Advanced Malware Detection

Introduction to the Cybersecurity Innovation Series

Creating and maintaining a resilient cybersecurity architecture – an architecture that is responsive to continual business change, the demands of evolving compliance and a sophisticated and hostile threat landscape – allows organisations to take advantage of new opportunities without compromise.

No business can afford to stand still and effective cybersecurity is no different. Understanding new approaches and evaluating, implementing and maintaining the latest innovative technology solutions can be difficult, time consuming and expensive.

Use the papers in our Cybersecurity Innovation Series to guide you through the latest advances in cyber approaches and technology, to focus your investments and build capability in the right areas for your business.

Advanced Malware Detection

The industrialisation of malware is a reality. Much like any growing enterprise those in the malware business have established a sales platform on the dark web, possess a motivated workforce, have rapid, to-order product development and are part of a competitive market that drives down prices for its growing customer base. Some even offer customer guarantees that their wares will evade detection.

The market for malware

Remember the days when viruses targeting your operating systems were as sophisticated as malware got? If you do, you don't need us to tell you how the internet helped the bad guys get creative with self-propagating worms that exploited enterprise networks, followed by the emergence of spyware and rootkits that, for the first time, ran stealthily on machines rather than trumpeting their presence.

When the extent of the financial gain became clear, cyber criminals developed new techniques at a fast and furious pace. Through encrypted tunneling, sandbox evasion and blended attacks, criminals exploited information about individuals and companies gleaned from organisations' ever-expanding digital footprints, combining this knowledge with phishing attacks to penetrate networks. And now we are witnessing the explosion in the use of ransomware – an escalation in activity from data theft to more frequent instances of damaging or destroying endpoints and information.

During all of this metamorphosis in malware, IT teams are also facing unprecedented challenges – including protecting a proliferation of endpoints; planning for the impact of the Internet of Things, which industry analysts predict will equal 32 billion devices by 20201; and attempting to understand and manage an explosion in Shadow IT and cloud adoption.

