ELSEVIER

network SECURITY

ISSN 1353-4858 September 2017

www.networksecuritynewsletter.com

...SPECIAL ISSUE...SPECIAL ISSUE...SPECIAL ISSUE...SPECIAL ISSUE...SPECIAL ISSUE...

The Nation-State Threat

There is a silent cyberwar in progress that is only ever partially reported. From time to time a breach occurs and blame is levelled – at Russia or China, usually. But the true extent of hacking by military groups or hacker gangs sanctioned by governments is a matter for speculation.

This is an issue for everyone, not just governments. Individuals and small groups may be targeted – witness China's alleged actions against activists for a free Tibet. Organisations are at risk if they possess intellectual property desirable to foreign states, and not just in the defence sector. To this day, many of Nortel's executives blame the company's spectacular demise on the theft of industrial secrets by China, and more specifically Huawei (which naturally denies it).

So what should you do? As an organisation, do you need to take special precautions against nation-state actors? Or are the appropriate defences the same as you'd use to thwart any hacker?

In this two-part investigation, all of the features in this issue are devoted to exploring the nature of the threat and what you can do about it. And we will follow up with a number of features on the same topic in next month's issue.

One lesson comes through clearly – sophisticated, widespread hacking by nation-state actors is a fact and we all need to deal with it.

State-backed hackers target US and European energy sectors

Skilled hackers, almost certainly working for a foreign government, have been attacking organisations in the energy sectors in the US and Europe, according to a report by Symantec. And in many cases they have succeeded in gaining access to core systems that control the companies' operations.

Symantec attributes the attacks to a group it dubs 'Dragonfly', which it says has been operating since 2011. According to the report, a 'Dragonfly 2.0' campaign has been underway since December 2015 but with a major ramping up of activity in the past couple of months. This is focusing mainly on organisations in the US, Turkey and Switzerland, with a smattering of targets in other countries.

Cyber-attacks against the energy sector are not new, but there does seem to have been a major increase in both attempted and successful hacking recently. In July, the US Department of Homeland Security and the FBI warned that hackers had been penetrating companies responsible for operating nuclear power stations and other energy facilities for a couple of months. And in August, EirGrid, which manages Ireland's electricity grid, revealed that hackers had installed malware on its systems capable of intercepting communications.

Symantec's research suggests that the Dragonfly hackers are mostly interested in discovering how the target systems operate and gaining access that would give them control. This knowledge, along with malware implanted on the target systems, would make it possible

Continued on page 2...

Contents

Editorial Office:
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.networksecuritynewsletter.com

Publishing Director: Bethan Keall

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Senior Editor: Sarah Gordon

Columnists: Tim Erridge, Karen Renaud, Colin Tankard

International Editoral Advisory Board:
Dario Forte, Edward Amoroso, AT&T Bell Laboratories; Fred Cohen, Fred Cohen & Associates; Jon David, The Fortress; Bill Hancock, Exodus Communications; Ken Lindup, Consultant at Cylink; Dennis Longley, Queensland University of Technology; Tim Myers, Novell; Tom Mulhall; Padget Petterson, Martin Marietta; Eugene Schultz, Hightower; Eugene Spafford, Purdue University; Winn Schwartau, Inter.Pact

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/network-security/1353-4858

12987
Digitally Produced by
Mayfield Press (Oxford) Limited

...Continued from front page

for the attackers to mount sabotage attacks, bringing down electricity networks, strengthening the idea that this is a nation-state attack rather than criminals looking to monetise the breaches.

"The Critical National Infrastructure (CNI) is the backbone of a nation's economy, security and health – with the electricity supply being fundamental to our everyday lives," commented Andrew Clarke, EMEA director at One Identity. "Studies in the US report that cyber-attacks are a constant and daily occurrence on utility companies, with some facilities receiving upwards of 10,000 attempted cyber-attacks each month – which equates to one attack every four minutes."

He added: "It is imperative that we continue to innovate to protect access and safeguard CNI. Segmenting networks with firewalls is one measure. And managing access by individual identity is key to really controlling who gets access and how they access systems. Patching systems so vulnerabilities are mitigated is also key."

The initial attack vectors were email phishing campaigns, watering hole attacks and email-delivered or web-based trojans. The emails were tailored to the energy sector – for example, some included invitations to an energy sector New Year's Eve party in December 2015.

Symantec has not publicly drawn any conclusions as to which state is behind the attacks. There's more information here: http://symc.ly/2ffGTAB.

Meanwhile, in the UK more than a third of organisations responsible for operating critical national infrastructure cannot meet the basic cyber-security standards set by the Government.

In March, Corero Network Security sent out Freedom of Information (FOI) requests to 338 organisation, including fire and rescue services, police forces, ambulance trusts, NHS trusts, energy suppliers and transport organisations. Around half of the organisations refused to respond, citing national security concerns. But of the 163 who did, 63 (39%) said they had not completed the National Cyber Security Centre's '10 Steps to Cyber Security' programme. This figure rises to 58% among NHS trusts. This is in spite of the fact that if they should be breached, these organisations could face fines of up to £17m, or 4% of turnover, under the Government's proposals to implement the EU's Network and Information Systems (NIS) directive.

Ransomware and IoT among leading threats

Increases in ransomware, business email compromise (BEC) campaigns and Internet of Things (IoT) vulnerabilities were among the biggest threats faced by organisations in the past six months, according to research by Trend Micro.

The '2017 Midyear Security Roundup: The Cost of Compromise' report from Trend Micro details the threats from the first half of 2017. The company detected more than 82 million ransomware threats in the first half of the year, along with more than 3,000 BEC attempts, reinforcing the need for security prioritisation. Despite the rising percentage of security spending in IT budgets, a recent report by Forrester notes that funds are not being properly allocated to address growing threats.

"Enterprises need to prioritise funds for effective security upfront, as the cost of a breach is frequently more than a company's budget can sustain," said Max Cheng, chief information officer at Trend Micro.

In April and June, the WannaCry and Petya ransomware attacks disrupted thousands of companies across multiple industries worldwide. The global losses from the attack, including the resultant reduction in productivity and cost of damage control, could amount to as much as $4bn. In addition, BEC scams raised the total of global losses to $5.3bn during the first half of 2017, according to the Federal Bureau of Investigation (FBI).

As predicted, in the first half of the year, firms experienced a rise in IoT attacks. In collaboration with Politecnico di Milano (POLIMI), Trend Micro showed it is possible for industrial robots to be compromised, which could result in massive financial damage and productivity losses. According to the firms, smart factories can ill-afford to dismiss the importance of securing these connected devices.

The full report is available at: http://bit.ly/2xtQpum.

In brief

Hackers use nation-state tools

Leaks suffered by intelligence agencies have put nation-state tools into the hands of ordinary cyber-criminals – that's one of the key messages of Check Point's 'Cyber-attack Trends: Mid-Year Report'. The most obvious example is the WannaCry (aka WannaCrypt) campaign that exploited tools and vulnerabilities disclosed in the leak of NSA material by the ShadowBrokers group. This led to criticism of intelligence agencies for stockpiling vulnerabilities. The Check Point report also claims to have recorded a near doubling of ransomware attacks in the Americas, Europe, Middle East and Africa. And nearly a quarter of the organisations the company contacted had been affected by malvertising campaigns. The report is available here (PDF): http://bit.ly/2h2aqBz.

Trump boosts Cyber Command

US President Donald Trump has promoted the US Cyber Command – the country's information warfare arm – to the status of a Unified Combatant Command. Until now, Cyber Command has been an offshoot of the NSA, sharing facilities and a commander. However, this move places it in a more autonomous position. 'Unified' commands typically draw personnel from at least two branches of the military and the upgraded Cyber Command will now report directly to the Secretary of Defense. A statement by Trump said that the move will, "help streamline command and control of time-sensitive cyberspace operations by consolidating them under a single commander with authorities commensurate with the importance of such operations." There are also moves afoot to separate Cyber Command entirely from the NSA. The changes have been driven by Defense Secretary Jim Mattis, a former US Marine Corps general. And it is consistent with Trump's known dislike of the intelligence agencies and trust in the military.

Embassies hit by malware

Security firm Eset says it has identified a strain of malware, dubbed Gazer, that appears to be targeting embassies and consulates in Eastern Europe. Delivered via spear-phishing emails, Gazer opens a back door on infected machines, allowing for full remote code execution and activity monitoring. The malware is very stealthy, living within an encrypted container and uses legitimate but compromised websites for its command and control channels. The binaries also attempt to look like a harmless game by scattering messages such as "Only single player is allowed" throughout the code. The malware has been active since 2016, Eset believes, and there is some evidence to connect it with the Turla hacking group, which has links to the Kremlin. Eset's report is here: http://bit.ly/2fhdzK3.

Sending back malware

Lieutenant-General Vincent Stewart of the US Defense Intelligence Agency has suggested that the US military may hit back at attackers by sending their malware back to them in weaponised form. Speaking at the Department of Defense Intelligence Information System Worldwide Conference, which was attended by representatives of US, Canadian and UK military forces and intelligence agencies, he said: "Once we've isolated malware, I want to reengineer it and prep to use it against the same adversary who sought to use against us. We must disrupt to exist." The comment seems to overlook the attribution problem and the general opinion among security experts that 'hacking back' is a dangerous (and usually illegal) move. However, it does reflect an overall mood among military forces that the cyber sphere is gaining ever-greater significance.

University breaches

A Freedom of Information request by *The Times* has revealed that UK universities are a major target for cyber-criminals targeting scientific, engineering and medical research. Breaches at places such as Oxford, Warwick and University College London have doubled over the past two years to 1,152 incidents in 2016-17. The attackers are nation states or hackers looking to sell the data to foreign governments. In many cases, the hackers did not have to work very hard as universities typically have weak security. There's more information here: http://bit.ly/2gXZjpr.

North Korea steals bitcoins

North Korea may be targeting Bitcoin exchanges as a way of obtaining foreign currency. A few weeks ago, South Korea's Cyber Warfare Research Centre alleged that at least one exchange had been breached and bitcoins stolen in an attack emanating from the north. Now, security firm FireEye claims that, "since May 2017, we have observed North Korean actors target at least three South Korean crypto-currency exchanges with the suspected intent of stealing funds". The attacks typically use spear-phishing emails aimed at employees working at digital crypto-currency exchanges. There is more information here: http://bit.ly/2xjzwlB.

Android botnet taken down…

Coordinated efforts by a number of tech firms have taken down the WireX botnet which was running mainly on compromised Android devices. The botnet was first spotted at the beginning of August and within a couple of weeks had acquired tens of thousands of infected nodes. Google found – and eliminated – around 300 malicious apps in its own Play Store posing as legitimate software such as media players and even ring tones. It's difficult to estimate the size of the botnet – one claim put it at "low six figures" – but users in over 100 countries were affected. The infected devices were being used to launch distributed denial of service attacks by sending out HTTP GET requests. Collaboration between the targets of the attacks, DDoS mitigation firms and threat intelligence companies resulted in the botnet being taken down. However, there are still questions to be asked as to why Google's Play Store accepted hundreds of trojanised apps. There's more information here: http://akamai.me/2woVvmE.

