FIGHTING MALWARE
The e-Brief
telecomasia

Sponsored By
CISCO

www.telecomasia.net

telecomasia
QUESTEX MEDIA

The new normal

Data breaches and malware threats

Lachlan Colquhoun

With the rapid growth of the online world has come the growth of a parallel world inhabited first by hackers and now by cyber criminals.

These Black Hats are encouraged by the exponential growth of the online world. Ransomware, for example, started small and was originally targeted at individuals and small companies, now it is in the arsenal for attacks on much larger corporates. Organizations need to accept the reality that attacks, ransoms and breaches are the new normal.

A typical hacker is not always the stereotype of a male teenage hacker wearing a hooded jumper and typing furiously away in a darkened room to crack the passwords of targets, just for fun.

As the Cisco-produced video "Anatomy of an Attack" describes, hackers look at what they do in the same way as anyone else looks at their job. They are proud of their competence and keen to perform their task well.

"I just spy on people and see what makes them click. It's not a bad job," the female hacker says in the video.

She goes on to describe her attack, and how a simple forged email can help perpetrators extort money, and also lead to a massive data breach and damage the reputation of any corporate.

After a period of intense research on the company and its people she begins sending emails to staff purporting to be the CEO, whose "voice" and way of communicating she has learned to copy.

When she sends the mail, it needs to appear like an email from the CEO, not a generic piece of spam, and in creating that believability her research is crucial.

"I get a lot of my information from the sales department, because they are always so quick and eager," she says. "People trust too easily. They don't look at the details."

The fake email includes an invitation from the CEO to open an attachment, which includes malware written not by this hacker, but by the people she works for.

Her skills are specifically around persuading people to click on the attachment. Other people do the rest for her. Ransomware can be bought or rented, the equivalent of downloading software, and hackers can even provide technical support.

The malware freezes the company's systems and they are forced to pay a ransom in Bitcoin before they can receive the decryption key. The hackers have timed their attack perfectly – the company is reporting earnings in two hours.

Ultimately, the ransomware attack is simply a diversion. While the company has been occupied dealing with that, another attack has stolen critical company information, such as customer data and financial information.

"All I did was get the file, I wasn't the one who decided to release them," says the hacker. "I'm not the one who shorted the stock. Somebody else had their reasons for that."

FIGHTING MALWARE
The e-Brief
telecomasia

www.telecomasia.net

telecomasia

QUESTEX MEDIA

The scenario in the video is fictional, but also increasingly typical.

The operation of hacking has gone well beyond random disruption to coordinated and targeted attacks with well-defined objectives in mind.

Year of the Cyber Attack

By any measure, 2016 was the year of the Cyber Attack. Hackers made off with $81 million from Bangladesh's central bank. The US National Security Agency was exposed when its own hacking tools were released to the internet, and then there were the claims of cyber intervention in the US presidential election.

This year, a cyber gang believed to be based in China targeted companies through their supply chains, using managed services providers to facilitate the theft of intellectual property. North Korean hackers are believed to have gained access to a secret plan of action in the event of war on the Korean Peninsula.

In the corporate sphere, mid-sized Australian insurer IAG says it is being attacked up to 60 times every day. Banking apps on smartphones in India are reportedly leaking personal data on a continuous basis.

Cyber attacks of all kind are ubiquitous and are increasing. In any single minute on the internet, Google processes 2.4 million searches, 150 million emails are sent, and there are close to 350,000 tweets. Given this volume and speed, total security is impossible to police or enforce.

The advent of the era of the Internet of Things is only going to increase the potential for attacks, given that five billion devices will be connected to the internet in the Asia Pacific region by 2020.

The health industry is expected to be a major adopter of IoT technology, but the consequences of effective attack in that industry could be calamitous. A US report, Beazley Breach Insights, found that ransomware attacks increased by almost 400% in 2016, and nearly half of those attacks were in the health sector. One hospital in California, for example, lost $100,000 a day for every day they were unable to operate their systems, and then paid a $17,000 ransom.

While the health sector prepares for more threats, the world of autonomous connected cars is yet to arrive, but its development raises another whole raft of risks.

Organizations must understand that they will be under attack, and that their devices and networks will never be secure. The default response is that everything is vulnerable. In this context, it is no surprise that cyber insurance is a growing market.

Stay protected

So where does this leave an organization's efforts to protect itself and manage its risk?

One key message is that regulatory compliance is not an answer. Compliance is a "tick the box exercise" which can only go so far.

Standards are a more promising area and a rigorous standard such as ISO 27001, for Certified Information Security Management Systems, gives an organization confidence that its service provider's policies and procedures have been independently verified, providing a systematic and proactive approach for managing security risks through to confidential customer information.

