ransomware**," security firm Panda Security said in a statement to Fin24.

"However, anecdotal evidence points to this being a widespread issue - Panda is increasingly being approached by organisations looking for a real solution after being afflicted with **Ransomware**," Panda Security said.

Unlike other malware, **Ransomware** is direct financial targeting. Once cyber criminals have encrypted data on a device, they demand payment, usually in the form of Bitcoins. However, electronic funds transfers have also been employed.

"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," said Paul Williams, major account manager for security firm Fortinet.

According to data from Kaspersky Lab, 41% of South African companies recognise the threat posed by **Ransomware**, also known as Cryptomalware.

The malware enters company networks through email attachments and some of the malicious software programs include Trojan-Ransom.Win32.Onion, Trojan-Ransom.Win32.Locky (known as Locky) and Trojan-Ransom.Win32.Scraper (TorLocker).

Locky, the most recent **Ransomware**, has already been detected in 114 countries and SA has experienced the sixth highest number of attacks at 220, the highest number in Africa.

"Among other Trojans, Locky caught our attention because it was so active and spread so pervasively and quickly. We also noticed that the attacks weren't partial to any particular region, where we have received notifications about attacks in over 114 countries across all continents – no other **Ransomware** Trojan to date has targeted so many countries at once," said Fedor Sinitsyn, Senior Malware Analyst at Kaspersky Lab.

Data from Kaspersky Lab shows that 2.3% of South African computers may have a cyber infection over the last 24 hours.

EXPERTS DO NOT RECOMMEND THAT VICTIMS PAY RANSOMS.

"Paying for ransom is a dangerous option. For starters, there is no guarantee your files will be returned or that the malware will be removed. Will the hacker exploit you again in six months' time?" said Eset South Africa of **Ransomware** scams.

Ransomware programs typically encrypt user files on computers, including those with pdf, doc, docx, xls, xlsx, ppt, pptx, jpg, jpeg, bmp, tiff, png, mpg, mpeg, avi, 3gp, mp4, m3u, mp3, wav, zip and java extensions among others with a 128 bit key.

Demands for payment will begin with about $300, but many cases the amount is increased the longer you take to pay – usually in Bitcoins.

According to Symantec, users' sentiment toward the encrypted data "can lead to irrational behaviour", and payment to the cyber criminals.

RANSOMWARE ATTACKS ON SOUTH AFRICAN ORGANISATIONS SPIKE IN NOVEMBER

South Africa is among the countries impacted by a 10% increase in **Ransomware** attacks in November, using Locky and Cryptowall, this is according to Check Point. As a result, South Africa moved up the list of 117 most attacked countries – to number 31 in November, from 58 in October.

In its monthly Global Threat Index, a ranking of the most prevalent malware families attacking organisations' networks, Check Point found both the number of active malware families and number of attacks remained close to an all-time high as the number of attacks on business networks continued to be relentless.

Continuing a trend first detected in October, Locky **Ransomware** continued to increase in prevalence, with a further 10% increase in the number of attacks using this family – a pattern that was mirrored by the fifth most common malware, Cryptowall.

Locky, which started its distribution in February 2016, spreads mainly via spam emails containing a downloader disguised as a Word or Zip file attachment, which then downloads and installs the malware that encrypts the user files. Locky was the no.1 malware family in the largest amount of countries (34 countries compared to Conficker, which was the top malware in 28 countries).

The pattern highlights the growing threat posed to corporate networks by **Ransomware** and suggests that many organisations are simply paying ransoms to secure the return of their files, making it an attractive – and lucrative – attack vector for cyber-criminals.

Once again Conficker retained its position as the world's most prevalent malware, responsible for 15% of recognised attacks. Second-placed Locky, which only started its distribution in February of this year, was responsible for 6% of all attacks, and third-placed Sality was responsible for 5% of known attacks. Overall the top ten malware families were responsible for 45% of all known attacks.

