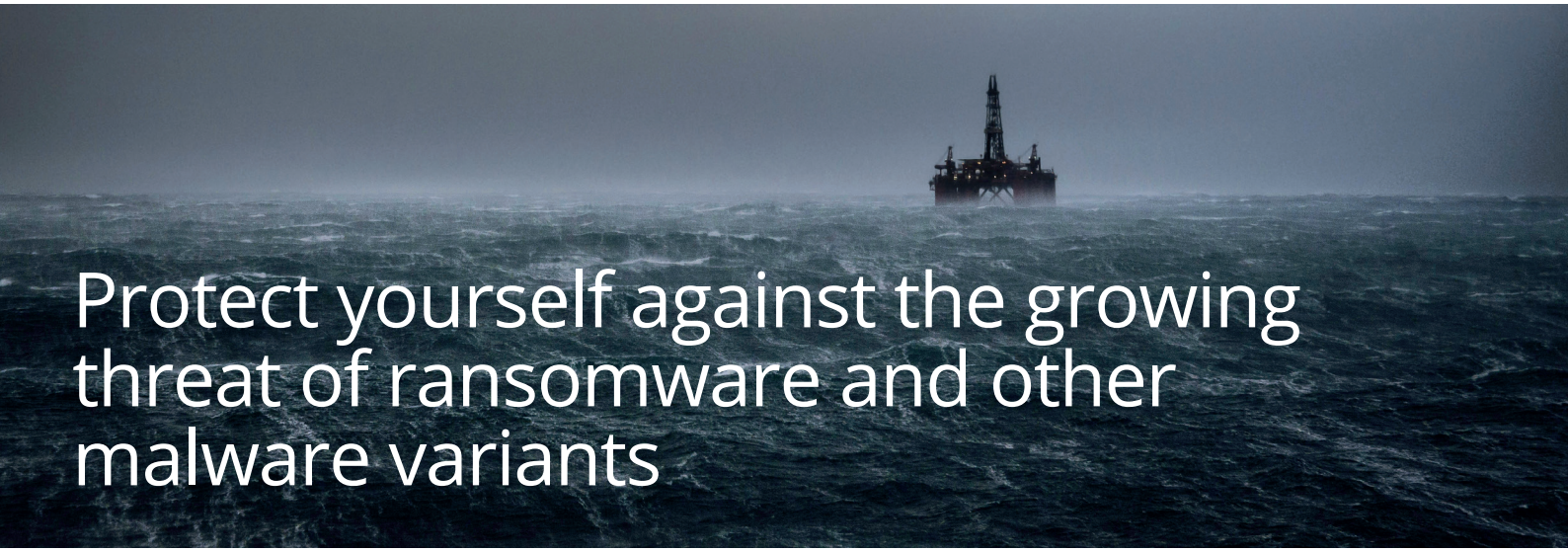
NTT Security

Whitepaper



Protect yourself against the growing threat of ransomware and other malware variants

Most organizations will be aware of ransomware – the increasingly common practice whereby an attacker uses malware to prevent users from accessing their systems or by locking users' files until a ransom is paid.

If you haven't yet been a victim of ransomware, chances are you soon will. With talk now of the 'ransomware business model', recent research across the US, UK, Germany and France highlights that ransomware attacks are on the rise, with 48% of businesses seeing attacks in 2016[1]. More than ten million ransomware-related cyber threats in Asia Pacific were detected and blocked from January to May 2016 by just one security company[2].

This paper looks at the rise of ransomware attacks; the evolution of ransomware; the cost to business; the evolution of attack methods; and the steps that NTT Security recommends that organizations must take to mitigate the risk of attack.

The evolution of ransomware

Ransomware has been around for some time, first seen in 1989 with the AIDS Trojan and is still one of the most pervasive of cyber threats three decades later. Early ransomware was disguised as PC clean up applications that damaged PCs and offered to fix them for a fee. This evolved a couple of years later into attacks using fake anti-virus applications, where attackers would trick users into paying for many years of support. In 2009 mainstream anonymous payment services such as bitcoins made it easier for hackers to collect money. And in 2013, we arrived at a pivotal moment for ransomware with the arrival of CryptoLocker – the first instance of ransomware sent to business users in the form of email attachments, designed to encrypt files stored on a user's computer or mobile device. Only recently, unknown attackers used the WannaCry ransomware to cause enormous disturbances in organizations and public services worldwide.