ISO 27001 covers specific service areas, such as Cloud or XaaS, and many larger service providers have this certification in place across a whole range of their services.

Selecting a trusted service provider is a key choice, but it can only be a part of an effective security stance. Many underwriters in the cyber insurance area are focusing their efforts oncorporate culture as the most important part of any response. An organization's employees have long been considered to be the "Achilles Heel" of internet security.

Poorly trained staff are the ones who click on the phishing email which contains the malware and the ransomware demand. Staff complacency is one of the front lines of effective response, and employees must understand their role in their organization's security stance – and must be persuaded to care.

At the same time, an organization needs to have a set of processes in place to respond to breaches and threats. The aim is to maintain business continuity, protect the company and employee morale, and avoid fines, legal fees and remediation costs.

The reality is that today, failure to execute and follow through on any of these can have a terminal impact on the organization. Even if the organization survives, Ponemon Institute analysis says that brand value could decline by more than 31%, depending on the type of data breach.

Current statistics show that organizations are struggling to respond. According to Verizon's 2015 Data Breach Investigations

www.telecomasia.net

telecomasia

QUESTEX MEDIA

Report, 60% of the time attackers are able to compromise an organization within minutes. Yet according to Cisco's 2016 Annual Security Report, the current industry estimate for the time to detection (TTD) of security incidents is 100 to 200 days.

Organizations should have multi-disciplinary response teams which, once an incident is detected, leads efforts to stop, contain, and then control the incident and data loss. The cause of the breach needs to be isolated and eradicated without risking the integrity of data and systems.

Once this is done, then the team moves to a forensic examination of the source of the incident, making sure to preserve all the relevant evidence, including maintaining the chain of custody.

And finally, as with any toxic spill, there is a process of remediation. This is not just a technical process, but one in which communication with stakeholders, both internal and external, is also critical. This might involve informing the market, or educating staff on what they need to look out for to detect the breach, and what they might do to help prevent similar incidents.

When it comes to ransomware, organizations need to take an architectural approach by implementing a multi-layered defense strategy which strengthens defenses with a combination of detection, visibility and intelligence.

Ransomware takes control of targeted systems on a user's device and then uses an asymmetric key exchange which encrypts files, and only the ransomware developer has the key. Some ransomware can spread across the network, and this form of self-propagation is becoming more common.

Devices on and off the corporate network can be protected by umbrella roaming solutions which block DNS requests before devices even connect to sites which host ransomware.

There is also specific protection available for endpoints, and protection for email security which blocks ransomware delivered through spam and phishing emails.

At the perimeter, there are next-generation firewalls and sandboxing technology which isolate and detonate potential threats, and also block command-and-control callbacks to ransomware hosts.

All of these tools must be configured in a cohesive architecture with layers which work together, beginning with umbrellas which block the ransomware's attempt to encrypt data and make it inaccessible.

Further along, if a file makes it past both the DNS layer and the firewall, protection for endpoints can then identify the malicious point and block it from running and progressing a step further.

Even organizations with best practice layered protection, cannot be sure that they have 100% protection from ransomware. The response is ongoing vigilance and a combination of governance, employee training and education, and the right combination of solutions and the leveraging of service provider relationships.

Organizations can't stop the attacks, but they can be proactive in adopting a security stance which can deflect some attacks, detect other attacks earlier, and respond more effectively to the threats they are certain to encounter. ●

Service Providers. Part of the Solution

Threat centric architecture is available to protect both the service provider and third parties, including customers. It comprises:

- DNS layer protection
- Endpoint protection
- Email threat protection
- Sophisticated segmentation
- Advanced defenses for advanced attacks

Education. Service providers have a role to play in educating their customers about cyber risks. They can alert customers on the risks, inform them of best practice, and convey information about legal, regulatory and compliance issues.

Collaboration. Sharing information with agencies and other service providers can help create a united industry front against wrong doers.

Responsibility. Service providers must understand that their responsibility to customers requires a proactive and encompassing response, and builds trust and confidence.

FIGHTING MALWARE
The e-Brief
telecomasia

www.telecomasia.net

telecomasia

QUESTEX MEDIA

Automation: the savior of cybersecurity?

Automating security processes is a concept that has been gaining traction recently with the enterprise market, both driving new innovative applications, and also absorbing some much-needed upgrades.

An introductory example for automation is automating malware detection and threat containerization—a task that has remained a mandatory component for companies worldwide over the course of decades.