The three most common malware distributed in South Africa in November were:

Virut – Botnet used in DDoS attacks, spam distribution, data theft and fraud. The malware is spread through infected devices such as USB sticks as well as compromised websites and files.

Sality – Virus that allows remote operations and downloads of additional malware to infected systems by its operator. Its main goal is to persist in a system and provide means for remote control and installing further malware.

Conficker – Worm that allows remote operations and malware to be download. Infected machines are controlled by a botnet, which contacts its Command & Control server to receive instructions.

The Ramnit banking Trojan saw the largest increase in attacks globally in November, entering Check Point's top 10 ranking for the first time as the 6th most common malware. It more than doubled its amount of infections since last October, and was mainly seen in Turkey, Brazil, India, Indonesia and the U.S. Ramnit is used to steal banking credentials, FTP passwords, session cookies and personal data.

For the eighth consecutive month, HummingBad remains the most common malware used to attack mobile devices globally.

Mobile malware families continued to pose a significant threat to businesses. The three most common mobile families were:

HummingBad – Android malware that establishes a persistent rootkit on the device, installs fraudulent applications and enables additional malicious activity such as installing a key-logger, stealing credentials and bypassing encrypted email containers used by enterprises.

Triada – Modular Backdoor for Android which grants super-user privileges to downloaded malware, as helps it to get embedded into system processes. Triada has also been seen spoofing URLs loaded in the browser.

Ztorg – Trojan that uses root privileges to download and install applications on the mobile phone without the user's knowledge.

Doros Hadjizenonos, Country Manager of Check Point South Africa, explained, "**Ransomware** attacks are still growing in volume for a simple reason – they work and generate significant revenues for the attackers. Organisations are struggling to effectively counteract the threat posed by this insidious attack form; many simply don't have the right defences in place, and may not have educated staff on how to recognise the signs of a potential **Ransomware** attack in incoming emails. This, of course, only makes it even more attractive to criminals.

"Organisations must use advanced threat prevention measures on networks, endpoints and mobile devices to stop malware at the pre-infection stage, such as Check Point's SandBlast™ Zero-Day Protection, Threat Extraction, and Mobile Threat Prevention solutions, to ensure that they are adequately secured against the latest threats," added Hadjizenonos.

Check Point's threat index is based on threat intelligence drawn from its ThreatCloud World Cyber Threat Map, which tracks how and where cyber attacks are taking place worldwide in real time. The Threat Map is powered by Check Point's ThreatCloudTM intelligence, the largest collaborative network to fight cybercrime, which delivers threat data and attack trends from a global network of threat sensors. The ThreatCloud database holds over 250 million addresses analysed for bot discovery, over 11 million malware signatures and over 5.5 million infected websites, and identifies millions of malware types daily.

SOUTH AFRICAN COMPANIES FALLING PREY TO RANSOMWARE

It hasn't been a good start to the year for many South African businesses as their employees returned to work only to discover that they had been locked out of their computers and company databases had been encrypted. Demands for large payments to be made, typically in the form of untraceable Bitcoins, in order to regain access inevitably followed. When payments were made by those who decided to take their chances and pony up the money in an attempt to continue doing business as usual, some of them were then advised that the amount had subsequently increased. Presumably this was because the original amount was deemed too affordable given the readiness of these hapless businesses to pay up.

"We've recently witnessed a major surge in **Ransomware** attacks as an unprecedented number of organisations have approached us to help them secure their servers and networks against malware", comments Grant Chapman of local data security and CRM provider Camsoft Solutions. "There are still many companies out there with inadequate or no protection against malware and many of them are generally ignorant of the consequences. This, together with a general naivety that it might never happen to them, is going to result in many more unfortunate organisations having to pay the price in more ways than just the money. Those affected will also not be restricted to large corporations which usually try and keep knowledge of an attack a secret, knowing what the reputation damage and other fallout could be. When these organisations report that they are wiping clean all their servers and computers and reinstalling all their software from scratch it's fairly obvious what has transpired. Some companies have even had to resort to reinstalling databases and mail servers that are over a year old after not keeping off-site backups. And then others who left backup devices connected to their servers at the time of the attack have had all their current backups encrypted as well. Regaining access to infected files by paying the ransom is also very risky because the malware is still resident on the infected machines and can very easily be re-activated for yet another ransom demand," adds Chapman.