Today, ransomware is a ubiquitous security threat with one aim – to extract payment from victims. Its impact on businesses around the world continues to be significant, with global organizations held to ransom every day.

The Evolution of Ransomware
– a surprisingly long history

1989
- **AIDS Trojan** 2,000 infected diskettes distributed

2006
- **Archiveus Trojan** First use of RSA encryption

2011
- unnamed **Trojan** exploits anonymous payment systems

2012
- **Reveton Trojan** spreads throughout Europe

2013
- **CryptoLocker** was born, the first cryptographic malware

2014
- **Crypto Defense** released, using Tor and Bitcoin for anonymity
- **Spyeng** released – the first Android based ransomware

2015
- **Locker Pin** released - malware capable of resetting the PIN of your phone to permanently lock you out
- **LowLevel04** ransomware released – unlike other ransomware campaigns, attacks were done manually by attackers

2016
- **Ransomscript** release – the first ransomware written in Java Script
- **Locky** ransomware discovered and quickly began to spread via aggressive phishing campaigns
- **KeRanger** discovered - the first official Mac OSX-based ransomware
- **Petya** released and delivered via Dropbox
- **SamSam** released, allowing attackers to communicate in real time with victims

Source: CSO online. Terrance DeJesus of NTT Security's Security Engineering and Research Team (SERT)

1. Vanson Bourne research 2. Trend Micro Incorporated press release dated July 12 2016

Many variants. One key aim.

There are many variants of ransomware with new strains appearing with regularity, and they all fall broadly into two areas – locker ransomware and crypto ransomware. Both are designed to deny the user access to something until a ransom is paid; although locker ransomware is generally less effective than crypto ransomware as a way to extract payment from a victim.

> **"The threat of ransomware attacks means that business should consider further mitigation and preventative solutions to combat it."**
>
> The cyber threat to UK business report, National Crime Agency

Locker ransomware is designed to lock a user out of a system, and typically leaves the underlying system and files untouched. Tech savvy teams and security vendors are often able to restore access to devices and files with data remaining unaffected.

Crypto ransomware, on the other hand, is designed to encrypt files stored on a user's computer or mobile device, rendering them unreadable until the victim pays for the decryption key. It quietly encrypts critical files and alerts the user once the damage is done. And unlike locker ransomware, recovering files that have been encrypted by crypto ransomware is technically extremely difficult, if not impossible. In most cases it is simpler to wipe the device clean and reinstall the operating system. This of course, means losing all your data.

The most common way to deliver crypto ransomware is by email message. Receiving the email itself won't trigger an infection, but opening an infected file attachment or downloading a linked, infected file will start a chain of events that starts with encrypting files and culminates in a ransom demand.

Gone are the days of poorly written ransomware and simple decryption. Today's ransomware authors are much more sophisticated and tenacious.

> **"Ransomware remains the most common cyber extortion method."**
>
> The cyber threat to UK business report, National Crime Agency

Business threat is more than financial

Unlike many targeted attacks where business disruption and reputational damage is at the core of the attack, ransomware has one goal – to extract payment from the victim in return for decrypting files. A key element in making ransomware so attractive to attackers is the availability of payment systems that are hard to trace including wire services, bitcoins and premium rate text messages. Such is the concern about the magnitude of ransomware attacks, and the lack of law enforcement resources available to deal with them, that key business sectors such as banking are maintaining stocks of bitcoins to pay attackers[3]. Attackers know that mounting a criminal investigation is out of the question for organizations who want to get back to business as usual and ransomware demands have typically been low enough for businesses to pay up and ask questions later. Reports on the global sums involved in ransomware attacks vary significantly with some reports suggesting that attacks in 2016 could top $1 billion.[4]

> **"Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money."**
>
> Garry Sidaway, NTT Security

But it's not just a financial consideration for a business – a ransomware attack has the ability to stop organizations functioning, resulting in reputational damage and, in the case of hospital attacks, patient safety concerns. No business can be run effectively today with pen and paper systems and fax machines, so the ransoms are often paid and attackers continue to exploit this.

Will paying the ransom be enough?

