Bespoke ransomware, targeted attacks – the hacker's new arsenal

By JONATHAN SHARROCk, CEO, Xlerated Assets

Cyber security is a hot topic in board meetings. Management wants, and needs, to know how cyber security is being controlled and monitored. If you are the person responsible it is essential that you can demonstrate effective management of this vital issue

Although it may appear to be good news that a competitor is receiving negative publicity due to a cyberattack this news should be an alert that your organisation could be next!

Contrary to popular belief, there isn't a silver bullet. No company can be 100 percent protected against a cyberattack. Anti-virus systems can easily be evaded, and security software can be misconfigured leaving your company at risk.

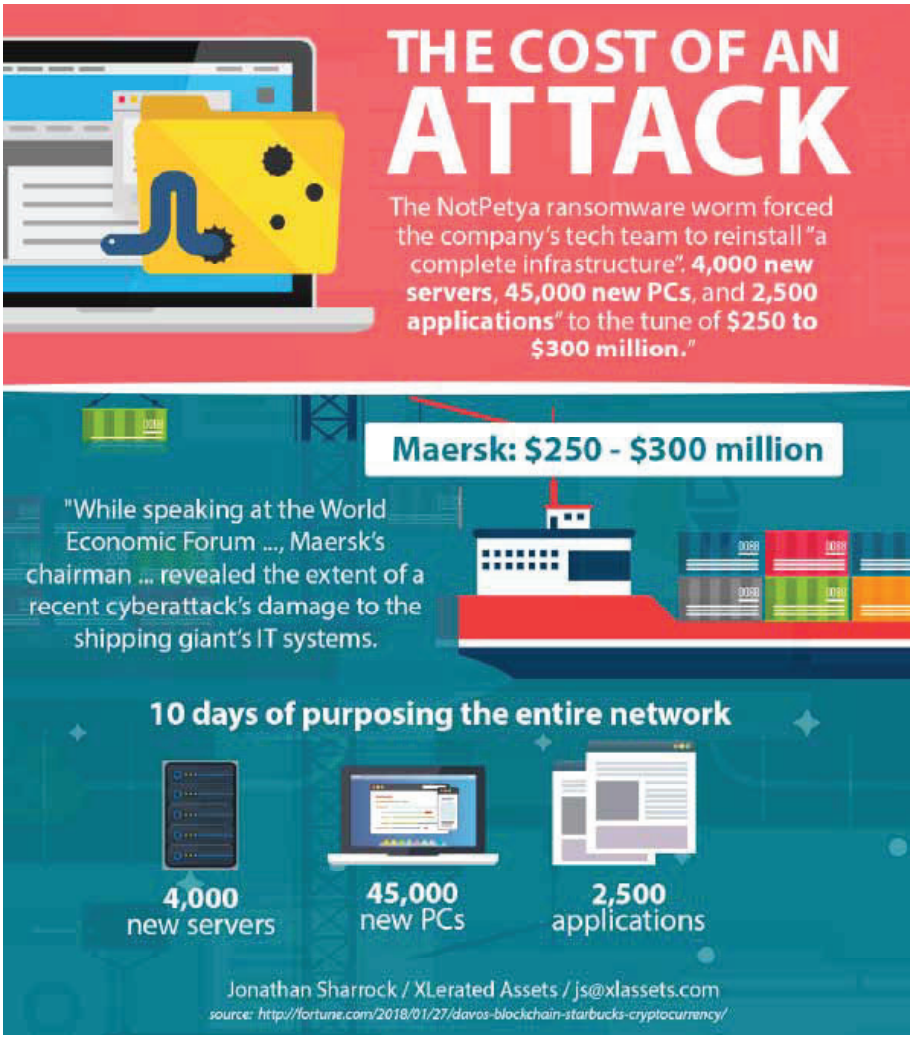
Logistics businesses nowadays operate in "real time" and need to exchange vast amounts of data but your "real time" tracking information may be out of date and vulnerable to attacks.

Risk one is a legacy systems targeted attack. Hackers often go after legacy systems that were built decades ago when security was less of an issue. Often companies decide to take on 'Technical Debt', with a lack of proper security controls in place.