Ransomware has become big news in the US and elsewhere in the world and it was only a matter of time before South Africa started becoming a target too. **Ransomware** attacks worldwide doubled in the last two quarters of 2016, indicating just how lucrative the practice is, with the FBI estimating that profits related to **Ransomware** exceeded a billion dollars last year.

"Usually, it is not so much the ransom itself, but business downtime and other consequences that will really disturb your business", comments Eija Paajanen of F-Secure Corporation. "Paying the possible ransom will of course hurt. But what will probably hurt more are the other repercussions resulting from a successful **Ransomware** attack. First, you have the lost business time. Think about an online store for example. Having your site down will have a direct effect on the bottom-line. The city of San Francisco was forced to give free rides to all commuters after **Ransomware** hit their transportation system. A major target for **Ransomware** has been hospitals and healthcare providers. What if you can't access patient data or sign in patients?

There would be no operations during that time. There will be other effects as well. Your IT staff has to spend a lot of their valuable time searching for the problems, isolating them and trying to fix them. In many cases, it is not just the infected computers that are rendered powerless, but also other devices need to be pulled down from the network to avoid further damage. Meanwhile, most of your employees will not be able to work and you face quite significant productivity losses, regardless of whether you pay the ransom or not. Secondly, there is the possible loss of critical data. In some cases, we have seen customers successfully back up their financial data, but not other business-critical assets. For a design agency, for example, the loss of their image and design files would be unbearable. Coming back to hospitals and other medical practices, the welfare of patients could be severely compromised by not knowing what medications or treatments they required or what their medical history was, should their data disappear. Thirdly, coming back to the potential loss of patient data, the problems that you might face with your operations are not the full story either. Privacy laws and regulations are pretty strict when it comes to personal data and the probability of facing penalties is high.

As for financial data, there are other laws governing the obligations to keep archives for several years. Therefore if a **Ransomware** attack makes you lose the data for, let's say even the current quarter, you would face a huge task to restore the data to be prepared for a possible audit two years later..."

One key element of protecting an organisation against **Ransomware** and other malware attacks is security awareness training, which is key to preventing employees from clicking on phishing links in e-mails. So, what should you do if and when you find out that your organisation has been hit by **Ransomware**? Here's some advice from Andy Patel, one of the security experts at F-Secure: "If your organisation has been hit by crypto-**Ransomware**, stop, take a breath, and respond to the incident in a level-headed manner. You're going to want to start by isolating and remediating affected machines before restoring data from backups and ensure that you have the right protection on your network to prevent it happening again. Make sure you don't restore the original infection vector during that process. And when your systems are back up and running, remember to kick off a root cause analysis. Learn from the experience and improve your processes and systems in order to avoid future infections, keeping your data security software updated regularly. The more prepared your organisation is for the eventuality of a crypto-**Ransomware** attack, the less likely you'll end up panicking and doing something that could be more damaging."

We're also seeing a major shift towards hosted data, such as our Maximizer CRM solution in the cloud, due to the highly sophisticated threat environment that exists currently", comments Chapman". The hosted servers are protected against malware with F-Secure's Endpoint protection by a team of specialists who take responsibility for ensuring that the servers always have the latest updates, are backed up off-site and monitored for any untoward activity. They aren't connected storage devices, which are still susceptible to attacks, and the connections between users and the server are encrypted with SSL security. Outsourcing the responsibility for your data to experts who make it their business to safeguard it makes a lot of sense. There is also a reduced likelihood of infection from malware such as that used for **Ransomware** attacks because sophisticated firewalls help prevent security breaches, caused for example by employees inadvertently initiating attacks by clicking on attachments in phishing e- mails. Whilst it is difficult to ensure that all IT resources are 100% protected against any potential threat, given the constantly changing nature of the threat landscape, there are tools available to minimise threats and stay ahead of the game and one should use these tools wherever possible."