…but major flaw remains

All versions of Android prior to the current one, Android 8.0 Oreo, are vulnerable to a form of attack that uses an invisible window drawn on the screen. This overlay attack, discovered by Palo Alto Networks, intercepts user input and can lead to the installation of malware, including data-stealing programs. Google has issued a patch, but the nature of the Android ecosystem means that most devices will never receive it. There is more information here: http://bit.ly/2eVzciv.

Bluetooth flaw

Security firm Armis says it has found a vulnerability in Bluetooth that could allow devices to be taken over, have malware installed or be subject to man in the middle attacks. It could even enable an attacker to spread an exploit by getting Bluetooth-equipped devices to spread an infection from one to the other. The so-called 'Blueborne' issue actually involves eight related vulnerabilities affecting Android and iOS mobile devices as well as equipment running various flavours of Linux, such as Tizen-based TVs. The precise details of the problem haven't been made public as Armis is following a 'coordinated disclosure' protocol. Google and Microsoft made patches available soon after the announcement of the issue and anyone running the latest version of Apple's iOS is already safe. However, Armis calculates that around 1.1 billion Android devices (about 55% of the total) will remain vulnerable because they are running outdated versions of the OS and can't easily receive patches. Similarly, around 80% of Linux instances, running on an estimated 960 million devices, will remain vulnerable. There's more information here: www.armis.com/blueborne/.

Reviews

BOOK REVIEW

Deception in the Digital Age
Cameron Malin, Terry Gudaitis, Thomas Holt, Max Kilger.
Published by Academic Press.
ISBN: 9780124116306. Price: £69.95, 284pgs, paperback.
E-book editions also available.

When you start studying information security in any depth, sooner or later you come to a realisation – that it's not really a technical issue but is actually about people and behaviours. The technical aspects are merely the tools and channels through which actors attempt to achieve their ends.

Sometimes technology can play a relatively minor role. Kevin Mitnick, once on the FBI's 'most wanted' list as a notorious hacker (and now, inevitably, a security consultant), was certainly technically adept. But most of his 'hacks' involved social engineering – essentially talking people into doing things they shouldn't do.

Similarly, I know of penetration testing firms that often manage to breach their customers' systems without employing a single technical exploit. Often 'pretexting' – pretending to be someone you're not to engage the sympathy or play on the anxieties of someone within the organisation – is more effective than malware, SQL injection or any other computer-dependent method.

Deception is a key element in social engineering. The ability to control another's beliefs and thought processes through fake narratives is a common enough phenomenon in human interaction, but it assumes even greater significance when deployed in political, military, intelligence and criminal pursuits. And technology is a powerful tool for the deceiver.

This book, then, examines many aspects of deception and particularly how it is used within the context and with the help of digital technology. It starts with a chapter on misdirection, moving from its use as one of the essential skills in magic through to showing how the same concepts are employed in weakening human defences in social engineering contexts.

The power of deception often stems from the use of narratives, pulling victims into a story whose threads cover the underlying lie. Scammers and confidence tricksters have exploited the power of storylines for centuries. And today, people still fall for emails with engaging and emotional tales – such as the fraudulent message that appears to come from a friend with a plea for financial help to get home after being robbed of wallet and passport. The book then moves on to cover psychological concepts deployed in a wide range of contexts, including business, advertising, politics and military operations.

Behaviour is shaped by one's environment and the authors go on to explore the nature of underground communities, such as cybercrime markets and how their social ecosystems affect the activities of individuals. The book also describes some of the main forms of attack that exploit deception, at least in their initial stages, including watering hole attacks and ransomware. The nexus of technology and psychology is further explored in studying how videos and photographs are manipulated and used online in order to deceive.

Then we get onto major threat groups, with most of the attention being given to cyber-jihadists and nation-state actors, followed by a chapter on honeypots before finally rounding off with some speculation on how deception is likely to be employed in the threats of the future.

The idea that deception is a key element in cyber-attacks will not come as much of a surprise to, well, anyone. It forms the basis of much, if not most, cybercrime, including spam, phishing, malvertising, fake AV and fake technical support, watering hole attacks, business email compromise and even fake news. And many scams trace their origins to pre-computer days – business email compromise, for example, was thriving as a fax-based form of fraud long before the Internet became ubiquitous.

How the power of authority is used to gain a victim's trust.

It would seem that the idea behind this book is that knowing how your attackers think and the dynamics of the deceptions they employ will help you build stronger defences. It's unlikely that this is going to be of much benefit to security professionals in the front lines of defending an organisation – the people writing firewall rules and responding to SIEM alerts. The approach and the writing style seem too academic and abstract to offer much in the way of practical assistance.

"It is people who are attacking you and frequently your own people who will prove to be the weak link in your armour. The strongest security strategies are those that acknowledge and get to grips with the human dimension"

However, it's easy to conceive of some groups of people who might gain valuable insight from this book. For a start, there are those who formulate organisations' security strategies. All too often, information security is perceived as a technical problem requiring a technical solution – hardware and software. 'Meatware' – which is to say, people – don't feature in the equation. And this is dangerous because it is people who are attacking you, and frequently your own people who will prove to be the weak link in your armour. The strongest security strategies are those that acknowledge and get to grips with the human dimension.

And this brings us on to the group that could gain the most from this book – anyone tasked with security training and raising awareness of cyber-risks. The insights into the psychology and motivations of attackers, as well as the tricks they use, could be highly valuable in adding depth to training aimed at combatting threats such as phishing and social engineering.

It's worth noting, too, that the book is well illustrated, both in terms of diagrams illustrating key concepts and screenshots of sample attacks. And it's well referenced for those who want to dig deeper.

While not every security practitioner will necessarily derive practical benefits from this book, deepening your understanding of the attacker's mindset and the toolbox of tricks likely to be used against you can only be an advantage in the constant battle of wits being fought in the digital realm.

There's more information here: www.elsevier.com/books/deception-in-the-digital-age/malin/978-0-12-411630-6.

– SM-D

Nation-state attacks: practical defences against advanced adversaries


Travis Farral

Travis Farral, Anomali

Many of the biggest stories in information security over the past few years have involved suspected nation-state actors compromising individuals and organisations, large and small, to advance state agendas. Most of these entities probably had no idea they were being targeted by nation-state actors at the time of being compromised.

This was probably the case for John Podesta, Hillary Clinton's campaign chairman during the 2016 US presidential election, whose private Gmail account was compromised, leading to the public release of thousands of his emails on WikiLeaks. It was partially due to the compromise of Podesta's email, along with an attack against the Democratic National Committee (DNC) that led the Macron campaign in France to step up security measures leading up to the French election. Despite those efforts, however, sensitive emails and other documents reportedly belonging to the Macron campaign were released to the public by hackers.

"Organisations of every size and in every industry have been impacted in one way or another by attacks suspected to have been carried out by nation-state actors. How do organisations know if they are being targeted and what should they do to protect themselves?"

Political attacks, like the two above, get a lot of attention – and rightfully so. But they are not the only attacks suspected to have been carried out by nation-state actors in recent months. Other attacks like those against power companies in Ukraine, the WannaCry ransomware, and the NotPetya (Petya) ransomware attack are all suspected to have been carried out by actors with ties to nation states.

Organisations of every size and in every industry have been impacted in one way or another by such attacks. With this reality in mind, how do organisations know if they are being targeted and what should they do to protect themselves?

Analysing the public details from these suspected nation-state attacks provides some answers that can give helpful guidance on how to tell where attacks may happen in the future and what organisations and individuals should do to protect themselves.

Examining attacks

The goal in looking through previous attacks attributed to nation-state actors is not to develop a list of domains, IP addresses and malware hashes to block. Those things can be easily changed for future attacks. The real aim is to look at common techniques used to develop defences that would detect or prevent similar attacks in the future.

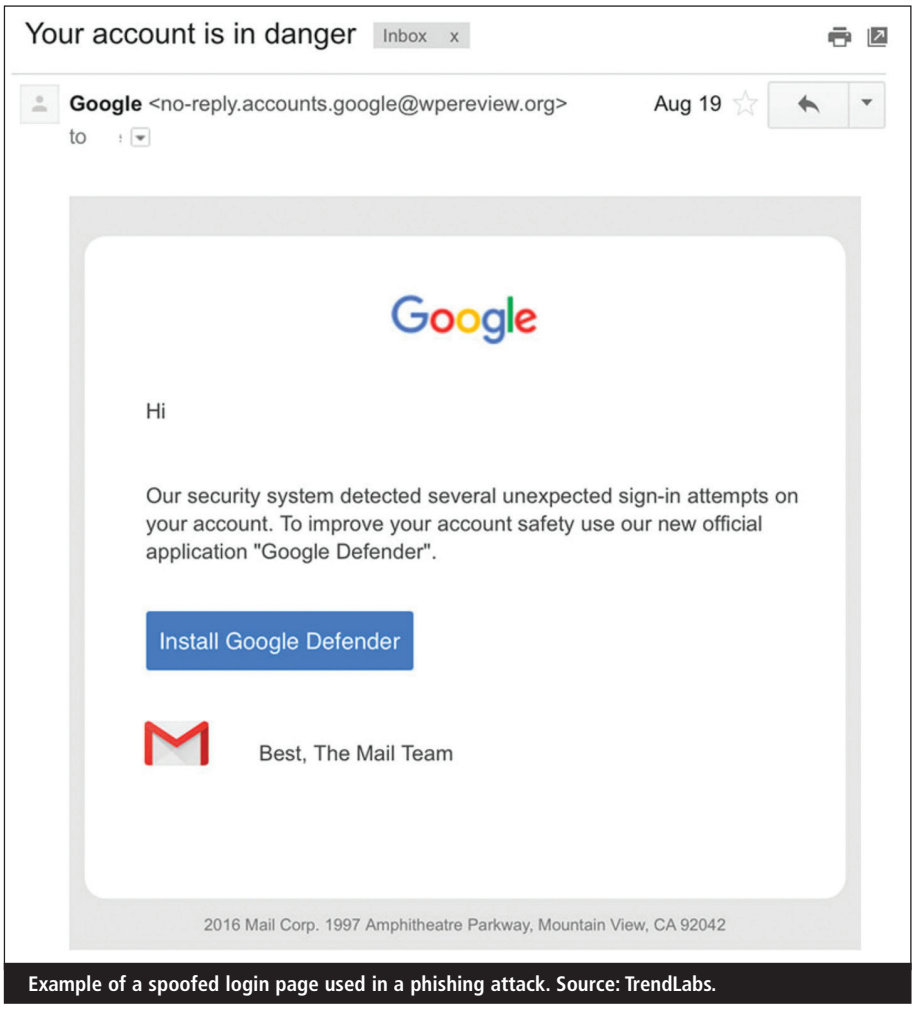
This will not be an exhaustive analysis but will merely review some public details from various attacks attributed to nation states and note some key techniques used. Finally, the analysis will conclude with some potential countermeasures and key takeaways.

