InfosecPartners
CYBERSECURITY

#SECURINGSCHOOLS

OH WHAT BIG EYES YOU HAVE

With cases of Ransomware and Cyber Fraud showing no signs of slowing down, Infosec Partners outlines ways to be better at identifying security threats and prevent your school from being the next victim.

The big bad wolf is real and it's actively targeting schools and the information they hold.

Once upon a time…

A dear little girl, wearing a red hood, brought her sick grandmother a basket of food. The grandmother lived out in the woods and despite the little girl promising her mother that she would be safe and stay on the path, the little girl wandered off it to pick some flowers.

If you hadn't recognised this well-known fairy tale, would you have predicted that two cases of fraud and criminal intent would have followed? Despite the dramatic rise in orchestrated cybercrime in recent years and the heavy investment by organisations in security technology, some very troubling statistics have recently been released regarding two types of cybercrime: Ransomware and BEC (Business Email Compromise).

Ransomware on the rampage

Ransomware has been around since 1989, but it was only from 2013 that criminals started to realise the potential of monetising this type of attack when ransomware evolved to using RSA- 1024 and AES-256 encryption. 'Cryptowall' was the first ransomware to use RSA- 2048, whilst 'Locky' has affected 24 million since first appearing in mid-February 2016. 'Petya' another recently identified ransomware type, causes a blue screen of death by overwriting the master boot record (MBR) of computer hard disk drives, meaning that it is impossible to load the Operating System even in Safe Mode.

Currently the most prevalent money-making scheme employed by cyber criminals, the rise of ransomware has been astonishing. According to the 2015 Cyber Threat Alliance report 'Lucrative Ransomware Attacks', throughout the whole of that year, a total of $325 Million (~£225 Million) was taken using ransomware. The US Federal Bureau of Investigation reports that ransomware is now on the rampage, with the amount taken for the first three months of

What is Ransomware?

- A type of malicious software designed to block access to a computer system, files or system functions until a sum of money (the ransom) is paid by the victim.
- $325 Million extorted by Ransomware in 2015. But $209 Million taken in just the first three months of 2016.
- Creators of ransomware use traffic anonymizers like TOR, as well as Bitcoin to receive ransom payments, in order to avoid tracking by law enforcement agencies.
- Ransomware uses every possible attack vector to infect a machine.
- Some ransomware use obfuscation techniques to evade detection from traditional antivirus products.
- Ransomware communication with 'Command & Control' servers is also encrypted and difficult to detect in network traffic.

RANSOMWARE & CYBER FRAUD: Attacks are turning to schools.

2016 rising to $209 Million (~ £146 Million), more than eight times the total for 2015. At this rate ransomware is expected to yield close to $1 Billion by the end of the year unless individuals and organisations improve both their defences and security awareness.

Schools. Victims of ransomware

There have been several notable instances of ransomware attacks including hospitals, local councils and schools. Many organisations are paying the ransom to free their data/ systems without reporting it, partly because they don't want people to think that they're not protecting their computer systems, but one US school district decided to share their story with news outlet CNN.

Charles Hucks, the technology director of Horry County school district in South Carolina explained how within minutes up to 60% of the school district's computers were frozen. He told CNN "You get to the point of making the business decision: Do I make my end-users - in our case teachers and students - wait for weeks and weeks and weeks while we restore servers from backup? Or do we pay the ransom and get the data back online more quickly? We chose to send the payment for one machine first, so that we could ensure that it would work."

The criminals sent a code for one computer and on seeing that this allowed the computer to return to operation, Horry County then paid the equivalent of $10,000 (~ £7,000) into the hackers' Bitcoin account in order to get rest of the ransomed systems back up and running.

Identity and Access Management

Knowing that little Red Riding Hood was going to her grandmother's house, the big bad wolf ran as fast as he could taking a shortcut and it wasn't long before he arrived. He knocked on the door.

"Who's there?" called out the grandmother.

"It's Little Red Riding Hood" replied the wolf.

"Come in child" called out the grandmother. "I am too weak to get up".

The wolf needed no second invitation. He ran in and gobbled her up.

The grandmother in the story was clearly too frail and hard of hearing to thoroughly assess the identity of the person knocking on her door, but would you believe that experienced finance professionals in large enterprises have also been guilty of not suitably confirming the identity of the person with whom they were communicating?

You would never expect your organisation to willingly hand over your personal information to a cybercriminal, but it's happening all the time. That's because hackers are spoofing the email addresses of CEOs and others in positions of authority, so employees don't realize they're transferring funds or sharing sensitive information to a hacker until it's too late.