It's not feasible for users to go through each and every security alert in their personal computers and manually rectify any security issues. This is unnecessary, bothersome, and also prone to errors.

In its latest report on the role of automation in cybersecurity settings, ABI Research finds seven vital automated IT security applications that will help advance cybersecurity in the new world of artificial intelligence. The automated processes will aid critical IT security functions that range from assisting security personnel to streamlining security alerts to system optimization.

"While it will be a valuable addition to IT teams' arsenals," says Dimitrios Pavlakis, industry analyst at ABI Research, "automation is a double-edged sword if not handled properly."

"We expect automated processes to first address key issues like TLS/SSL, or Transport Layer Security/Secure Socket Layer, certification and privilege management prior to tackling critical functions like incident response," says Pavlakis.

As security analysts, network engineers, and IT personnel face increasingly tougher challenges due to the proliferation and magnitude of modern cyber threats, automation will become key—ABI Research anticipates it will reach critical mass within the next four years.

Big data, business intelligence, and data analytics platforms are forecast to top $54 billion by 2021 with network security and incident response predicted to climb to $59 billion by the same year. ●

Cybersecurity attacks on the rise in Asia

59% of organizations surveyed in Asia reported one security breach at minimum on a monthly basis during 2016, says Telstra's Cyber Security Report 2017.

The findings of the report, which surveyed 360 organizations across Asia, reflect a growing state of unease on the state of cybersecurity in the region.

India is most at risk of cyberattacks, accounting for 14.8% of all weekly security incidents. Hong Kong accounts for 14.7% of weekly security incidents.

"Businesses in Asia are dealing with unprecedented security and business challenges," says Neil Campbell, Telstra's director of security solutions. "Many of these are fueled by mobility, cloud-based service offerings and the need to have an environment that adapts to the way users want to work and interact. Organizations must invest in appropriate security initiatives in order to reap the benefits of innovative technologies, like Cloud and IoT devices, as they emerge."

According to the survey, 30% of organizations experienced at least one phishing attack per month. Inbound email threats and business email compromise scams also topped the list. Australia was the main target for malware last year.

Ransomware attacks were among common security breaches with one in four organizations across the region experiencing an attack on a monthly basis. Half of those affected indicated that they paid the ransom but nearly 40% of those who paid the ransom did not recover their files.

Security is also being recognized by C-level executives as being of major importance. C-level executives in Asia are perceived to be the primary stakeholders in taking responsibility for security incidents which has increased from 35% in 2015 to 65% in 2016.

The growth in cyber-attacks and incidents across Asia has also resulted in a heightened awareness of the business impacts such risks can have. This has in turn led to increased IT security spend with close to 94.7% of organizations in Asia increasing their security budget this year, the report found. ●

FIGHTING MALWARE
The e-Brief
telecomasia

www.telecomasia.net

telecomasia

QUESTEX MEDIA

Addressing data lost protection and ransomware attacks

Beware the insider security threat

Recent surveys have demonstrated the risky prospect of insider security threats. *Baseline Magazine cited* an industry survey showing a marked increase in the number of IT pros that are willing to steal company information if they lost their jobs. *PC World* cited a similar survey showing that almost two-thirds of employees steal data when they leave the company. Cisco's global data loss survey showed that nearly one in ten current employees have either stolen company equipment or data for profit or know someone at work who has. These cases only describe malicious insiders and not the far greater number of users who inadvertently allow protected data to escape the organization's control.

Insider threats don't always only involve employees, either—partners and suppliers often become part of an organization's Extended Enterprise. If external parties were granted access an organization's network they become "insiders" by extension; often with the ability to access and even extract sensitive data for commercially legitimate reasons.

Information-centric risks such as the loss or disclosure of data that is protected by law, convention, or company policy have driven rapid awareness and growth of data loss prevention best practices as expounded by the security industry.

The analysis of content is a technology function, but without effective information governance as a business function a DLP product can only do so much. DLP technology should never be deployed in a business process vacuum, as DLP technologies leverage a number of different techniques for content analysis. These techniques range from straightforward pattern, logic or expression matching against standard data types like social security or credit card numbers to more advanced and complex linguistic analysis used to identify "unstructured data" found in human natural language. In-between are commonly found techniques built around subject-specific content dictionaries and hashing or fingerprinting strategies for data repositories.

The use of technology must be applied within the context of business requirements and mitigation of risks or exposure. This means organizations must know & classify the types of data they are required to protect, and must implement policy and processes that support the DLP technology or infrastructure that they plan to deploy. Implementing a sophisticated DLP technology without a thorough understanding of an organization's data loss posture is like building fortifications with no clue of the attack-vector. At best, it's an inefficient strategy—at worst, it can be a counter-intuitive & costly venture.