As attackers continue to reap the monitory benefits of ransomware campaigns and gain an understanding of which entities are paying ransoms, the motivation to create modular and robust strains becomes the norm, as evidenced with Cerber, CryptXXX and Maktub. Continuous development cycles suggest that Ransomware-as-a-Service (where the ransomware author sells the code to other criminals in return for a percentage of the profit) and successful campaigns delivered via TeslaCrypt, Locky, Cerber and CryptXXX will not be abandoned once the attackers have attained their initial goal, money. In other words, paying the ransom does not guarantee that the victim will regain access to their data – some victims are never provided with the decryption key. Paying a ransom emboldens the attacker and incentivizes other criminals to engage in similar activity for financial gain. Researchers are finding it difficult to reverse-engineer variants and conduct crypto analysis on encryption methods. Therefore, the risk of reinfection remains high and predicting and detecting attacks has never been more important.

MongoDB attacks

MongoDB is an open source database built on an architecture of collections and documents, unlike a relational database with tables and rows.

Early 2017 saw a surge in attacks against publicly accessible MongoDB installations. The message to the victim was to send a small bitcoin payment to regain access to their files. In several cases, the databases had already been deleted before the ransom was requested.

The main problem with MongoDB is that it's easy to find a list of the databases, publicly accessible from the internet, using tools like Shodan, which means that multiple hackers are able to easily access the database and demand a ransom for the return of the same database.

The likelihood of paying the right hacker and getting your data back is slim. Which means that preventative measures are essential – such as removing the server from the public internet, having a robust backup plan, and ensuring that some sort of authentication is always required.

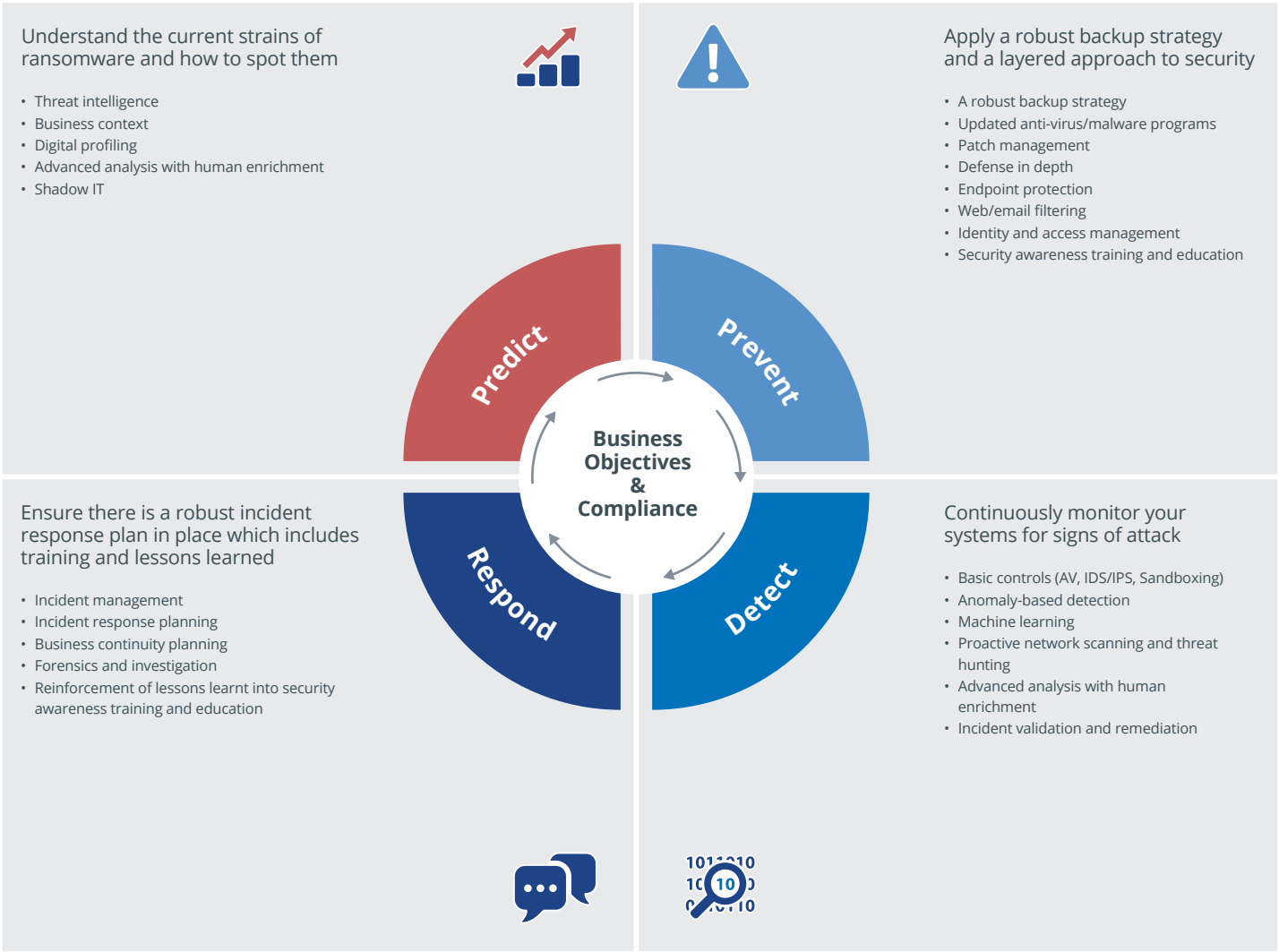
3. The Guardian: City banks plan to hoard bitcoins to help them pay cyber ransoms *4. Hackerpocalypse: A Cybercrime Revelation*