Identity and access management plays a big part in a cyber security strategy. Managing who has access to what (especially privileged accounts or high value information assets and systems) as well as managing access based on conditional criteria including time, location, and comparison to the baseline norm are all key components. But these technology measures need to be built around robust processes of checks and counter checks.

Multi-Factor Authentication (MFA)

Multi-factor authentication ensures that someone is who they claim to be. The more factors used to determine a person's identity, the greater the trust of authenticity.

There are three methods to prove you are who you say you are.

Something you **know**

This could be your user id and password or PIN, your date of birth, mother's maiden name or any other 'secret'.

Something you **have**

This could be your passport, driving license or other form of ID card. Or it could be a smartcard or token which uses an authentication approach perhaps using time, an algorithm, and a unique identifier to strengthen cryptographic value.

Something you **are**

Biometrics, the use of physical characteristics and traits for identification includes fingerprints, retina scans, face scans, voice prints, hand prints etc.

Multi-factor authentication requires two or more of these factors to be presented to authenticate an identity.

RANSOMWARE & CYBER FRAUD: Attacks are turning to schools.

Business Email is being compromised

The FBI refers to the scam as “Business Email Compromise” (BEC) and like Ransomware it is a fast growing threat because of the success enjoyed by cybercriminals in monetising the scam. Since October 2013, the FBI reports that $2.3 Billion USD (approx. £1.7 Billion)” has been taken through email wire-transfer scams, affecting 17,642 businesses across 7 countries.

One of the more significant examples of BEC came to light in the third quarter results report of FACC AG, an Austrian aerospace parts supplier for Boeing and Airbus.

“On January 19, 2016 FACC AG announced that it became a victim of fraudulent activities involving communication and information technologies. To the current state of the forensic and criminal investigations, the financial accounting department of FACC Operations GmbH was the target of cyber fraud… The damage is an outflow of approx. €50 million EURO (approx. £39 Million)”.

Belgian Crelan Bank was another victim of BEC, and criminals were able to scam an even larger amount reported to be €70 million EURO (approx. £55 Million)

“Thanks to ample reserves, Crelan can comfortably manage this loss without it affecting any of our clients or partners in anyway. The intrinsic profitability of the bank remains unchanged”, said Luc Versele, the CEO of Crelan Bank.

A spokesperson from the bank indicated, “Additional security measures have been put in place in order to reinforce the procedures for internal security”.

Schools and Email compromise

Banks and large enterprise are not the only ones being hit by Business Email Compromise, the statistics from the FBI outlines that the total values includes scams on businesses of all sizes. The Olympia School District in Washington, USA was recently hit. An attacker spoofed the email address of the District Superintendent and sent a phishing email requesting the personal information of staff members employed during 2015.

Personally identifiable information (PII) of more than 2100 employees including 630 teachers was shared including names, addresses, salary information and social security numbers. Were you aware that attackers target PII because it is worth up to 10 times more than Credit Card information on the Dark Web, the online black market for illegal items including stolen hacked data?

Little Red Riding Hood finally arrived at her grandmother’s house. All the curtains were drawn in the house and when Red Riding Hood walked into the bedroom she could barely make out the figure in the bed wearing a night gown. She started to open the curtains and as the dim light seeped into the room she said “Oh Granny, what big eyes you have!”

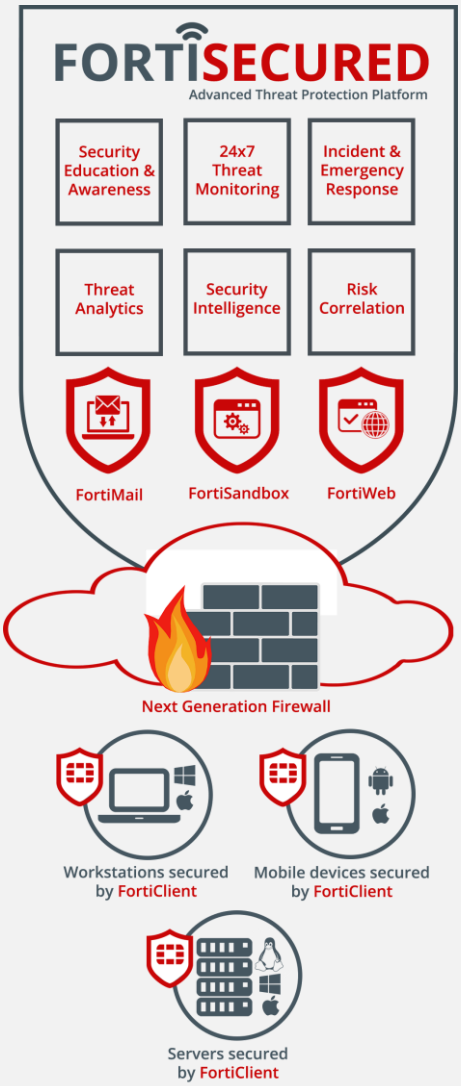
“All the better to see you with my dear” replied the wolf.