If you wish to assess your current capabilities to handle **Ransomware** attacks or any other type of malware attack for that matter, please check out F-Secure's practical handbook for endpoint protection. It will give you the tools to assess your current capabilities, give guidance on best practices and help evaluate the most critical requirements for an endpoint protection solution that can stop **Ransomware** and other malware in its tracks.

RANSOMWARE – THE MALWARE THAT IS HOLDING SOUTH AFRICAN COMPANIES AT GUNPOINT

Ransomware is a type of malicious software (malware) that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back.

There are different types of **Ransomware**. However, all of them will prevent you from using your computer, server or now even mobile device. They can:

- Prevent you from accessing your operating system
- Encrypt files so you can't use them
- Stop certain apps from running (such as your web browser)

They will demand that you do something to get access to your device or files:

- Demand you pay money – normally in Bitcoins
- Make you complete surveys

Often the **Ransomware** will claim you have done something illegal and that you are being fined by a police force or government agency. These attacks can be incredibly lucrative: One researcher found that a hacker made more than $1 million in a single day off of hapless users desperate for their data back. These claims are false. It is a scare tactic designed to make you pay the money.

Ransomware has the potential to attack the Internet of Things. In one instance, a researcher was able to infect a TV with **Ransomware**. **Ransomware** is now even attacking smart phones.

Last month, one hospital paid $17,000 in ransom when **Ransomware** attacked its computer system. The computer network was down for more than a week, and patients had to be transferred to other hospitals.

PREVENTION TIPS

Essential first steps

- Use a reputable antivirus solution and ensure it is up-to-date.
- Regularly backup your important files.
- Ensure all software is up-to-date especially highly targeted software like Java, Acrobat Reader etc.
- Avoid clicking on links or opening attachments or emails from people you don't know or companies you don't do business with.
- Awareness is key - Educate all users about the threat.

Advanced

- Have a pop-up blocker running in your web browser.
- Show hidden file-extensions.
- Filter EXEs in emails.
- Disable files running from AppData/LocalAppData folders.
- Disable Remote Desktop (RDP).

Dealing with an Infection

- Disconnect from WiFi or unplug from the network immediately.
- Remove the malware with your AV vendor’s removal tools; additionally look at the list provided below.
- Use System Restore to get back to a known-clean state.
- Set the BIOS clock back.
- Decrypt the encrypted data (tools listed below).

REMOVAL/PREVENTION TOOLS

Computers

- Solutionfile.trendmicro.com
- Labs.bitdefender.com
- Foolishit.com
- Blog.malwarebytes.org
- Mobile
- Play.google.com

Decryption tools

- Noranson.kaspersky.com
- Decryptcptolocker.com
- Blog.emsisoft.com
- Talosintel.com
- Thirdtier.net
- Bitbucter.org

THE DANGERS OF RANSOMWARE

The challenges businesses face with **Ransomware** include business disruption and loss of productivity; financial loss without any guarantee the data will be restored; and possible compromise of company intellectual property, customer data and confidential information. Jeremy Matthews, regional manager, Panda Security Africa responds to typical questions on this ever-present threat.

How are businesses dealing with the threat of Ransomware?

South African businesses are slowly realising that advanced threats such as **Ransomware** require more robust security than convention antivirus can offer, and are beginning to implement more advanced security solutions. However, organisations without adequate protection face having to pay the ransom and hope that their data can be retrieved, either from the criminals or from the companies' backups. We do not advocate the payment of the ransom as this only creates an incentive for criminals to continue these malware campaigns and does not guarantee that data will be returned.

Do we have an idea of the level of attack businesses in SA are facing?

