The NEW WORLD ORDER of CYBER THREATS

The recent worldwide assault on computer users and the internet involving worms, ransomware, malware and digital currencies, illustrates the complexities of the new threats in cyber space. The scale of the incidents came as a surprise to organisations of all sizes and industries, as well as the average computer user. It also left many cyber security professionals scratching their heads and asking how this could have happened on such a large scale.

This is the new world order of cyber threats.

With cyber risk on the rise, and business interruption a growing concern, we explore in detail the so-called WannaCry and Adylkuzz incidents and provide guidance on how organisations can better prepare for the future.

The changing nature of recent threats

WannaCry is a combination of a self-propagating worm and ransomware that fully exploded onto global networks around the 12 May 2017. It is estimated that around 300,000 - 350,000 computer systems have been impacted and most were infected in the first 24 hours. Traditionally, ransomware has required human support as it is usually triggered by clicking a malignant web link or file attachment. That being the case, hundreds of thousands of infections in a short timeframe would not be possible. WannaCry raised the bar, as the first time there was a worm attached to the ransomware. This worm, built around an exploit called DoublePulsar, latched on to computers with outdated Microsoft Windows software to launch its attack.

Simply put, there is a built-in component in the Microsoft Windows network operating system known as SMB, and it was never designed for secure communication. It was built for printer and file sharing. It has proven vulnerable many times in the past and it is unlikely that many security professionals have installed, configured and managed firewalls that allow this communication, especially from the internet.

Those impacted by WannaCry were left with two choices; either pay the ransom or revert to the last system backup, a choice that unfortunately many organisations have had to make. In many cases, paying ransom is a trigger to further malicious cyber-attacks.

Another major global cyberattack is underway and experts say that it could be even bigger than WannaCry. Adylkuzz operates in an entirely different manner. Pre-dating WannaCry and the resultant hype, the Adylkuzz virus had been using the same exploit since late August 2016. Rather than give you a pop-up asking for ransom, it steals computer power. Why? To mine something called Monero, a digital currency favoured by the darker parts of the internet. To earn money in these digital currencies, like Monero and Bitcoin, you must have the computer power to effectively 'solve puzzles'. Latest estimates are that over 600,000 systems have been infected so far. The only way you would know is that your computer runs slow. There is not much organisations can do regarding this virus, other than wipe their systems, patch and start again.

These two exploits and the scale of their reach indicate we are experiencing a new world order of threats.

Behind the hack: Shadow Brokers

Ransomware has been a big problem in recent times, and accounts for the majority of cyber insurance claims globally. Worms have been around for a while, and many IT security professionals will remember the Nimda and Code Red worms exploiting unpatched systems in the early 2000s. However, seeing a worm attached to ransomware is a new and highly concerning issue. So just how exactly did these threats come about?

In April 2017, an anonymous organisation called the "Shadow Brokers" hacked the US National Security Agency (NSA) and obtained some of the tools that the intelligence body has used to gather information from vulnerable systems. They attempted to auction these for a reputed USD 70 million, but were unsuccessful. They then carved them out into smaller "packages" for a lower value but were still unable to sell them.

The exploit that drives WannaCry and Adylkuzz is one of these tools. It is estimated that there are around 150 other tools out there. The NSA has been criticised by many, including Microsoft, for hoarding hacking tools, as opposed to notifying the vendors so they could fix the vulnerabilities. After the stolen NSA exploits were revealed publicly, Microsoft issued a patch for all supported Windows systems so that SMB would be secure from these kinds of exploits.

Unfortunately many organisations didn't install this patch, and in some cases they couldn't. To Microsoft's credit, after WannaCry they also released a patch for Windows XP which has been an unsupported operating system since 8 April 2014.

The legacy of Microsoft Windows

Applications are dependent on the operating systems they run on. The UK's National Health Service (NHS) has proven to depend on legacy or outdated Microsoft Windows operating systems and they were hit very hard by WannaCry to the extent they had to turn non-critical patients away. Custom applications that have been developed to run on the latest version of Windows will not work on an older version of the program. They would have to be re-developed, which involves cost and a software development life-cycle. As a result of this, many organisations are still using older version of the program. All types of systems never thought of like parking pay stations and billboards running on legacy Windows software have been victims of WannaCry and Adylkuzz.