Political targets

In April 2017, just weeks before the French Election, Trend Micro released a report that contained suspected activity by Russian actors that may have been used to target the Macron campaign.[1] The report highlighted a particular domain, onedrive-en-marche[.]fr, that might have been used in a phishing attack against campaign staffers to gain access to emails or other documents. While no specifics have emerged on whether or not this domain was used for malicious purposes, just days before the French election a trove of data was released by hackers that was supposedly taken from Macron's campaign.

Registering domains that are similar to the domain of the target organisation and then using those in social engineering attacks such as phishing, is a technique favoured by some nation-state actors. This was precisely the type of attack suspected in the compromises of the DNC and Podesta during the US election in 2016. Although no details have emerged about how the DNC was initially compromised, there is a suspicion that a misspelled domain name (misdepatrment[.]com) may have been used. Podesta's compromise may have happened via a phishing email containing a Bitly URL that obfuscated a link to myaccount.google.com-securitysettingpage[.]tk. To carry out the attack, this page would have been made to look like a Google login page and would be able to capture any username and password entered in the appropriate fields. Using URL shortening services such as Bitly is a technique used to mask links to malicious URLs and, like using misspelled or obfuscated domains in phishing emails, is a technique that is not limited to use by nation-state actors.

So far, we have two distinct techniques that seem to be leveraged by nation-state actors to compromise their targets



Example of a spoofed login page used in a phishing attack. Source: TrendLabs.

– leveraging domain names similar to domains used by the target (obfuscated or misspelled) and use of URL shortening services to obfuscate malicious domains.

Critical infrastructure

On 23 Dec 2015 at around 3:35pm local time, several electricity substations were disconnected around the Ivano-Frankivsk Oblask region in Western Ukraine. The resulting power outages affected around 225,000 customers. Ultimately, the power company had to switch to manual operation to restore power as a remote attacker had gained control of the management system used to control the substations.

The attack was eventually blamed on Russian state actors. Once again, phishing attacks appear to be the start of this attack. The adversary used weaponised Microsoft Office documents to gain a foothold and harvested credentials to carry out the attack. To ensure success, the targeted users would have had to enable macros after attempting to open Office documents attached to phishing emails.

In this example, one could observe a classic nation-state technique – that of using Microsoft Office attachments in emails as bait to entice users to click. The attackers would then hope that the targeted users enabled macros so the attackers could gain access to their systems.

Ransomware

The WannaCry attack used a new creation – part worm, part ransomware. Neither worms nor ransomware are new in 2017, but the idea of combining the two along with a recently patched exploit made it particularly effective. It's unknown how WannaCry was initially deployed but it is well-known how it spread. Once infected, systems would scan both the internal network as well as a random set of IP addresses on the Internet and attempt to infect new targets. Because WannaCry leverages a potentially unpatched exploit to spread to new systems, it spread quite effectively among Windows systems that hadn't deployed the Microsoft MS17-010 patch. The exploit used can also be referred to as EternalBue and is a rare type of exploit that can be delivered remotely, gains administrative access to the targeted system and works against the default installation of a broad installed base of Microsoft Windows users. The last time an exploit of this magnitude was discovered was in 2008, which was patched as part of Microsoft MS08-067. WannaCry has been blamed on a group of hackers associated with the Government of North Korea.

"As systems checked-in for updates, they pulled down and executed the malware. Once infected, systems would then quickly spread infections to other internal systems"

The NotPetya attack in June 2017 was another ransomware that came with worm-like qualities although it did not spread as effectively as WannaCry. This may have been by design to contain the malware as closely as possible to the country of Ukraine and organisations that do business there. This ransomware also included the EternalBue exploit but this was not its primary method of spreading to other systems. NotPetya was initially deployed via a compromised update server for the MeDoc Ukrainian accounting software. As systems checked-in for updates, they pulled down and executed the malware. Once infected, systems would then quickly spread infections to other internal systems using credentials stolen from memory. This process turned out to be very effective. Russian state-sponsored actors are suspected to be behind the NotPetya attack.

Within these two examples, a number of techniques were used: a recently patched remote code execution exploit; leveraging a supply-chain attack by attacking a small accounting software company and using its update server to deploy malware; and credentials stolen from memory to spread through a network.

Guidance and practical defence

The following summarises the findings in this analysis along with some practical guidance for defence. Note that because these techniques aren't limited to nation-state actors, applying these defences also helps against a variety of attackers.

Spoofed/misspelled domains used for social engineering attacks:

- Proactively search for and block new or existing unofficial domains similar to your organisation's or its partners' and suppliers'.
- Look for the presence of spoofed or misspelled domains in logs as a hunting activity; investigate any findings.

Use of URL-shortening services in emails or social media:

- Block or remove URL-shortened links from emails.
- Train collaborators to use full URLs in email communications.
- Block URL-shortened links in social media or use tools that reveal the full URL and train users to leverage those before clicking.

Use of macros in Microsoft Office documents sent over email:

- Block macro-enabled office documents at email gateways.
- Train users to not enable macros for Office documents received over email or downloaded from the Internet.

Use of recently patched exploits:

- Deploy critical patches in a timely manner across the entire enterprise.
- Patching can be difficult to do quickly in certain environments; seek ways to mitigate exploitation against unpatched systems for critical patches until patches can be deployed.

Use of supply-chain compromise to access an organisation from the inside:

- Limit access of systems that require communication to outside resources (network isolation, limit use of broad access or administrative accounts, limit user access).
- Play out scenarios where an update server is fully compromised and mitigate any findings; test resulting mitigations.
- Apply additional investigative controls to systems with outside access or that require communication with outside resources.

Use of tools to harvest credentials from a compromised system:

- There are a handful of ways this is done – use endpoint tools to look for or block any signs of this type of activity or the use of known tools that can do this.
- Anti-virus may help against known tools that harvest credentials from memory; test common tools against standard builds to understand strengths and weaknesses with current endpoint solutions; work with endpoint companies to improve results.

Using compromised credentials to spread inside an organisation:

- Limit interactive administrative and broad access logins especially to sensitive systems (domain admins should only be logging to domain controllers and only from known secure systems, for example).
- In general, consider that email and web access are the most dangerous activities in an organisation – treat those systems as hostile and limit the access of accounts that work from those systems; this limits the potential damage should one become compromised.
- Use two-factor authentication for all sensitive systems and sensitive accounts; also use for all external and third-party access.

Determining risk

Although analysing past attacks by nation states helps inform future defence strategies, it is important that this is reinforced with regular risk checks. Organisations need to have a good understanding of the threats that are coming into their networks. They should ask themselves which of their assets are the most valuable to nation-state hackers. By doing so, they can identify which assets are most valuable and better distribute security resources.

Organisations should assimilate intelligence from multiple sources to illuminate any blind spots and make informed decisions. For too long, businesses have relied on just data, forgetting that it is the data's context that is often the most valuable. The tactical approach of responding to threats as they happen is no longer enough. Given hackers' adaptability and sophistication, organisations must look at intelligence more strategically.

Understanding the threats that are coming into your business will allow you to develop an effective and customised system that means you'll be aware of all of the possibilities. Having a well-educated team is invaluable and one of your best lines of defence against hackers.

Conclusion

Nation-state attacks are often portrayed as advanced and sophisticated but this is rarely the reality. Nation-state actors are persistent in achieving their goals but mostly use non-sophisticated techniques because they continue to see success using them. Organisations that investigate and learn from the public details that come from these attacks can deploy smart mitigations against the techniques used. The result is a harder target that stands a better chance of discovering or preventing attacks from nation-state actors.

About the author

Travis Farral, previously supervisor of cyber-security intelligence & strategic services at ExxonMobil, brings more than 15 years of experience to the Anomali team. He has worked with technical security solutions for both cyber-security companies and global corporations. As director of security strategy, Farral applies his deep knowledge of the threat landscape to support Anomali's customer growth and product roadmap.

Reference

1. 'Two Years of Pawn Storm'. TrendLabs, 2017. Accessed Aug 2017. https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf.

Assessing nation state threats

Jon Condra, Flashpoint

Jon Condra

Cyber-attacks by nation states are increasingly emerging from the shadows and garnering greater public awareness. Suspicions over meddling in elections have given rise to mounting political tensions and even led many to question the accuracy of election results. These issues are in turn creating widespread public concerns over the cyber activities and capabilities of nation states.

For example, in 2017 a furore ensued following Russia's alleged hacking of the French presidential election when Emmanuel Macron's emails were leaked just prior to his election. Meanwhile in the US, concerns over Russia's possible interference in the presidential election of Donald Trump persist. These and other issues are inevitably raising questions about the origins of and reasoning behind such attacks, as well as how countries can defend themselves.

A recent report examined the cyber and geopolitical threat landscape over the first half of 2017, providing additional visibility into the activities, potential impacts and capabilities of nation states.[1] In addition, the report identified 'flashpoints', also known as bellwethers or key events, to watch for 2017 that – should they occur – may prove to prompt shifts in the cyberthreat and geopolitical environment.

Some of the major flashpoints identified in the report focus on nation states, including:

- Tensions in East Asia over the North Korean conundrum boil over into more direct and heated conflict between North and South Korea, the US and potentially China. A potential trigger for such an incident may be the continuing provocation of North Korea's nuclear weapon and long-range missile tests.
- The Trump administration adopts a less-compromising approach towards US-China relations, or otherwise enacts policies that threaten Chinese 'core interests'. Alternatively, China adopts an increasingly aggressive policy towards securing its vital 'core interests', including the South China Sea and the questions of Taiwan's and Hong Kong's political sovereignty.
- Russia is found to have interfered in additional European elections, including the upcoming German federal election in September 2017.
- The situation in Syria deteriorates further into armed conflict between major states with differing interests in the region.
- Other nation states, such as China, Iran, and North Korea, adopt the Russian model of engaging in 'cyber influence operations' via proxies, resulting in the exposure of such a campaign.

To be clear, these flashpoints are not intended to be near-term predictions, but instead to serve as potential events to monitor given the global geopolitical environment.

Nation-state threats

Russia – one of a handful of the US's peer competitors in cyberspace – remained highly active during the first half of 2017. For the most part, malicious cyber activity emanating out of Russia has been linked to Moscow's efforts to influence various elections in Western European countries, not the least of which include France and Germany, through compromising political opposition groups and engaging in disinformation campaigns. This behaviour is reminiscent of the campaign against the US Democratic National Committee and the Hillary Clinton campaign at the end of 2016 – over which the US Government is still debating an appropriate response.

Aside from attempts to influence high-profile elections, in April the UK Foreign Office stated that several civil servants were targeted by a spear-phishing campaign with direct links to the group that perpetrated the attack on the US Democratic National Committee in 2016. Likewise, Denmark subsequently accused APT28 of carrying out attacks on the Danish Defence and Foreign Ministries in 2015 and 2016.