Unfortunately there are very few reliable statistics regarding **Ransomware** attacks in South Africa, this is partly because companies are generally unwilling to admit that they have fallen victim to **Ransomware**. However anecdotal evidence points to a very high prevalence of attacks in South Africa. **Ransomware** attacks appear to hit in waves coinciding with the release of each new strain of **Ransomware**.

What are the blind spots that companies with existing security solutions have?

There are a few important "blind spots" to be aware of:

The users themselves are often unknowingly responsible for the initial infection and general security education is the first step to ensure your company remains safe and secure.

Reliance on traditional security solutions – almost all traditional security solutions work in much the same way, they rely on the malware either matching a sample (malware signature) they have taken previously or triggering some kind of heuristic or behavioural rule. This creates a window for what are called Zero-day threats. A Zero-day threat is simply a threat that has never been seen before in the wild and thus has never been seen by an antivirus. We refer to this as the malware window of opportunity.

Businesses overly rely on individual layers or protection such as AV instead of taking a multi-layered approach to securing their network.

What level of employee is likely to be targeted?

Like any other criminal, hackers are looking to optimise their profits by targeting high profile individuals or institutions. That being said, no employee or individual is immune to these attacks as hackers will use a specific individual's endpoint to access the organisations network and encrypt data on that network. **Ransomware** as a malware category is normally very broadly targeted going after anyone they can get infected.

What is best practice in terms of dealing with Ransomware?

In addition to employing advanced security solutions, the best way to prepare yourself would be to ensure you're following best practice:

- Do regular backups (ideally off-site).
- Mail and URL filtering for dangerous file types – common infection route.
- Ensure systems are patched and up-to-date.
- Educate your users to the dangers of **Ransomware**.
- Ensure users are aware of suspicious emails and attachments.

If you are infected, then generally speaking it is already too late, your only options are to either restore from any backups you may have, lose the data or pay the ransom.

You mentioned needing advanced solutions for combating Ransomware. What are some of these solutions and how do they work to protect against advanced threats?

The current threat landscape is incredibly dynamic and cyber criminals are constantly developing new ways to attack. This requires a more advanced approach to security – the industry response to this has been in the development of endpoint detection and response (EDR). According to Gartner, EDR was created to satisfy the need for continuous detection and response to advanced threats – most notably to significantly improve security monitoring, threat detection and incident response capabilities. Panda Security's EDR solution is a cloud based managed solution that will monitor all actions on the endpoint and classify them as either malware or goodware. If a new program tries to run and has not been automatically classified as goodware the program will be blocked until it can be classified by PandaLabs. The solution is available in two versions Adaptive Defence and Adaptive Defence 360, the latter being the first of its kind combining Panda's traditional endpoint protection and EDR to monitor and protect individual endpoints.

Anything else that you think is important?

It is always important that companies have visibility and control of their network so that areas of risk can be identified and dealt with before a breach occurs. This can be a challenging task, however a security information and event management (SIEM) tool can ease this burden. SIEM tools allow for access to information like network load, software usage, data flow, data loss detection and much more. The AD 360 offers an advanced reporting tool as well as integrating with SIEM solutions to provide detailed data on the activity of all applications run on your systems.

ANTIVIRUS VS SENTINELONE

	SentinelOne EPP	Legacy Antivirus + Add-on Tools	Next Generation Antivirus	Endpoint Protection and Response
Advanced Signature-Less Prevention	✓	✗	✗	✓
Behaviour-Based Detection	✓	✗	✗	✓
Machine Learning	✓	✗	✗	✗
Policy-Driven Mitigation and Remediation	✓	✓	✗	✓
Detailed Forensics	✓	✗	✗	✓
Next-Gen Protection for Windows, OS X and Linux	✓	✗	✗	✗
Cyber Intelligent Systems Monitoring and Response	✓	✗	✗	✗