Mitigating ransomware risks. A view from NTT Security

In some ways, ransomware is much like any security threat with the criminal seeking to expose vulnerability in order to make money. The methods might have evolved and the technology might be different, but the threat needs to be handled in a similar way to any other threat.

The security tools and practices that NTT Security recommends that organizations must consider to mitigate the risk of a ransomware attack fall into four over-arching steps – Predict; Prevent; Detect; Respond (Figure 1).

Figure 1 – A resilient cyber defence architecture for ransomware



1. Predict

Threat intelligence is a hot topic, but having more data about threats and exploits is not necessarily the key to understanding and predicting attacks. Few organizations have the time and resources to organize and analyse threat information on their own. Many will use the services of a qualified and trusted third party to provide this information. These experts will integrate threat feeds from both their own data sources and multiple, 3rd party public and private data sources and then use advanced analysis techniques to provide business context to the threats. And to do this, the organization needs to first understand its own assets and associated values in order to prioritize the tasks at each stage.

Understanding the current strains of ransomware and how to spot them can also help. Ransomware authors are constantly innovating to stay one step ahead of security controls. As a minimum, every organization should continuously update itself on the current strains of ransomware out there – a basic first step towards prevention.

2. Prevent: Make it a policy to back up

Once a system is infected with ransomware, paying the ransom is no guarantee that your data will be recovered. But a robust back up strategy will help you recover most, if not all, of the files. In addition to any real time or online backups, it's important to have offline and offsite backups. Any backup that can be accessed over the network is vulnerable to ransomware, so it's important to perform your backup, verify it and then unplug it from the network. And don't assume that cloud-based or server-based backups are immune. Any drive that you can access can also be accessed by ransomware. Just because it's not held on drive C: doesn't make it immune. And remember: backups **must** be verified; backups **must** be restorable; know the difference between incremental, differential and full backup; always rotate your backups to a schedule; and always test the restore procedure during disaster response drills.

3. Prevent: Don't ignore security awareness training

Proper security awareness training will dramatically reduce the chance of an organization falling victim to ransomware and end users should be aware of your email and web browsing policies. Make it your business to understand the strains of malware doing the rounds and advise employees of the steps they should take to avoid attacks. For example, one well-known piece of malware, Locky Ransomware is also spread via Facebook Messenger by pretending to be a harmless image file. If your users are actively using Facebook, then they need to be reminded that there are threats facing them on every link they click and those threats are not only against them, but your entire corporate network. Provide updated security awareness, conduct social engineering penetration tests and utilize fake phishing campaigns to ensure your users are abiding by security policies. A trusted security advisor will keep you up to date with notifications on the strains of malware to look out for – you're not on your own.

4. Prevent: Defense in depth

Defense in depth is the coordinated use of multiple security countermeasures to protect your information assets and works on the principle that if one mechanism fails, another will be ready to stop an attack. With a wide variety of attack methods available, there's no single method for effectively protecting a network against a ransomware attack, so a defense in depth strategy ensures that security has been implemented at the perimeter, DMZ, internal network, host, application and data levels.