Fast moving targets: The damage

The financial and physical impacts of WannaCry and Adylkuzz are very difficult to gauge at this stage. They are both very fast moving targets. It is estimated that around 15 Australian businesses have been held to ransom by WannaCry, however many suspect that number is much higher as many organisations would have not reported it. They would have simply reverted to their last system backup, absorbed the business interruption and paid the associated clean-up costs, and moved on.

Adylkuzz was discovered when a researcher was looking at WannaCry and how it worked. The only impact to the end user is that the system runs slow because resources have been prioritised elsewhere, to solve puzzles to earn Monero digital currency.

WannaCry's impacts are covered under most cyber insurance policies. One aspect of insurable loss from Adylkuzz is potential business interruption from slow systems. Another is the remedial costs that could be associated with spreading the malware to other organisations and individuals. Australia is widely considered as a highly litigious society, and with the mounting pressures on organisations to deliver results, it is only time before incidents such as these results in legal liabilities. Whilst the business interruption costs may be significant, the legal costs and settlements may be disastrous, and can potentially cause damage to brand and reputation in the long term.

In the US, recent cyber events are shining the light on actions of directors and officers, with allegations including failure to supervise and failure to approve appropriate systems and controls.

Many observers are predicting the legal defence costs for directors and officers could be between USD 5-8 million.

A well-crafted cyber insurance policy will cater to these exposures, protecting an organisation's balance sheet from liabilities as well as reimbursing the business interruption costs. With these events becoming almost every day occurrences, prudent organisations will be considering the use of insurance as an integral part of their cyber risk mitigation strategies.

DECODING THE TECHNICAL TERMS:

MALWARE: short for malicious software and refers to any software used to disrupt computer or mobile operations

RANSOMWARE: is a type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a ransom is paid.

WORM: a self-replicating malware computer program designed to spread to other computers

EXPLOIT: a software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware

DIGITAL CURRENCY: an internet-based form of currency which enables instant, borderless and anonymous transactions

Considerations for IT risk management

First and foremost: patch your systems as soon as you can.

Regarding Microsoft Windows legacy systems, consider moving them to enclave networks. If organisations have to keep managing old systems then they need to think about improving their security.

From a risk management perspective, the business needs to confirm that the IT and IT security teams are on top of patch management and general software life-cycles.

Cyber risk is a fast-moving target and organisations at all levels must support their technical teams; and be aware that the adoption of new technologies for business advantage often moves faster than the controls required to fully secure them.

The future threat landscape

The emerging trend is that organisations are adopting new technology before they are able to secure them, and this is largely due to the evolution of the Internet of Things and the Industrial Internet of Things. In this evolving digital age, we are seeing increasing levels of information sharing, supply chain and other automation, and general technical advancement. This brings opportunity, but it also brings cyber risk - any system connected to networks has the potential to be hacked.

Verizon's 2017 Data Breach Investigation Report, which is based on the incidents that their forensics team have worked on, says that 73 per cent of the incidents are financially motivated. This is crime, organised crime and state-sponsored actors. As long as people are making money and achieving their goals, cyber-crime will not stop.

Many cyber-crime experts are speculating that WannaCry is a proof of concept. The back-end money generating capabilities of the ransomware were very poorly executed, and many believe it was put out there by the Shadow Brokers to demonstrate the impact that the other 149 exploit tools they stole from the NSA can have, which are all for sale on the dark markets. If this theory is correct then there has never been a time to be more vigilant with cyber risk management than now. Senior management of organisations must understand that we are moving into a new world order of cyber threats.

Unfortunately it is very often that the cyber security teams within organisations are not empowered with the tools they need due to budgetary restraints and the drive to adopt new technologies to facilitate business. In the face of these new threats, organisations need to be more supportive both financially and organisationally to their cyber risk management teams.

How Aon can help

Aon are leaders in cyber risk consulting and insurance solutions. We offer a range of cyber risk management solutions including risk profiling that helps you understand the cyber risk exposures unique to your organisation. We also offer cyber insurance, which can cover ransomware and other cyber incidents. Cyber insurance can include the provision for a cyber incident response team who can assist with the first response to a cyber incident and coordinate the actions required. Please contact us if we can assist you in preparing for, responding, mitigating and transferring risks of cyber incidents.

For all the latest updates about the recent cyber-attacks, please visit our cyber risk information page.

aon.com.au/cyber

Contacts:

Michael Parrant

Cyber Insurance Practice Leader
T +61 3 9211 3485
E michael.j.parrant@aon.com

Stephen Trickey

Director, Growth Strategies
T +61 2 9253 7577
E stephen.trickey@aon.com

Empower Results®

FSG0050 0918