These legacy systems remain a vital part of the supply chain process. However, the messages that are sent between the logistics partners are often unencrypted and an attacker with a limited amount of knowledge can disrupt the supply chain process and cause huge costs to an organisation.

Risk two is ransomware. This malicious software can inflict the maximum amount of damage on the supply chain because the attacker knows that causing major disruption will provide a good opportunity to short sell the logistics company's stock and make a huge financial gain in the process. This is a low risk and attractive option as companies are now paying the ransom. A recent cyberattack that hit Maersk, the world's largest container shipping company, is estimated to have cost up to US$300 Million.

Risk three is a distributed denial of service 'DDOS' Attack. This attack is multiple compromised computer systems attacking a server, network resource, or system that is responsible for communicating with your logistics partners. This will cause the system to slow down or even crash. These DDOS attacks can be purchased for as little as US$2 per hour as they are available as-a-service, in the cloud. This makes for a very affordable option for attackers wanting to take a logistics company offline. Imagine thousands of employees unable to access systems, causing a melt-down in the supply chain. This type of attack undermines your company's reputation and may lead your partners to consider alternative partnerships.



Risk Four is the Shared Responsibility of security in the cloud. You need a clear understanding of what your cloud provider does and does not provide.

For example, AWS will patch and fix flaws within their infrastructure, customers are responsible for patching their guests Operating Systems 'OS' and Applications. This sounds straight forward, but it is often an oversight, where the customer is unaware that there is any patching required and critical systems are left open to vulnerabilities.

The Amazon Virtual Private Cloud (VPC) is categorised as Infrastructure as a Service (IaaS) as such the customer is responsible for all the security configuration and management tasks.

What this effectively means is the customer needs to provide this work and might not be aware this was a problem when moving to the cloud.

Microsoft states Data Classification and protection controls are the responsibility of the customer.

Amazon breaks down the responsibility into two main categories: security in the cloud and security of the cloud. Amazon is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud. The Customer is responsible for 'Security in the Cloud"

It is common that software developers either leave security until the end of the project or neglect it all together. These developers with little or no understanding of security, make the customer believe that they have this security under control, but in reality, they have interpreted the Shared Responsibility Model incorrectly, or have not included Security in their initial development costs and as a result have left the customers network vulnerable to exploitation.

The time to act is now

If your business is in Australia, you will soon be required to report any 'eligible' data breaches to the Australian Privacy and Information Commissioner and notify your customers that may have been affected. improving your security stance will require time.

You need to install appropriate controls immediately and adopt a roadmap to identify and address any gaps in your system.

We know that hackers are methodical, organised and they have automated systems.

Fighting against an automated hacker and fighting back manually is not a fair fight. Using Automation helps even out the balance against the hackers and there ARE defences available against cyberattacks even though hackers are constantly striving to stay ahead of security measures.

Security is all about layers or 'defence-in-depth'. Even if the attacker can penetrate the first layer of security there will be multiple additional layers to counteract and report the threat.

It is therefore, vitally important to receive security advice, not only to understand the likelihood of a security event, but to understand the next steps and what level of investment will reduce the risk and improve your overall security posture.

A useful report to read is the Australian Signal Directorate's (ASD) Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained. This is easy to follow advice that will give you an initial strategy to implement the most effective security controls to prevent over 85 percent of intrusions.

The big four – Deloitte, EY, KPMG and PwC accounting firms offer a consultancy-based approach to solving these questions. Many systems integrators (SI's) will offer a similar service and can help with the security assessment.

Using consultants to assess your organisation's cyber security risk does present an advantage: Although the assessment results can be highly complex and technical in nature, the consultancy can provide you with a clear understanding, in layman's terms, of the risks to your business and the steps you need to take.

A final point to consider: More and more organisations are seeing the wisdom of investing in cyber insurance. If you invest now in cyber insurance you will have a far better conversation later with your insurer when asked: "Did you engage a security consultant at any point?"

WANT TO KNOW MORE

Jonothan will be presenting at the Global Shippers Forum (GSF) and ICHCA International Conference and Exhibition (10-11 May 2018, Melbourne - www.FTAlliance.com.au)