Not all insider threats are deliberate and malicious. Most DLP technologies today are focused on the negligent and the careless rather than the unscrupulous and the dishonest. The latter are much harder to stop with technology alone, thus organizations seeking to adopt DLP are wise to consider it holistically, as part of an aligned business-technology initiative that addresses people, processes, and technology.

Cisco addresses the issues with multi-tier approaches focusing both on technologies and the security framework process policy governance of an organization responsible for security. The technologies include:

Cisco Cloudlock: a frictionless solution that combats cloud account compromises, data breaches and cloud malware, while providing codeless security for home-grown apps and actionable cybersecurity intelligence across an organization's entire cloud infrastructure. Unlike part-proxy, part-cloud API solutions that attempt both approaches and succeed at neither, Cloudlock orchestrates existing security investments to provide a coordinated, best-of-breed security solution. And with Cisco Umbrella, organization can stop phishing and malware infections earlier, identify already infected devices faster, and prevent data exfiltration as it's delivered from the cloud, Cisco Umbrella provides an effective security platform that is open, automated, and simple to use.

Email DLP (Cisco Ironport), provides protection for sensitive data with a fully integrated, comprehensive, accurate, and

www.telecomasia.net

telecomasia

QUESTEX MEDIA

easy-to-deploy solution. This feature has more than 100 predefined policies, covering government regulations in different regions as well as industry regulations such as PCI DSS. These policies use sophisticated content analysis techniques and are specifically tuned to virtually eliminate false positives and increase the catch rate. Additionally, administrators can easily build custom policies to identify company-specific intellectual property or sensitive data.

In a single user interface, administrators can configure anti-spam, anti-virus, content filtering, encryption, and email DLP actions on a per-user basis. Administrators can access real-time and scheduled reports to view violations by policy, severity, and senders.

ZixGateway with Cisco Technology: integrates transparently with Cisco Email Security Appliance to automate the protection of sensitive email content.

Cisco Advanced Malware Protection, is available as an add-on that provides file reputation and sandboxing in the cloud to block advanced malware that would otherwise pass undetected through traditional antivirus scanners. The AMP system can be deployed completely on premise with the AMP private cloud license—also included is auto remediation of malware for Office 365 customers.

Cisco Talos: a security ecosystem that identifies, analyzes, and defends against threats. It consists of three components:

- Cisco SenderBase: the world's largest threat-monitoring network and vulnerability database.
- Cisco Threat Operations Center: a global team of security analysts and automated systems that extract actionable intelligence.
- Dynamic updates: real-time updates that are automatically delivered to Cisco security devices, along with best-practice recommendations.

Technologies are useful but don't forget the end-users. People control the processes that drive an organization's initiatives on Data Loss, either through educating or creating awareness of negligent behavior or simply being ignorant and unsophisticated in daily operations. All users across an organization (partners, suppliers, staff, and contractors) must also be made aware of the risks of data loss in their roles and responsibilities in the organization—from the CEO to the contractors. This can be achieved either through a formalized program or a series of yearly exercises in drills or table-top discussions/seminars.

In addition to taking a tactical approach in combating data loss and malware situations, Cisco also recommends organizations to take strategic and operational views through;

Vulnerability Management Program to collect, analyze, and use data and information regarding security vulnerabilities to improve security posture by actively managing and remediating security weaknesses.

Security Segmentation to go beyond typical network considerations that focus narrowly on isolation. Take a new approach to segmentation that more fully considers identity and trust, visibility, policy enforcement, availability, application inter-dependencies, business and application impacts and vertical-specific design patterns. The result for you is a reusable segmentation framework that will reduce risk, simplify your audit profile, secure your data, and help you comply with board-level requirements.

Third Party Risk Management help ensure that your third-party relationships do not expose you to unacceptable levels of risk. Learn to understand and manage third-party risk throughout the entire relationship lifecycle, from selection through relationship conclusion. By identifying the information needed to balance risk and opportunity, making sure that you engage with the most risk-appropriate organizations. With this knowledge, you can make better decisions about your business and about how you connect, communicate, collaborate and share critical data with third party providers.

Incident Response significantly strengthens your network and information security defenses. It is not a matter of 'if', but 'when' and your response to a security situation matters. You need access to latest intelligence and best practices, so that you can have a proven process that engages all layers of defenses and provides a comprehensive range of capabilities to prepare, manage, respond to, and recover from incidents quickly and effectively. ●

For more information on Cisco security visit https://www.cisco.com/go/spsecurity