The component parts of a Defense in depth strategy

Multi-layered security measures will go a long way to protecting your assets. For example, **patching** needs to be under control – your network is only ever one click away from a compromise and timely software updates will help close this area of vulnerability; deploying **advanced malware detection tools** – for example, non-signature or cloud-based anti-virus tools will also help; and creating firewall rules to block specific ports to untrusted IPs can be an effective way to prevent attacks. Hadoop Distributed File Systems attacks in 2017 appeared to have targeted traffic to port 50070, for example.

And of course, key to successfully dealing with ransomware attacks is to have a sound solution for protecting all your endpoints. As they are ransomware's entry point, using endpoint protection solutions will enable an attack to be isolated before it can spread.

5. Detect

Common detection methods such as anti-virus, IPS/IDS and sandboxing are all important controls to have in place to detect known attack signatures. New and unknown attacks, however, require heuristics and anomaly-based detection such as behavior modelling and machine learning which can catch ransomware early on in the initial download phase or during command and control communication.

These advanced tools help organizations with huge volumes of data, where a high degree of automation is required to detect threats. However, automation alone will not detect those needles in a haystack. For this, you need to combine automation with human enrichment – validation by real security experts who can remove false positives and only send notifications of critical incidents with actionable remediation guidance.

Using advanced analysis methods such as log correlation and kill-chain analysis with machine learning can help information security professionals to detect ransomware that is moving laterally within the network, and is often invisible to traditional perimeter defenses.

Detecting all ransomware types including the latest advanced ransomware, is time consuming. It can be more cost effective and efficient to outsource this responsibility to a security partner who has the global resources and expertise to constantly monitor your network around the clock, and apply advanced analytics to detect both known and unknown attacks as early as possible.

6. Respond: Review your incident response plan

It's safe to assume that your organization will, at some point, suffer a breach so incident response planning should be embedded into the organization and must then form a key element of your business continuity planning. If you already have an incident response plan, make sure it's up to date. If you have never written a plan, it's a good idea to do so.

A successful proactive incident response plan commonly includes the following components:

- **Define the incident response team** along with their roles and responsibilities – and agree any skill sets that may be required which don't exist within your organization;
- **Define your communications process** and plan for effective communication during and after the incident – it is also necessary to define when it is or is not appropriate to include law enforcement or industry regulators during, or following an incident;
- **Define the criteria** to declare when an incident has started as well as when the incident has ended;
- **Document the incident** – a checklist with dates and times, and other pertinent information can be extremely useful for both reporting the crime and for a 'lessons learnt' exercise and should form part of your **security awareness training** program;
- **Containment** – the primary purpose of this phase is to limit the damage and prevent any further damage from happening;
- **Removal and restoration** – to ensure that proper steps are taken to remove malicious content from the affected systems;
- **Recovery** – testing and verifying that the compromised systems are clean and fully functional.

Case Study – Rapid detection and response prevents wider malware infection

Rapid detection identifies problem
As part of our Managed and Professional service to a client in the oil and gas sector, we were able to quickly detect a malware infection that had broken out at one of their sites in Africa. Following the detection we gave clear advice and guidance on where the infection had spread, how it had impacted them and the criticality of identifying those assets that had been infected.

Rapid response contains the risk
We quickly identified the infected assets including a laptop belonging to a vice president of the organization, who was travelling at the time by air.

To reduce the risk of further infection when he next accessed the network, an IT representative was sent to meet the vice president at the airport and quarantine and clean his device.

Without this rapid detection and response, the likely outcome would have been a spreading malware infection throughout the organization.

Ongoing education
Understanding the threats to your organization is an ongoing responsibility.

NTT Security provided an advisory service to remind teams about mitigating these threats in the future based on lessons learnt and best practice.

Conclusion

Ransomware is not going away and experts predict that we will continue to see multiple, new variants emerging from attackers who are both knowledgeable and skilled. Delivery methods via email, compromised websites and exploit kits will continue to be successful, and attackers will continue to make money out of ransomware campaigns, increasing their understanding of which organizations and individuals are likely to pay ransoms. We now have a vast infrastructure of anonymous networks and payment services. Threat actors, emboldened by their success, will now be determined to increase their income while decreasing efforts.

Our best line of defense is to accept this and take every necessary precaution to mitigate the growing risk it presents. Ignoring basic IT security rules is enabling the attackers to profit. It's a very real business problem and requires a security strategy that leverages the right people skills, processes and technology to incorporate threat prediction, threat prevention, threat detection and a comprehensive incident response plan from organizations of all sizes, in all sectors.

About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.