Furthermore, China remains a highly capable actor in cyberspace and a demonstrated threat to Western and East Asian entities. Despite Chinese state-sponsored actors' relative quiescence throughout the first half of 2017, several organisations linked China to attacks against Western and East Asian targets during this time. In particular, in early March the US Department of Homeland Security released a report detailing recent activity under the 'Pleasantly Surprised' campaign, which involved spear-phishing attempts against commercial entities in the financial, retail and technology sectors.

In at least one other case, the suspected Chinese Advanced Persistent Threat (APT) group APT10 was linked to a campaign targeting the US-based National Foreign Trade Council (NFTC) at a time that coincided with Chinese President Xi Jinping's and US President Donald Trump's summit in the US in early April. Around that same time period, a joint report between PricewaterhouseCoopers and BAE Systems detailed APT10 activity against unnamed international managed service providers and a host of Japanese entities.

Threat Actors	Financial Services	Retail	Legal	Energy	Healthcare	Tech / Entertainment	Telecom	Gov / Military	NGOs / Civil Society	Capabilities	Potential Impact
China	√		√	√	√	√	√	√	√	Tier 6	Catastrophic
Five Eyes	√			√		√	√	√		Tier 6	Catastrophic
Iran	√			√			√	√	√	Tier 4	Moderate / Severe
North Korea	√			√		√	√	√		Tier 4	Severe
Russia	√		√	√		√	√	√	√	Tier 6	Catastrophic
Disruptive / Attention-seeking Actors						√		√		Tier 3	Moderate
Cyber-criminals	√	√	√	√	√	√	√			Tier 4	Severe
Hacktivists	√	√		√		√	√	√	√	Tier 3	Moderate
Jihadi Hackers	√					√		√		Tier 2	Negligible

Tier 1	Tier 2	Tier 3	Tier 4	Tier 5	Tier 6
The cyber actor(s) possess extremely limited technical capabilities and largely make use of publicly-available attack tools and malware. Sensitive data supposedly leaked by the attackers are often linked back to previous breaches and publicly-available data.	Attackers can develop rudimentary tools and scripts to achieve desired ends in combination with the use of publicly-available resources. They may make use of known vulnerabilities and exploits.	Actors maintain a moderate degree of technical sophistication and can carry out moderately-damaging attacks on target systems using a combination of custom and publicly-available resources. They may be capable of authoring rudimentary custom malware.	Attackers are part of a larger and well-resourced syndicate with a moderate-to-high level of technical sophistication. The actors are capable of writing custom tools and malware and can conduct targeted reconnaissance and staging prior to conducting attack campaigns. Tier 4 attackers and above will attempt to make use of publicly-available tools prior to deploying more sophisticated and valuable toolkits.	Actors are part of a larger and well-resourced organisation with high levels of technical capabilities such as those exhibited by Tier 4 actor sets. In addition, Tier 5 actors have the capability of introducing vulnerabilities in target products and systems, or the supply chain, to facilitate subsequent exploitation.	Nation-state supported actors possessing the highest levels of technical sophistication reserved for only a select set of countries. The actors can engage in full-spectrum operations, utilising the full breadth of capabilities available in cyber operations in concert with other elements of state power, including conventional military force and foreign intelligence services with global reach.

Major threat actors, the sectors they most threaten and their capabilities. Source: 'Business Risk Intelligence: Decision Report – 2017 Mid-Year Update', Flashpoint.

Finally, in early May, FireEye reported that its researchers had observed Chinese threat actors attempting to compromise an organisation associated with the deployment of the Terminal High Altitude Area Defence (THAAD) anti-ballistic missile system in South Korea. In its totality, suspected Chinese state-sponsored cyber activity in the first half of 2017 suggests that China remains a potent force both technically capable and intent on compromising foreign targets in support of its national objectives. However, it is worth noting that the overall volume of such attacks appears to have dropped precipitously since its zenith and targeting has pivoted substantially towards entities and governments in East Asia and China's geographic neighbourhood in particular.

Five eyes

The 'Five Eyes' countries (consisting of the UK, US, Canada, Australia and New Zealand) together represent the pinnacle of cyber capabilities of all actors in cyberspace: they do not carry out highly disruptive or destructive attacks against allied or Western systems, especially during peacetime. As such, the Five Eyes are unlikely to be considered threat actors for Western organisations and individuals. Nevertheless, their broad reach, unparalleled levels of technical sophistication and high levels of co-ordination make them formidable adversaries for those who are targeted for either the purposes of intelligence collection, disruption, or destruction during wartime.

Iran continues to be a moderately capable threat actor in cyberspace that is believed to have invested a great deal in cyber weapons as a means both of countering the US's conventional military clout and of projecting power regionally. Iran also boasts a relatively robust cadre of researchers and technology enthusiasts known to comprise various well-known hacking groups, such as the Ashiyane Digital Security Team and OffSec.

One notable aspect of Iran's cyber strategy is the overwhelming focus on exploiting vulnerabilities in critical infrastructure systems, largely due to such targeting's ability to cause widespread damage and disruption even for more classically powerful adversaries such as the US.

"Pyongyang's capabilities in cyberspace are believed to be heavily contingent on Chinese infrastructure and, at a minimum, tacit political support from Beijing."

Iranian cyber actors have been relatively quiescent throughout the first half of 2017, with some notable exceptions. In early February, the Iran Threats Team detailed a new malware sample linked to Iranian actors dubbed

'MacDownloader' that was being used against the defence industrial base and a human rights advocate.

North Korea is widely believed to remain a potent threat in cyberspace. In the past, the reclusive country has proven its capability to strike foreign targets both in the US and South Korea, in particular, with significant effect. Pyongyang's capabilities in cyberspace are believed to be heavily contingent on Chinese infrastructure and, at a minimum, tacit political support from Beijing.

Nevertheless, despite heightened tensions in the region, Pyongyang appears for the most part to have been quiet in cyberspace thus far in 2017, with at least two exceptions affecting neighbouring South Korea. In January, South Korean media reported on a series of phishing emails ostensibly sent by North Korean threat actors to South Korean organisations focused on North Korea research and policy, as well as human rights issues, using clever lures that would quite likely be of interest to the victims.

Again in late March, phishing emails were disseminated to North Korean defectors and organisations whose main missions revolve around the cause of human rights in North Korea; the attackers feigned affiliation with the 'South Korean Public Relations Department'.

Countering the threats

The number one way to mitigate the risk emanating from adversaries who are utilising the deep and dark web is to understand and effectively monitor their activity in that space. If you know what your adversary will do before he or she does it, then you can act to mitigate the threat and implement the defences needed to guard against an attack.

Linguistic and cultural expertise is also vital to using the deep and dark web for defensive purposes. Understanding how networks communicate and having an understanding of the true meaning behind their interactions is crucial; the most successful analysts have spent years immersed in the deep and dark web working to acquire and hone their skills.

It is imperative to recognise that the deep and dark web plays a critical role in international cyber-espionage. The numerous examples above all highlight how various nation states are continually seeking to disrupt vital infrastructure in countries that are considered to be weak or adversaries. The bellwether events we have identified make the likelihood of increased cyber-attacks orchestrated by nation states very likely. A combination of investment and expertise is therefore vital in helping to counter the threats, which are growing and very real.

About the author

Jon Condra serves as director of Asia Pacific research at Flashpoint. He joined the company in 2014 from Versign iDefense. Aside from helping co-ordinate Flashpoint's subject matter experts and the delivery of intelligence products, Condra specialises in East Asian – and in particular Chinese – underground communities, including hacking, hacktivist and cyber-criminal communities. Condra speaks and reads Mandarin Chinese and has a BA from Gettysburg College and an MA in Security Studies/Intelligence from Georgetown University.

Reference

1. 'Business Risk Intelligence: Decision Report – 2017 Mid-Year Update'. Flashpoint. Accessed Aug 2017. http://go.flashpoint-intel.com/docs/BRI-Decision-Report-Midyear2017.

State-sponsored hackers: the new normal for business


Adam Vincent

Adam Vincent, ThreatConnect

State-sponsored hacking has become an all-too-common part of the cyber-security landscape – and not just for governments but for commercial business too. Organisations of all sizes, from small businesses to NGOs, political parties and governments have had to deal with attacks from state-backed actors in recent months.

These attacks play into the foreign policy aims of major global players such as Russia, China and North Korea, serving to test their opponents' defences and extract useful information on everything from economic activity to military might. The Cold War has been replaced with the Cyber War, as world powers use the relative anonymity of the Internet to conduct espionage and sabotage operations. And as we've seen with the recent NotPetya and WannaCry attacks bringing down Heathrow and the NHS, cyber-attacks now carry a danger of serious real-world effects.[1,2]

National impact

The attacks surrounding the 2016 US presidential election are a perfect example of the impact that state-sponsored attacks can have on a national stage. The attackers gained access to large amounts of sensitive data and demonstrated their ability to influence a national election, causing a series of disruptions that are still rolling on nearly a year later in the

form of the FBI probe and the Comey inquest. It's no longer a question of small-time criminals extorting browsers – hacking has reached centre stage in the world's biggest political environment.

State-backed attacks are not confined to corridors of power like the Kremlin and the Pentagon, however. Private enterprises that engage in sensitive activities or support government systems are just as likely to come under attack as public institutions. The same is true for non-profit and regulatory bodies. And for companies that have no direct connection to government activity, there is also the risk of economically motivated attacks – last year, for example, we identified Chinese-based hacks targeting a European consumer electronics company that specialises in drone technologies. While there are potential military uses for Western drone tech intelligence, it's equally possible that any information gathered could be put to commercial use, helping China's vast consumer manufacturing industry to keep one step ahead of the global competition.

"Private enterprises that engage in sensitive activities or support government systems are just as likely to come under attack as public institutions. The same is true for non-profit and regulatory bodies"

National pride can be a motivation, too. That was demonstrated by the Russia-based hack by the so-called 'Fancy Bear' hacker group (also known as APT28, Pawn Storm, Sofacy Group, Sednit and Strontium) on the World Anti-Doping Agency (WADA) shortly after the Olympics.[3] Activity that is perceived to damage the Russian national character is liable to call down a retributive state-sponsored attack – in this case, as revenge for banning Russian athletes from the Olympic and Paralympic Games for drug use. Fancy Bear replicated the WADA's actions against Russia by revealing US and UK athletes' (so far legal) drug use. Clearly, being seen to support or oppose a particular state's interests can put an organisation in serious danger of attack.

The Fancy Bear hacking group carried out attacks related to the banning of Russian athletes from the Olympic games.

Organisations of all kinds need to be aware of this powerful type of threat – the days when companies had nothing worse to fear than enterprising fraudsters are long gone. It is essential that security directors have the knowledge and the tools to defend their businesses against state-prompted cyberthreats. To do this, they must first understand the key behaviours of state-sponsored hackers.