1 WHO
- State linked / Issue based
- Criminal syndicate / Opportunist

2 WHAT?
- Data / Applications / Devices / Network
- Vulnerability of business

3 WHEN?
- Timing – Reason?

4 WHERE?
- Which part of the IT estate has been compromised?

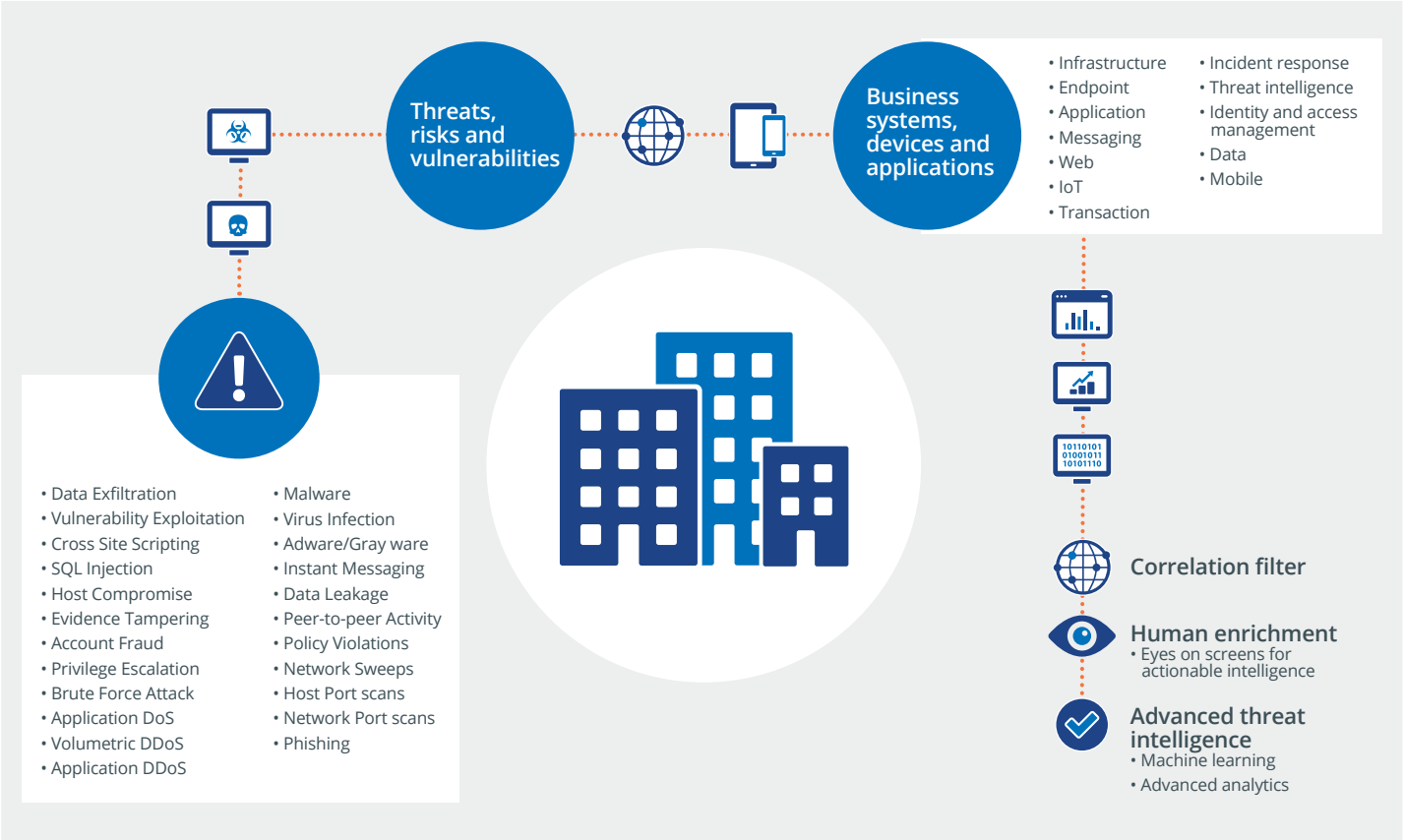
5 WHY?
- Motivation
- Goals

Motive, opportunity and ability for cybercrime

But some things don't change. Successful cyber criminals, much like other criminals, have three consistent traits – motive, ability and opportunity. To focus investment on the right controls and solutions and build an advanced detection and response capability, organisations are seeking to understand more about the 'why' and 'how' of malware.

1. IDC

Figure 1 NTT Security model – how we deliver



Motive

We have not lost the battle against Malware. But as our 2016 Global Threat Intelligence Report report highlights, the UK has now become the number one source of attacks.[2] As businesses increase their security maturity and capability, they are no longer content to look for symptoms of malware attacks, instead seeking to invest in the latest protective and prevention capabilities with digital shadow profiling. To regain control, they want to establish an 'attackers' eye' view – not only to understand their adversaries' techniques, tactics and procedures, but also to get closer to the motivation for an attack. Understanding more about who is attacking you, where they are based and which assets or data are of interest, as well as the timing of any activity with the right 24/7/365 monitoring – can help an organisation establish the motivation of its attackers. With the right profiling tools, contextual knowledge and analysis skills, suspicious activities as well as known attack patterns, can now be traced back to their source and dark web chatter can give real insight into an attacker's intent. Developing this type of capability turns the tables on the reconnaissance activities usually deployed by attackers to help organisations assess their vulnerabilities and develop faster, more effective threat prevention and incident response.

NTT Group analyses malware samples from a wide range of sources, including security platforms, incident response investigations, malware repositories, malware feeds, interaction with clients and privately-maintained honeypot networks. The resulting analysis allows for development of proprietary detection and prevention signatures which we share with our clients.

Ability

There is no question that cyber criminals' ability to exploit gaps has increased. Malware can now actively evade detection by hiding itself and rather than using a single technique, cyber criminals often combine clever, highly targeted and tested malware over long periods. Establishing a detailed understanding of how users behave helps them to achieve their objectives. But our ability to detect and prevent malware could be transformed by the application of machine learning or 'deep learning' techniques. Innovative solution providers are now demonstrating advances in algorithms that can be applied to recognise the common patterns in malware variants, giving organisations a longer window to respond.

Advances in processors and the reduced cost of computing power enables organisations of all sizes to exploit big data analysis techniques to match patterns within billions of sample characteristics – for example, being able to capture and log keystrokes. The industrial scale of malware production needs industrial detection capabilities, an automated ability to learn how malware is adapting so that analysts can make decisions about their next move.

Opportunity

The facts are clear. We could make life much harder for cyber criminals than we do today. The NTT Security 2016 Global Threat Intelligence Report highlighted the high percentage of organisations that still lack controls such as patch management, incident response planning, best practice network segregation, advanced malware prevention and comprehensive 24/7/365 monitoring. For example, the top 10 internal vulnerabilities are exclusively related to patch levels – accounting for more than 78 percent of all observed internal vulnerabilities during 2015.[3] These information security fundamentals could have prevented or mitigated a significant portion of incidents and

2. GTIR 2016 3. GTIR 2016

malware infections documented by the NTT Group. And large organisations are just as likely to have these gaps as smaller, growing businesses.

Traditional signature based prevention controls such as antivirus software, policy-based firewalls and sandboxing, remain necessary components of our cyber defence capability against 'known threats' – if they are maintained in the right way. But these solutions on their own are no longer sufficient. To detect, analyse and defend against zero day and sophisticated APT attacks, emerging deception tools and techniques, such as next-generation honeypots and decoy systems, could offer game-changing capability for advanced malware detection. Analysts such as Gartner are excited about the possibilities that deception techniques and a new generation of distributed decoy technologies could offer organisations, to make life much more difficult and costly for those in the malware business.