Ransomware-as-a-Business

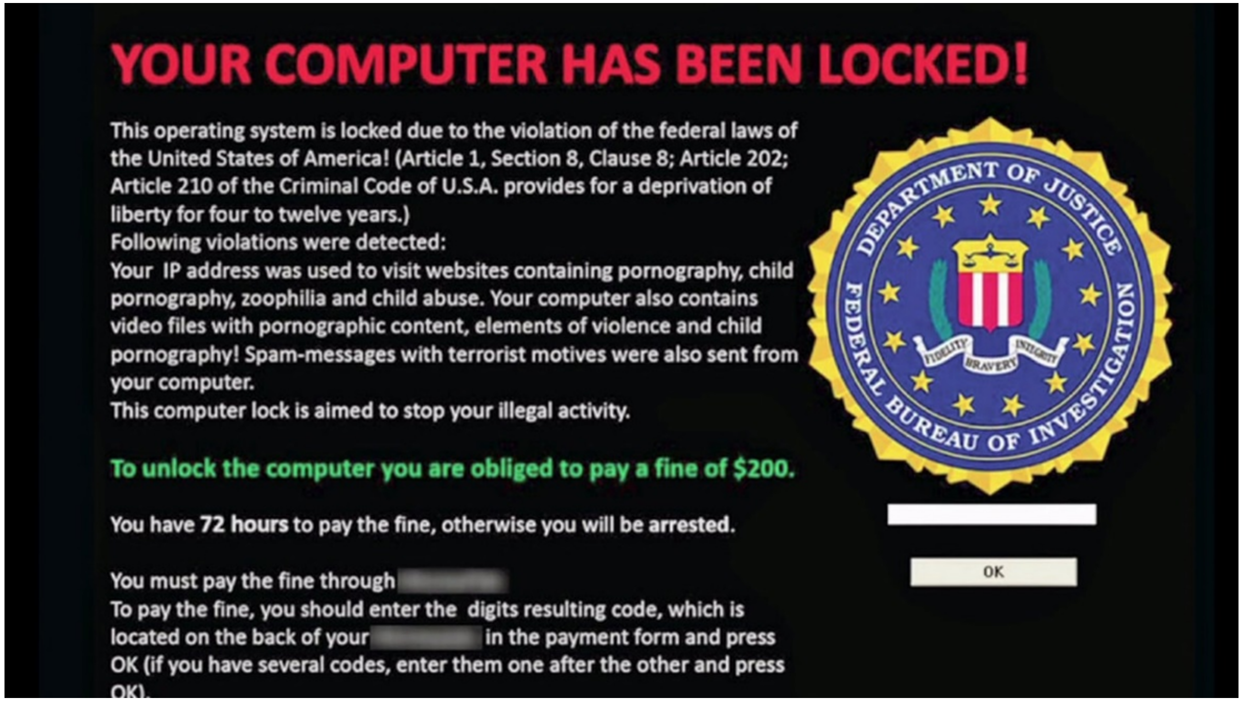
- As the market grows, ransomware attacks developed into ransomware **operations**
- Sporadic infections became streamlined campaigns
- The clear monetary incentive is an engine that drives this “industry” to constantly improve and evolve

The Questions to Ask

- What would you do if you were locked out from accessing your own information?
- What would happen if your information is made public or sold?
- How much would you be prepared to pay to keep your business out of harm’s way?
- Does your antivirus supplier have a guarantee against ransomware?
- Would you trust a free ransomware tools and free antivirus to protect you?
- Does your antivirus supplier send you automated SMS alerts when your computer or server is under threat?
- Does your antivirus supplier respond when your computer or server is under attack?
- Can you Antivirus respond to the threat, remotely intervention
- Can your antivirus stop unknown and sophisticated threats dead in their tracks?
- Do you receive monthly reports detailing the number of threats you were protected against?
- Does your antivirus prevent, detect and respond to advanced threats immediately?

Common Advice

- Backup Your Data
- Whitelisting
- Patch your Operating system and Applications
- Maintain an updated Antivirus
- Scan all software downloaded from the internet
- Restrict Users from installing software –Least Privilege
- Avoid enabling Macros
- Do not click on unsolicited Web links in emails
- Don’t click on adverts on social media



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

RANSOMWARE