Smokescreens and aliases

One of the most prevalent tactics among this class of state-sponsored actor is 'denial and deception' – essentially the practice of using a false identity to throw investigators off the trail. The anonymity of web-based attacks means that nation states can operate via puppet actors, making it extremely difficult to prove links between individual hacks and state intelligence. Even if those links are made, it is still unlikely that analysts will be able to determine the exact origin and purpose of the orders behind them.

For example, Fancy Bear carried out the WADA breach using patterns that are strikingly similar to known Russian *modus operandi*. The waters are muddied, however, by the fact that they also claim allegiance with Anonymous Poland, a hacker group that ordinarily operates within the Polish political sphere and with Polish interests in mind. As a result, its purported involvement seems suspicious – it certainly doesn't sit easily with the hack's clearly pro-Russian motives. This ambiguity makes it extremely hard for analysts to pin down the culprit.

'Guccifer 2.0', the hacker behind the DNC leaks, exemplifies this slippery aspect of the state-sponsored hacker. He has presented himself on Twitter and during an 'in-person' appearance in September 2016 at the Future of Cyber Security event in London as a lone hacktivist out for justice, in the same vein as Edward Snowden and Julian Assange.[4] However, tell-tale details including his unlikely server hosting locations and his lack of credible backstory point towards a Russian denial and deception operation. In effect, this means he is likely to be either a puppet actor (potentially even a full-time intelligence agent) or a construct – a straw man designed to draw attention away from the root aims of the state.

The purpose of these distractions is to confound security analysts' attempts to plug the gaps through which hackers are entering – if you don't know whether you are facing a single hacker in a basement in a foreign city or the combined power of a state intelligence agency, it's hard to know how to prepare against attack. As a result, it's essential that security directors have a comprehensive view over all their defence systems in order to identify a wide range of attack types. The best way to counter an unknown adversary is to have visibility into activity at all entry points.

Single focus

State-sponsored hackers are also often identifiable by their dedication to a specific

target. Criminal hacking is usually designed to target the largest possible number of victims in order to increase the chances that someone will click on a malicious link or mistakenly transfer money. By contrast, state hackers are more likely to have a particular high-value target in their sights and, as such, will often dedicate more time and effort to finding an entry point.

For example, the WADA breach was executed through a successful spear-phishing campaign, in which phishing emails were closely tailored to that particular organisation, containing details and inside knowledge that fool employees into believing the communications are genuine. They then open malicious documents or install malicious software. Another example of this is the so-called 'CEO scam' method, in which an email purporting to be from the company chief requests the employee make a money transfer to the attacker.

Organisations need to ensure they have strict communications policies in place in order to combat this, and educate their employees in the types of email they can expect to receive from management, and what is likely to be malicious. Caution is of paramount importance – any irregularity should be viewed with suspicion.

Covert ops

Another frequently deployed tactic is to quietly remain embedded on the network once access has been gained. For example, some malware can edit its code once installed to mask its presence, making it harder for security solutions to backtrace it and remove it. It can then gather sensitive data in secret, either extracting personal details or monitoring communications and feeding information back to the hacker. This has the added benefit of allowing the hacker to develop a long-term picture of the target organisation – its habits, regular contacts, ongoing crises and so on.

As a result, security teams need to be aware that a lack of immediate fallout after a suspicious incident does not necessarily mean that the danger is past – it may be only biding its time. For example, when Chinese hackers stole personally identifiable information from over 80 million of US healthcare provider Anthem's customers in 2015, the breakin was not discovered for some time. A covert operation can reap much larger rewards in the long run, so security teams need to keep in mind that silence doesn't necessarily indicate a lack of activity.

Successful defence

For a successful defence against such advanced adversaries, an intelligence-based, automated platform is essential. You need to be able to see what's going on across your network and be able to respond in real time to help quarantine and mitigate the threats as quickly as possible once discovered.

Orchestration gives security operations centres a leg-up, increasing the chance of a successful response. A platform can also make use of threat data from partner organisations – even competitors – to draw intelligent conclusions about the best way to handle a particular threat. If organisations enter into information-sharing agreements with others in their industries, they can input threat data into cloud-based platforms and help to generate insights based on patterns.

For example, if two organisations in a political party's digital supply chain see similar infiltration attempts through credential-harvesting phishing emails, they can improve their chances of diagnosing that activity as state-related by comparing behaviour across both networks.

At the same time, intelligence should not be separated from the human element – it should not be a question of orchestrate and retire. There should be a symbiotic relationship between the two. Actions taken off the back of automated systems' recommendations such as clean-ups, further investigations or other mitigations will beget data and information in the form of artefacts such as lists of targeted or affected assets, identified malware, network-based indicators of compromise (IOCs), newly observed attack patterns and so on. These artefacts can be refined into intelligence that can then inform decisions for future operations. While many organisations do not have a formally defined intelligence function in their team, the concept of using what you know about your threat landscape to inform your operations exists in all organisations regardless of whether or not they have threat intelligence analysts employed.

Increasing threat

State-sponsored hacking is becoming an increasingly public cyberthreat and organisations across the world need to ready themselves for the possibility of a highly targeted, stealthy attack. Many organisations are used to the idea of scattergun cybercrime, but are unprepared to meet a well-equipped and dedicated state-level attacker.

It is the duty of security operations directors to address this now, and ensure that they have complete visibility into their security posture. With hackers' tactics evolving all the time, a comprehensive and flexible threat response is a must – neither governments nor enterprises can afford to leave the back door open.

About the author

Adam Vincent is the CEO and co-founder of ThreatConnect, which provides a threat intelligence platform. He has been at the company since 2011 and was previously CTO at Layer 7 Technologies. He trained in computer science at George Washington University and holds a certificate in computer security and information assurance.

References

1. Thomson, Iain. 'Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide'. The Register, 28 Jun 2017. Accessed Aug 2017. www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.
2. 'What you need to know about the WannaCry Ransomware'. Symantec, 12 May 2017. Updated 23 May 2017. Accessed Aug 2017. www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware.
3. 'Fancy Bear'. Wikipedia. Accessed Aug 2017. https://en.wikipedia.org/wiki/Fancy_Bear.
4. Uchill, Joe. 'Prewritten Guccifer 2.0 remarks read at security conference'. The Hill, 13 Sep 2016. Accessed Aug 2017. http://thehill.com/business-a-lobbying/295670-prewritten-guccifer-20-remarks-read-by-confederate-at-security-conference.

Distributed denial of government: the Estonian Data Embassy Initiative


Nick Robinson


Prof Keith Martin

Nick Robinson, Prof Keith Martin, Royal Holloway, University of London

In an age of increasing and evolving cyber-attacks and disruption, recent events have shown that threats to critical national infrastructure and vital government services are both genuine and effective. In light of this, what measures might a government be willing to take in order to safeguard its critical infrastructure and ever-expanding 'digital ecosystem'?

One small country in the Baltics, with a recent history of dealing with such threats, may just have the answer: to 'back-up' the nation state. To protect itself from cyber-attacks (but also legitimate concerns of military occupation), the Estonian Government is planning to open 'data embassies' around the world, ensuring that the state can endure and continue to function, even outside its own borders.

Concern and anxiety

The dramatic rise in cyber-attacks, particularly those emanating from states (or state-sponsored groups), is of great concern and anxiety for many governments around the world. The recent UK National Cyber Security Strategy (2016-2021) underlined the "political, diplomatic, technological, commercial and strategic advantage" for state and non-state actors to utilise such tactics, with "government, defence, finance and telecommunications sectors" becoming primary targets for those seeking to disrupt, destabilise or exploit a potential adversary.[1]

Within an ever-changing threat landscape and against an increasingly complex and volatile geopolitical backdrop, states are having to think of new and creative ways to mitigate against emerging cyberthreats: from co-ordinated distributed denial of service (DDoS) attacks against vital organs of the state, to new forms of espionage and the onset of 'information warfare' and 'fake news'.

What happens, for example, when a targeted DDoS attack brings a state's financial sector to its knees? Or if vast troves of citizens' healthcare records are effectively wiped from existence or encrypted in a ransomware attack? The recent WannaCry ransomware virus, which crippled the UK's National Health Service, has shown that state institutions and their vital services are still vulnerable and extremely susceptible to ever-growing cyberthreats. Doomsday scenarios are often envisaged by those in the media or information security circles, but can every government be certain that its defence and mitigation strategy is up to the job?

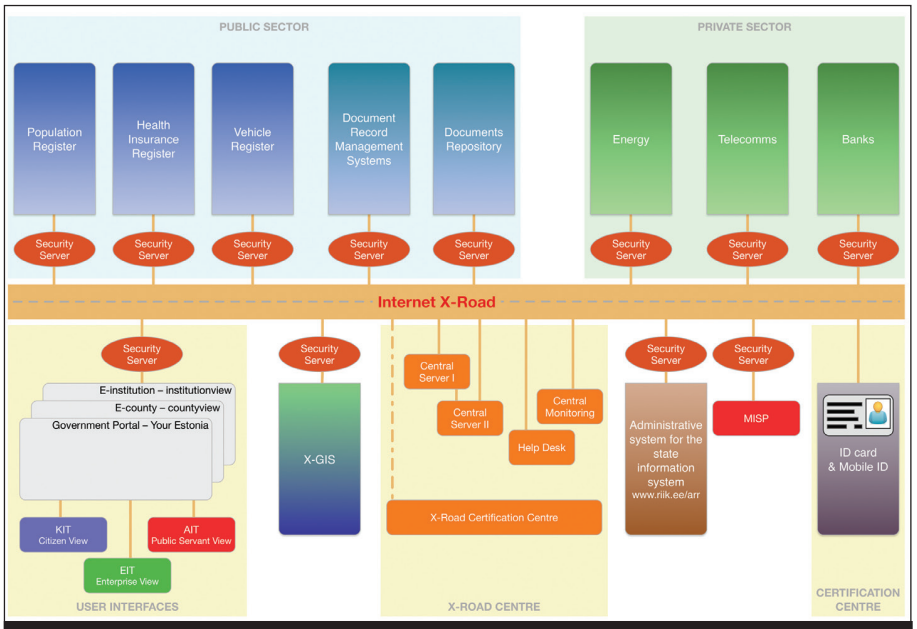
Governments around the world have increasingly utilised cloud-based services in order to improve accessibility and reduce the costs of some functions of the state. However, by virtue of redundancy and geographical distribution, cloud-based services can also be used to improve the availability and overall security of government data. Taken to extreme, just as individuals increasingly secure their personal lives (photos, documents, etc) in the cloud, a nation-state could choose to outsource to the cloud its entire digital function (land and business registries, tax and healthcare records, etc). In this way a government, even if forced into disarray or exile, could potentially continue to function from beyond its own borders. This might seem a fantastical idea, but it could soon become a reality.

e-Estonia and the X-Road

Estonia is a country that is continually trying to reimagine itself *virtually*, above and beyond its own physical limitations. Whether this is through the recent decision to store every citizens' healthcare records on an immutable, verifiable blockchain; or the rather bold attempt of amassing 10 million 'e-Residents' by 2025, Estonia's status as a digital vanguard is rarely disputed.