So how do deception solutions work? The goal is to disrupt malware at multiple points along the attack chain. When intrusions are detected, the malicious actors and systems compromised are automatically isolated and held in a network deception zone. In this zone, attackers are forced to invest valuable time and resources trying to establish what is real and how to proceed with an attack. They are deceived into seeing things on the network or endpoint that are not there. In some cases, they are convinced that they have been successful on fake systems and network components that operate exactly like an organisation's real assets.

The good news for those organisations looking to build a resilient cyber defence architecture is that a deception approach can be built into existing components. Firewalls with blacklists, intrusion prevention, URL filtering and other controls can be configured to transport connections from known malicious hosts to network emulation services or to deception decoy services within the enterprise network. And for those whose focus right now is endpoint protection – endpoint detection and response tools can also be exploited using deception at the malware host layer.

User behaviour anomaly detection – context for malware analysis

Another innovative solution that integrates with existing data loss prevention (DLP) tools and end point protection is user behaviour anomaly detection. Whereas DLP focuses on protecting sensitive data – techniques such as user behaviour anomaly detection focus on building comprehensive visibility of everyone within your user community accessing or using the data.

Earlier in this paper we talked about profiling your organisation's digital shadow to establish an 'attacker's eye view' as a context to focusing resources and closing gaps. In the case of user behaviour anomaly detection, the goal is to join the behavioural dots across all of your users' accounts, devices, and IP addresses – building up a picture over time of normal practice so that exceptions can be identified in real-time and investigated. This technique can add a range of capabilities to a resilient cybersecurity architecture but from a malware perspective these solutions can help analysts, using granular behavioural algorithms, to spot where malware has entered and is trying to behave in a certain way. Even if malware has remained dormant for months and has successfully compromised a user's identity, it still has to be able to act like the user. This is where behaviour anomaly detection can set the alarm bells off without adding more noise to an analyst's role.

Managing 'unknown unknowns' is very different for each business but by using user behaviour anomaly detection information security professionals can 'know' their colleagues - gaining invaluable context for rapid analysis and action. Industry analysts such as Gartner predict that by 2017 up to 20 percent of serious security technology vendors, that focus on user controls or user monitoring, will incorporate advanced analytics and UEBA into their products, either through acquisitions, partnerships or internal development.

NTT Security point of view

As information security professionals we cannot remove the motive for cyber criminals, although by increasing our understanding we can focus investment and resources.

What we can do is match their ability to function and reduce their opportunity to be successful. Although still in the early stages of application, interesting and innovative approaches such as machine learning and deception techniques are providing sophisticated ways to automate advanced malware detection – enhancing protective, detection and even predictive capabilities.

Case Study – advanced malware protection – evolving a resilient cybersecurity architecture

A large financial organisation was concerned about the current and future impact and cost of malware. It was aware that existing signature based controls were inadequate, but was hesitant to increase the complexity of its information security estate with further point solutions. As part of an initiative to evolve a more resilient cybersecurity architecture, the organisation wished to create an advanced malware detection capability that would protect the current and future availability of customer IT services, data and information systems and prevent sensitive information disclosure.

Having worked with the customer to establish their business and investment priorities, NTT Security helped the internal client team to:

- Assess their current and desired malware detection capability in a business context
- Execute a comprehensive product evaluation process
- Implement the chosen technology solution – integrating with existing information security systems to deliver:
  - Detection of custom malware attacks that existing signature based controls were failing to identify
  - Rapid, relevant response to contain and eradicate malware threat
  - Increased data integrity
  - Intelligent threat reporting and contextual analysis that focused investment and increased predictive capability

The client has not only achieved its objective by enhancing the integrity and protecting the availability of its data systems – it is also confident that its investment in an integrated advanced malware detection solution will adapt to meet future organisational requirements.

What is resilient cyber intelligence capability?

At NTT Security, we work in partnership with our clients to build resilient cybersecurity architectures, transforming a mass of point technology solutions into a sustainable cyber defence capability. Internal and external threat data sources are transformed into intelligence that can help predict and prevent future attacks, defending the business from and responding to, current threats.

Technology innovation is at the heart of the cybersecurity industry as it attempts to keep pace with those that wish to disrupt, defraud or damage our organisations. Our technology partners consistently develop solutions that make the tasks associated with cybersecurity easier and faster – but more strategic planning, business context and rigorous evaluation must be applied to investment decisions.

Look out for the rest of our Cybersecurity Innovation series where we will examine how new solutions and approaches can help to create sustainable, resilient cyber architectures - or contact us to explore how our range of innovative services can help your organisation to drive greater business value from people, processes and technology to close the cyber intelligence gap.

Our range of consulting, managed security and technology services to help our customers build a resilient cyber defence architecture include:

- Assessment services including architecture, risk, capability and compliance
- Independent technology evaluations
- End-to-end implementation experience
- Managed services to build capability such as 24/7/365 monitoring and intelligence analysis

Visit **www.nttsecurity.com** to find out more

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organisations to build high-performing and effective security and risk management programmes, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com**

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.