THE PROBLEM

Cyber fraud is on the rise. Organisations of all sizes are being exposed with attackers often targeting third party suppliers in order to get to the larger companies. The FACC breach shows how attackers could have been targeting Boeing and Airbus to whom they supply parts.

THE SOLUTION

Work with proven security experts and take a full-spectrum approach to security. A fully integrated platform of security controls and expert ‘Partner of Excellence’ resource will provide advanced threat protection designed to reduce likelihood of attack and minimise impact of any successful intrusion.



RANSOMWARE & CYBER FRAUD: Attacks are turning to schools.

Red Riding Hood continued "Granny, what big ears you have!"

"All the better to hear you with my dear" replied the wolf.

Red Riding Hood started backwards towards the door. "Oh grandmother, what big teeth you have!"

"All the better to eat you with my dear!" shouted the wolf whilst leaping out of the bed.

Who's coming to the rescue?

Unlike the fairy tales, victims haven't always been able to call on a 'Woodcutter' like the one that saved Red Riding Hood and killed and opened up the wolf to rescue the distraught grandmother. All companies that have suffered a high profile security incident through ransomware or cyber fraud had in place a firewall, antivirus protection and an IT department. Standard controls are not adequate to protect against these advanced threats. Technology is not enough and generalist IT teams are simply not equipped with the knowledge and experience needed. Expert security management and awareness programmes are key in combating the rising tide of ransomware and cyber fraud such as BEC.

Next-Generation Antivirus

Static, signature-based solutions simply can't keep up with the rising tide of advanced malware, exploits, and other cyber-attacks. The key to effective endpoint protection lies in the ability to dynamically analyse and predict any threat's behaviour. Cylance Protect is an example of the next generation of antivirus solutions that aren't dependent on signature updates. Using mathematics and machine learning, Cylance effectively teaches a machine to make the appropriate decisions on files in real time to provide security even for previously unseen and 'Zero Day' malware.

Effective Security Awareness & Education

The main vulnerabilities targeted by Business Email Compromise scams are poor levels of security awareness and weak procedures. Infosec Partners are working with organisations like the Police and schools across the UK to provide better security awareness education and decision making capabilities.

A Fully Integrated Security Ecosystem

Infosec Partners' FortiSecured platform provides the expert resource to conduct training and awareness programs at multiple levels within the business, testing the responses and reactions to multiple types of attacks. Infosec Partners manage and monitor the security platform and are contracted to manage the incident process in the event of an attack

The FortiSecured platform is unique. It is the only fully integrated platform of security controls and expert resource available to businesses. The service is specifically designed to both reduce the likelihood of any attack and also to minimise the impact of any successful intrusion.

The technology security platform is designed to extend the clients' existing next generation firewall and AV protection into a fully integrated, seamless protection platform. Fortinet's advanced controls around Sandbox / APT protection, email security and web security are integrated with endpoint software that protects all devices whether they are inside or outside of the corporate perimeter.

InfosecPartners
CYBERSECURITY

ABOUT INFOSEC PARTNERS

A trusted advisor to significant organisations, Infosec Partners provides full-spectrum information security expertise and managed services to some of the world's largest and most sensitive businesses, high-profile individuals and families.

Infosec Partners' flexible security service portfolio allows clients to outsource whole or component parts of their information security requirements, or access specialist security support as needed, when impartiality is critical. Founded in 2004 and head quartered in the UK with a trusted global network, Infosec Partners combines a business-led risk management approach and highly trained advisors, with proven technical capability to deliver optimal security solutions for all types of organisation.

www.infosecpartners.com

Our partners include:

FORTINET

Infosec Partners were named Fortinet's first ever Partner of Excellence, UK.

CYLANCE

Infosec Partners integrates the latest technologies to provide robust security.

Speak with a trusted advisor today:

+44 845 257 5903

secure@infosecpartners.com