The journey Estonia has taken since regaining independence from a collapsing Soviet Union in 1991 has been nothing short of remarkable – and in many ways, it was this collapse and the opportunity to start again with no political legacy that was ardently seized by a youthful, forward-thinking government. The introduction of project Tiigrhüpe (Tiger Leap) in 1996 is often seen as a catalyst in this regard, as large-scale improvements in both infrastructure and education oversaw a period of enormous social, economic and political change.

A powerful post-Soviet vision emerged that recognised technology as the facilitator for streamlining cumbersome, bureaucratic government institutions and nurturing innovation, in a tiny nation



The X-Road forms the spine of Estonia's Internet-based services for both the public and private sectors.

otherwise bereft of any infrastructure or resources. A 'conveyor-belt' like period of innovation soon followed with the introduction of an eID system (2002), i-voting (2005), and e-Health (2008), offering huge benefits for the everyday Estonian with efficient, secure e-services. They soon adopted the now renowned prefix 'e-Estonia' – a visible brand and message that the Estonian government is keen to present to the rest of the world.

In Estonia today, you can vote online, tax returns are completed digitally within minutes and almost all health prescriptions are issued electronically, reducing administrative burdens on the country's health service.[2] Citizens elsewhere rarely have a one-stop shop for all of their government services: Estonia is certainly an exception to this rule. Estonians often joke that the only thing you can't do online today is get married or divorced.

All of this is kept fully functioning by, unsurprisingly, yet another Estonian creation: X-Road. Understood to be the backbone of today's e-Estonia, X-Road provides vital cryptographic services and infrastructure, enabling data to be securely exchanged between different information systems, registries and databases but also allowing all of Estonia's e-services to link up and operate in harmony across a seamless, decentralised network. Services are efficient, interoperable and – most importantly – secure.

However, the Estonian Government also recognises that many of its databases, registries and services (eg, land or population register) only exist in digital form. It is this lack of a paper trail – considering the evidential value each register or database holds – that is the cause of great anxiety for the Estonian Government. Could the Government continue to effectively function in the event of a large-scale cyber-attack? What if Estonia's territorial integrity and independence was suddenly under threat? History has taught Estonians that such eventualities are legitimate and valid.

Backing up the nation

In 2013, the Estonian Government began pursuing the Data Embassy Initiative (DEI) – an ambitious (but also timely) solution to the plausible scenario that the Government would be required to sustain its numerous digital services and functions of the state outside its own borders. Its desideratum, as outlined by the Estonian Government, is to ensure digital continuity: "The capacity of a state to maintain its services and digital data relevant for the functioning of the state, regardless of any adverse changes or interruptions".[3] This, in the case of Estonia, would ensure that the state – its numerous databases, registries and digital services – would continue to function, "even in the direst of scenarios", which, they say, includes the loss of territory.[4]

To ensure digital continuity, the DEI consists of three fundamental approaches. First – and not too dissimilar to other governments' cloud strategies – purpose-built datacentres located within Estonia's own borders will allow for improved maintenance of regular data back-ups and live services. Next, the Estonian Government will look to migrate its so-called 'digital monuments' – websites and other non-sensitive resources that hold national symbolic significance – to an international public cloud service (such as Amazon's AWS or Microsoft Azure). Resources such as the State Gazette – the online depository for all Estonian legislation since 2010 – do not hold sensitive information, but are part of the state's critical national infrastructure and could be significant targets for disruptive attackers and require full availability at all times for Estonian citizens.

The final (and perhaps most novel) step the Estonian Government is now proposing, will see the creation of a network of 'data embassies' around the world in an effort to back up its more critical and sensitive data. Located outside of Estonia's own borders, this offers an effective solution for housing backups of Estonian registers and databases, while still being under full control of the Estonian Government. In the first instance, this will involve the continued utilisation of Estonian embassy buildings in different cities around the world. Many Estonian embassies have been used this way for the past decade or so, but will now see more systematic backups as previous quarterly/twice-annual back-ups were insufficient in ensuring 'digital continuity'.

Obvious drawbacks

There are, however, obvious drawbacks to this proposal – namely the lack of technical competence within each embassy to offer support during times of emergency but also that it is patently clear that embassies are not constructed to the correct standards and data security requirements expected within a (regular) datacentre.

Because of this, the Estonian Government has proposed a supplementary solution: to procure additional datacen-

tre resources through bilateral agreements with so-called 'friendly' governments across the globe. The Estonian Government would, in effect, 'rent' server space within existing datacentres, with Estonian jurisdiction being deemed applicable within these agreed spaces. Under such an agreement, the datacentre will operate in a similar capacity to a physical embassy, where diplomatic immunities will be applicable under the Vienna Convention on Consular Relations (1963). Together, these two solutions will present a robust, distributed network of data embassies (see Figure 2) that the Estonian Government believes will not only be costly and exhaustive to attack, but also improve data security, integrity and availability of services in the event of a crisis.

On 20 Jun 2017, it was announced that the first data embassy would be located in Luxembourg after a bilateral agreement (the first of its kind) was signed by both heads of state. While the data embassy is not expected to be fully operational until 2018, the historic agreement lays out each country's necessary rights and obligations, along with 10 priority databases being chosen to be backed up in the data embassy's secret location. It may be a little while longer, however, until we see a fully operational data embassy network. Future locations remain undisclosed, while the uncertainty surrounding Brexit has stalled plans for a data embassy in London.

The team tasked with implementing this ambitious project have also admitted that certain technological and legal hurdles still need to be overcome. Decisions are yet to be made over what kind of scheme will be used for distributing the data across multiple embassies – but, as with many Estonian innovations, the Government will look towards the private sector for answers as companies such as Cybernetica and Guardtime play critical roles in the design, development and upkeep of Estonia's digital ecosystem.

From a legal perspective, questions remain over how governments should respect the integrity and sovereignty of other governments' data when stored in the cloud. Or, how to legally ensure that government data held in the cloud has immunity from being tampered with or copied. In a recent joint research report with Microsoft, it was acknowledged that minor revisions to domestic Estonian law may be required, but with no form of legal precedent as a guide and no data embassies tested under international law, further investigation as to how diplomatic and international protections can be applied is essential.

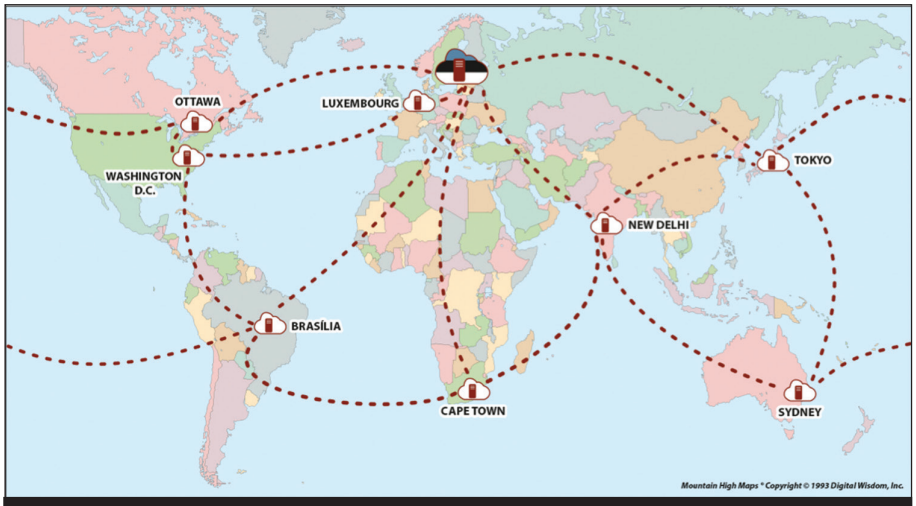


Figure 2: How a network of 'data embassies' might look when in full operation.

Distributed denial of government?

The Data Embassy Initiative may raise questions within the information security community, namely: why is any of this even necessary? Such an initiative will ultimately place a hefty financial burden upon the state, with some governments perhaps questioning whether the potential risks even outweigh the benefits. So, under what circumstances (or indeed pressures) does a government like Estonia's feel that it is imperative to utilise such a bold strategy as 'backing up' the nation-state?

Mentioned already, Estonia's reliance upon its digital ecosystem could ultimately become its own downfall. Despite its many benefits, the aforementioned 'paperless' vision of a digital society can lead to obvious vulnerabilities and weaknesses.[5] As the Government outlines, scenarios whereby "digital signatures do not work for days at a time, or the data in the Land Register is corrupted" are not acceptable in today's Estonia.[6] With the recent introduction of e-Residents into the equation, the onus is even higher on the Estonian Government to ensure that all databases, registries and services are secure and available 24/7.

The Estonian Government has also learned lessons from its own recent history. In 2007, Estonia was victim to what is widely considered to be the first instance of a state-sponsored cyber-attack (allegedly Russian-orchestrated), as its government institutions, media and news portals, banks and telecommunications infrastructure were subject to a significant DDoS attack. Although damage was minimal and 'normal service' was resumed in a matter of days, it was deemed a wake-up call not only in terms of attitudes towards cyber-security, but in asking vital questions of how (and where) its databases, registries and services should be held and secured. Around this period, a comprehensive cyber-security strategy (2008-2013) was published, while NATO strategically placed its Co-operative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.[7]

But these worries and concerns are not solely confined to the 'digital'. Another reason for building data embassies, it might be suggested, is down to a prevalent and ongoing geopolitical anxiety over the potential occupation of Estonian territory. Such concerns are not quixotic either. Estonia spent a large percentage of the 20th Century under repeated occupations from the Soviet Union (1940-1941 and 1944-1991) and Nazi Germany (1941-1944), so understandably the threat of future occupation now finds itself deeply ingrained within the Estonian psyche. The geographical proximity to the recent annexation

of Crimea in 2014, or further conflicts in Ukraine and Georgia, have arguably exacerbated such fears, while some commentators have speculated on whether Estonia (or others in the Baltics) 'might be next'.[8,9] With the question of digital continuity now firmly at the forefront of the national conversation in Estonia, the DEI might not only be seen as a necessity in a digital age, but as a stringent additional defence mechanism against an intimidating and potentially aggressive neighbour.

Trend setters?

Will the concept of data embassies ever catch on? When speaking to one official within the Estonian Government, it was made clear that Estonia should by no means be an exceptional case. Data embassies, they said, should become an "integral part of any government's cyber-security strategy in the future".

This year has so far shown us that governments are now facing a multitude of threats to both critical infrastructure and vital services, while concerns over the way in which data is collected, stored and used continue to grow. It seems unlikely that the Data Embassy Initiative will become the panacea that governments are looking for overnight. In a best-case scenario, data embassies could be extremely beneficial in providing greater reassurances over the integrity and reliability of data and government services, but in a worst-case scenario, a network of data embassies could ensure that a government could continue to function, even if forced into exile. While governments have operated from exile before now (Poland and Norway did so from London in World War II), none have benefitted from the use of the cloud. Many states – especially those without universal recognition or status – could be drawn to the notion of an extraterritorial state and infrastructure.

Granted, Estonia's circumstances are somewhat unusual, but they offer a fascinating example of a government looking to push the boundaries in terms of data and national security in the 21st Century. Estonia's lack of political legacy and its 'start-up' mentality mean that it is often open to such radical initiatives, comparative to the UK or other western governments.

Many governments have taken to experimenting with cloud computing in recent years, with the benefits of reduced costs, increased efficiency and increased scalability of digital services an obvious advantage to any state's future digital strategy. We are yet to see a government attempt such a bold strategy as 'backing up' the nation-state, but will it be long before we see a complex international network of data embassies forming around the world?

About the authors

Nick Robinson is a PhD student in the Centre for Doctoral Training (CDT) in Cyber Security at Royal Holloway, University of London. His research is primarily grounded in Estonia, with a focus on the numerous technological innovations its government has deployed since regaining of independence in 1991. Supervised by Prof Keith Martin and Prof Klaus Dodds, Robinson's thesis will be exploring the implications of the Data Embassy Initiative from both geopolitical and cyber security perspectives – from its motivations and technological challenges, to its potential efficacy in safeguarding a state's vital digital ecosystem.

Prof Keith Martin is a professor of information security and former director of the Information Security Group at Royal Holloway, University of London. He has broad research interests in cyber security, with a focus on application of cryptography and geopolitical aspects of cyber-security. He is a former associate editor for cryptography of IEEE Transactions on Information Theory. Martin has been teaching on Royal Holloway's MSc Information Security since 2000, and was a co-creator of the successful distance learning version of this programme. He is author of the book Everyday Cryptography (OUP, 2012), now in its second edition, which introduces cryptography to non-mathematical audiences. He has also presented courses on cryptography to a wide range of audiences, including specialist industrial short courses, the general public and school audiences.

References

1. 'National Cyber-security Strategy 2016 to 2021'. Cabinet Office, HM Government, 1 Nov 2016. Accessed Aug 2017. www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
2. 'e-Estonia: The Future Is Now'. Enterprise Estonia, 2015. Accessed Aug 2017. https://issuu.com/eas-estonia/docs/e-estonia_thefutureisnow.
3. 'Transforming digital continuity: Enhancing IT resilience through cloud computing'. Ministry of Economic Affairs & Communications and Microsoft, May 2016. Accessed Aug 2017. www.mkm.ee/sites/default/files/transforming_digital_continuity_-_joint_research_report_finaly_may_20.pdf.
4. 'Implementation of the Virtual Data Embassy Solution'. Ministry of Economic Affairs & Communications and Microsoft, 2015. Accessed Aug 2017. www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf.
5. Pernik, P. 'e-Residency and Data Embassies: A Country Without Borders'. European Cyber-security Journal, 2(1), 2016, pp.54-61.
6. Kotka, T; Liiv, I. 'Concept of Estonian Government Cloud and Data Embassies'. In Kő A, Francesconi E (eds). 'Electronic Government and the Information Systems Perspective'. EGOVIS 2015. Lecture Notes in Computer Science, vol 9265, 2015. Springer, Cham.
7. 'Cyber-security Strategy 2009-2013'. Ministry of Economic Affairs & Communications, Estonia, 2008. Accessed Aug 2017. www.cyberwiser.eu/estonia-ee.
8. Stuttaford, A. 'After Ukraine, are the Baltics in Putin's sights?'. Prospect Magazine, 16 Jul 2015. Accessed Aug 2017. www.prospectmagazine.co.uk/magazine/after-ukraine-are-the-baltics-in-putins-sights.
9. Trimbach, D; O'Lear, S. 'Russians in Estonia: Is Narva the next Crimea?'. Eurasian Geography and Economics, 2015, 56(5), 493-504.

Data and IP are the new nuclear: facing up to state-sponsored threats

Phil Beckett

Phil Beckett, Alvarez and Marsal

It used to be that the biggest threat a business or government faced was bad luck. Back then, power cuts, bank heists or markets not performing as expected were considered threats. In those innocent times, businesses did not need to consider the range of threats they now encounter in today's digital age. As technology and its uses have become more advanced, so have the issues businesses face on a daily, if not hourly basis. Businesses and governments have to deal with so much more – embarrassing reputational issues that will haunt them on the Internet forever, social media allowing anyone and everyone to directly voice their views and, of course, data management and security.

Data is the modern equivalent of a block of gold – it holds the key to potential great wealth and power. But it also has the pitfall that many gold-diggers have come to realise – if you have it, others will want it too. In the old days, the answer was a smash and grab: get what you want through physical brute force.

In the digital age, this is simply not possible, as stealing a server room is not feasible and, often, the threats don't come from down the street or even within the same country – they are international. Everyone wants to gain insight into competitors' knowledge, assets and intellectual property (IP), be it in business or interstate espionage, in order to beat them and take control. Money makes the world go round, specifically *how* money is made rather than actual monetary theft is of real relevance – and if that means stealing data to get valuable IP, then that's the new world we're living in.

Knowledge is power

Sixteenth century English philosopher Francis Bacon said that knowledge is power, and he is still right. Hacking and stealing IP is now commonplace, as it's one of the easiest ways to get one up on a rival. Be it states hacking states, businesses hacking businesses or a combination of the two, targeted cyber-attacks are commonplace globally. For example, NATO has said recently that the alliance is coming under an increasing number of state-sponsored cyber-attacks, while Microsoft released security updates for a platform it no longer supported, Windows XP, due to state-sponsored attacks.[1,2] No-one is safe and institutions need to become more vigilant about the threats they face.

While it's possibly understandable – although not condonable – that commercial rivals might try to steal each other's data, state-sponsored activity can sometimes be harder to pinpoint in terms of motive. While our minds might spring to a few 'usual suspects', who are known for their cyber warfare, the truth is, anyone could be – and probably is – doing it.

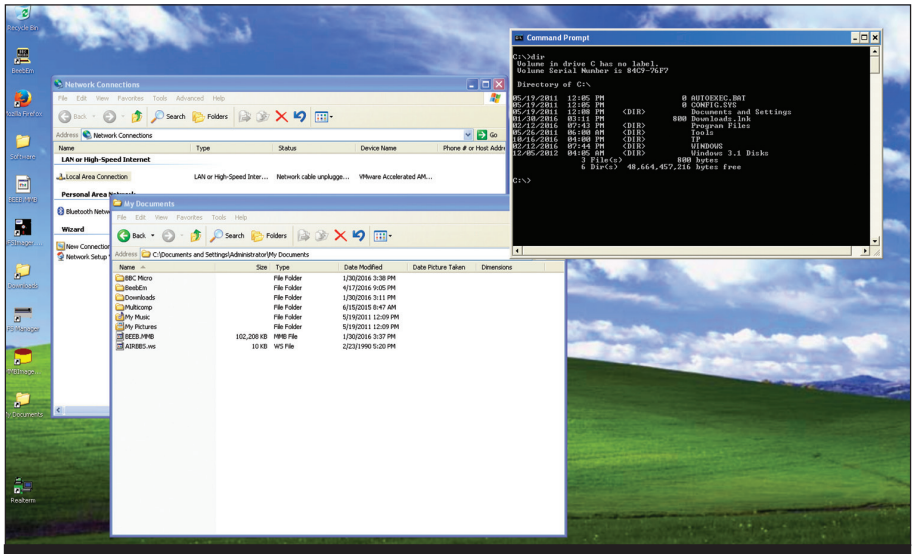
There is also a problem in the definition itself, as state-sponsored attacks will have different meanings in different continents. In the UK and other European countries, state-sponsored sounds more severe, as there is a clearer divisible line between government and business, with fewer state-owned businesses. However, elsewhere, lines are more blurred between private and state ownership and the ultimate goal is for powerful businesses that glorify the state. Therefore, state-backed initiatives are more common because they have dual benefits, not just one.

Examples of this include Nortel and Cisco. As widely reported, both were hacked by overseas competitors, with damaging consequences. Cisco lost market share to Huawei, a Chinese multinational networking and telecommunications equipment and services company, in two key markets. Meanwhile, Nortel, based in Canada, collapsed, wreaking havoc with sky-high debts, lost jobs and the loss of the country's most important tech company.

The lesson? No one is safe and protection needs to be taken seriously. Attacks are always targeted and the motives behind them can vary. Sometimes, they are in retribution, if those responsible feel it's warranted. Other times, it's simply to gather information. Attacks are being launched to gather intelligence on what companies are doing, how they are doing it and to steal their data. Often, this involves researching the target, launching an initial attack, establishing a position (to see if it's detected), navigating through the network until the gold is found, extracting the data and getting out. This isn't just over the period of a few days – depending on the complexity of the system, the attack can take years. Investigations into the APT1 hacking group showed an average stay of 356 days, with the longest being 1,764, or over four and a half years.[3,4] For long-term gain, the sophisticated attacking groups know to play a waiting game.

Mitigating the risk

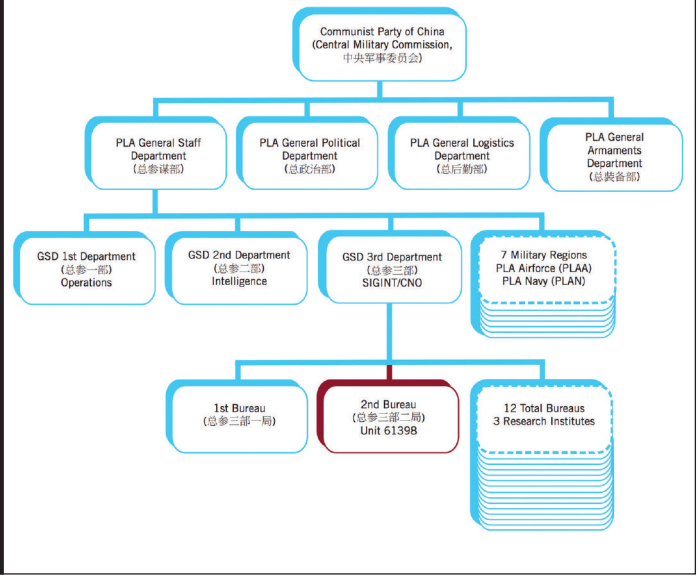
But what can governments and businesses do to mitigate their risk? The answer is it depends on who they are and where they are. Specific geographies are going to be more at risk, with the US, UK, France, Germany, China, Japan and Russia the



State-sponsored attacks prompted Microsoft to issue an update for its venerable – and long-obsolete – operating system Windows XP.

most likely to be in the firing line due to their economic power and the types of companies they do business with. Additionally, specific sectors will be of greater interest to those looking to steal information. Everyone wants to be a market leader and hold power, so industries such as tech or energy – ie, the ones who hold serious power over how we live our lives – will be a more attractive proposition from which to steal information.

That being said, whatever the sector, an attack is an attack and the response should not differ if the enterprise is publicly or privately owned. Every entity should have a cyber framework and have measures in place to mitigate the current threats associated with the business, taking into account its geographic location and industry. Just as we employ fire and burglar alarms in our houses, preventative measures should be implemented against cyber-attacks. This is not just in relation to the cyber framework, but also education, creating a security-conscious culture. People are a key line of defence and can often spot things a computer can't. For example, educating employees about phishing can help reduce the possibility of a mistake turning into a hack. By knowing what to look out for, suspicious emails may not be opened, stopping the spear-fish attack getting into the system. This is hardly rocket science, but phishing was the most common cyberthreat to UK businesses last year, with over one million attacks.[5]



The position of 'Unit 61398' – the hacking group identified in Mandiant's ground-breaking report on APT1 – with China's People's Liberation Army (PLA). This, said Mandiant, clearly showed that the attacks emanating from this group were state-sponsored. Source: Mandiant.

Perhaps the most common attack is currently the CEO fraud, in which attackers use the company CEO's email address to ask employees to send sensitive information or payments details. As previously reported, Snapchat has previously fallen foul of this, as have several German firms in recent months, showing how easy it can be to be tricked.

Outbound traffic

Another key control when dealing with the advanced threats associated with nation states is to monitor outbound network traffic. A pitfall many fall into when searching for cyberthreats is only looking at in-bound threats, as they presume nothing has already breached their defences. However, a true clue to suspicious activity is checking outbound traffic, focusing on where activity is destined to go as this can shine a light on unusual, suspicious activity such as when it is related to specific unusual locations, or occurring at unusual times or in unexpected volumes. Admittedly, this requires a knowledge of what 'normal' activity looks like, but baseline configurations of network traffic can help flag up when abnormal patterns occur.

If already under attack, then private or publicly owned institutions should follow the same course of action – their incident response plan. Internal responses will vary company by company as well as within a company based on the type and criticality of the incident, but they will include, depending on the nature of the incident, informing law enforcement, lawyers and industry regulators.

Also, it's key to remember that although the obvious answer may seem to be to pull out the cables or shut down computers, once the hackers are in, they're in. The approach taken will vary by situation (for example, if the incident is causing the generators to overheat then it's wise to shut them down). But for some, it may be best to not to take drastic action and risk losing money – it's about damage control. The ideal situation would be to try to identify who is in the system and not to alert them that you know. This is not only so you can try to bring them to justice (albeit that

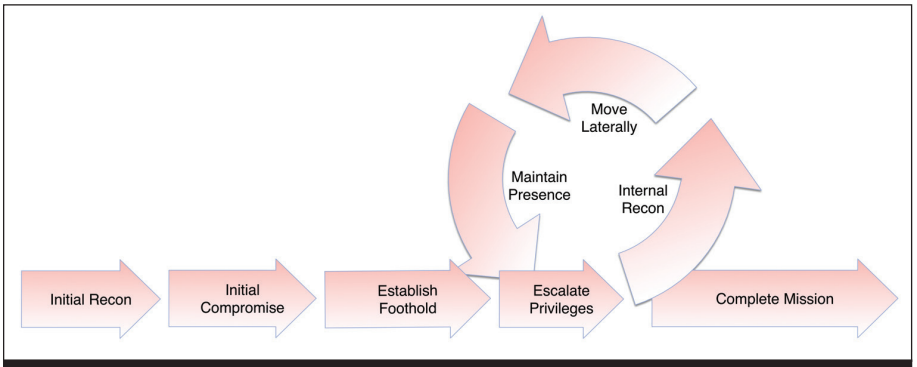
this is not a certainty), but also to show evidence of the attack before it's deleted and prevent it from becoming malicious.

Cyber-attacks are like physical ones and fight or flight can kick in – some may pull out and cover their tracks, others may wreak ultimate destruction. What is important, however, is to speak with counsel in order to establish privilege and the legalities around breach notification. Having a plan in place is vital when systems are potentially breached and it may not be possible to access the information needed. The scenario encountered will, of course, dictate the response plan, but preparing for the worst in advance can help speed recovery. Not resting on one's laurels is key here and any plans should be constantly reviewed in the light of technological advances and increased threat possibilities.

The attribution problem

Attribution is often an issue following an attack, as the natural response is to want to bring the attacker to justice. However, the most important action after a hack is to get the business or government department back on its feet. Getting emotional is not an option, it's about speedy recovery. This means taking action in advance to ensure that key data can be preserved when under threat, so valuable assets are not lost. This relates to both data you can control (such as logs and forensics) and data outside your control. Safeguarding the IP crown jewels will only help the institution in the long run.

State-sponsored or not, cyber-attacks are becoming more commonplace and we can fully expect the situation to get worse before it gets better. Plus, with increased media attention and the incoming General Data Protection Regulation (GDPR), more incidents will no doubt be reported, thus raising awareness of the ongoing threat. Hopefully, we can soon get to a point where businesses and governments are mitigating risk and sharing information as standard, so threats are harder to come by and attacks become less successful.



The attack lifecycle model, as described by Mandiant in its APT1 report.

It's inherent in human nature to want what others have and as new industries evolve, intelligence will be stolen. From the space race to being the first company to create a successful driverless car, inter-sector and international rivalry has driven and will continue to drive extreme measures, including illegal ones. Hacking is everywhere and it's undeniable that states, companies and individuals are at it, whether it's being done offensively for financial gain or competitive advantage, defensively to protect the security of a nation or neutrally where the motivation is the technological challenge or notoriety. Therefore, it's time to get ready – taking action now can help save time, money and reputation if disaster were to strike. As Winston Churchill said, "Let our advance worrying become advance thinking and planning" – take this mantra, implement it, live by it.

About the author

Phil Beckett, a managing director with Alvarez & Marsal's Disputes and Investigations practice in London, has more than 15 years experience in forensic technology engagements, advising clients on forensic investigations of digital evidence, the interrogation of complex data sets and the disclosure of electronic documents.

References

1. Petit, Harry. 'Microsoft releases Windows XP security updates as it warns of 'destructive' state-sponsored cyber-attacks'. Daily Mail, 14 Jun 2017. Accessed Aug 2017. www.dailymail.co.uk/sciencetech/article-4602964/Microsoft-warns-state-sponsored-cyber-attacks.html.
2. 'NATO sees sharp rise in state-backed cyber-attacks: Stoltenberg'. Phys.org, 19 Jan 2017. Accessed Aug 2017. https://phys.org/news/2017-01-nato-sharp-state-backed-cyber-stoltenberg.html.
3. Zetter, Kim. 'Chinese military group linked to hacks of more than 100 companies'. Wired, 19 Feb 2013. Accessed Aug 2017. www.wired.com/2013/02/chinese-army-linked-to-hacks/.
4. 'APT1: Exposing one of China's Cyber-espionage Units'. Mandiant, 2013. Accessed Aug 2017. www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.
5. Muncaster, Phil. 'Cyber-Attacks Cost UK Firms £30bn in 2016'. InfoSecurity, 1 Mar 2017. Accessed Aug 2017. www.infosecurity-magazine.com/news/cyber-attacks-cost-uk-firms-30bn/.

The Firewall

Who are the attackers?

Colin Tankard, Digital Pathways

The headlines surrounding the US Presidential Elections in 2016 often had talk of hacking and subsequent leaking of embarrassing data in an effort to discredit one or the other parties. But just who is doing this?

The finger is often pointed at Russia or China. For the Russians, while they remain committed to hacking business information that will assist their competitive standing in the world, their first priority is collecting military and diplomatic information. In comparison, the primary objective of China's cyber collection capability is to enable their state-owned enterprises to dominate on a global economic level. But are all nation-state hacks from these two players? Clearly not, as Columbian hacker Andrés Sepúlveda claims to have used a variety of 'dirty tricks' to influence elections in Nicaragua, Panama, Honduras, El Salvador, Colombia, Mexico, Costa Rica, Guatemala and Venezuela over the past 10 years.

Hacking for political gain is not new. For example, both the McCain and Obama US presidential campaigns in 2008 were compromised by hacks on their offices where sensitive data was taken and publicly used.

A worrying change to this cyber game is the masquerading as a particular country or person as a way of hiding blame or pointing it at an innocent party. This was highlighted in the recent WannaCry malware attack, where part of the code checked for the keyboard language and, if it was Russian, did not execute the WannaCry exploit. Was this really put in to protect Russian machines? Or was it to point the finger at Russia for launching the exploit?

Rumours circulate about North Korea hiding behind, or mimicking, Chinese hacking groups, in order to release malware targeted at national resources in the US. This keeps the North Koreans in the clear by putting the spotlight on China as the bad guys.

The common thread of so-called nation-state attacks is that they deploy sophisticated malware tools to achieve their objectives. In many cases, the common element of the attack is the exploitation of the human element within an organisation. This attack vector has also increased in complexity. For example, the use of social media profiling has greatly increased, which enables the attacker to focus on individuals – cyber 'snipers' so to speak. This makes the content of the malware very relevant to the target, thus greatly increasing the chance of the victim opening a document and launching the exploit. It is not just the ones and zeros of an attack that are sophisticated, it is also the development of exploitations of other weak points within an enterprise.

However, with all the talk of cyber hacks against a nation's infrastructure and with most countries setting up national cyber protection agencies such as the UK's National Cyber Security Centre, it is easy for commercial organisations to think these agencies will protect them. But criminal groups are adopting the same tools and techniques as state-influenced hacking teams, shrinking the gap between deployment by a nation state and deployment by a criminal group, in terms of time and quality, leaving commercial organisations very vulnerable.

It is time to stop thinking that all cyber-attacks are committed by a few nation state-backed groups. It should be remembered that most data has a value to someone and ultimately a monetary one. The cyber villains may just be pawns in a complex game of cyber chess and may not necessarily be after the 'king'. In fact, they may be playing by very different rules, where other pieces on the chessboard are even more valuable to them.

EVENTS CALENDAR

1–4 October 2017
High Technology Crime Investigation Association Conference
Anaheim, CA, US
http://bit.ly/2eADgIs

2–6 October 2017
BruCON
Ghent, Belgium
http://2017.brucon.org

2–4 October 2017
ISACA CSX North America
Washington, DC, US
www.isaca.org/cyber-conference/

4–5 October 2017
InfoSecurity North America
Boston, MA, US
www.infosecuritynorthamerica.com

9–10 October 2017
Hacker Halted USA
Atlanta, Georgia
www.hackerhalted.com

9–11 October 2017
ISSA International Conference
San Diego, CA, US
www.issa.org/?issaconf_home

18 October 2017
Cyber Security EU
Leeds, UK
www.cybersecurityeurope.com

30 October – 1 November 2017
ISACA CSX Europe
London, UK
www.isaca.org/cyber-conference/csx-europe.html

31 October – 4 November 2017
Hackfest 2017
Quebec, Canada
http://hackfest.ca