5 June 2018

What to Do When Your Hacker Is a Nation State?

Ryan Johnson, Senior Manager, International Public Policy

Companies have learned to deal with cyber criminals going after their data, whether sophisticated transnational crime syndicates or the "somebody sitting on their bed that weighs 400 pounds." But what about when a powerful nation-state decides to attack a company's systems?

Last week, the House Foreign Affairs Committee introduced the "Cyber Deterrence and Response Act." If the bill is passed by Congress, the White House will designate several foreign governments[1] and non-state actors as "critical cyber threat actors" to US national security, economic or financial stability, and critical infrastructure. The president will be able to raise sanctions on these actors, giving the government economic leverage to deter foreign cyber criminals from attacking American infrastructure. Naming and shaming has worked in the past, particularly in regards to state sponsors of terrorism. This will also inevitably lead to significant lobbying on behalf of industry and the attacker nations to include or exclude names on the list, which will quickly become politicised.

For the private sector, the spectre of nation-state-based attacks continues to grow. Industry controls the vast majority of critical infrastructure (above 90% in Western countries) and is therefore likely to see state attacks on its networks, despite being a civilian target. Governments are increasingly reliant on cyber means to acquire intellectual property. As trust in global business remains relatively low following the Snowden revelations in 2013, some states have turned to complex cyber espionage campaigns to verify information provided by businesses.

The 2015 UN Group of Governmental Experts (UNGGE) had a lot to say about what form of behaviours might be acceptable for states, encouraging the protection of critical infrastructure by states, pushing for the sharing of information, and providing assistance between states when critical infrastructure is under attack. While this is a good start, the application of these norms to practical measures is still in its infancy. Access Partnership, leading a group of industry players, partnered with the Singaporean Cyber Security Agency in 2017 to help promote the adoption of norms in South East Asia. The adoption of these norms is not a priority in many regions.

Attribution remains a stubborn problem. Microsoft's proposed Digital Geneva Convention relies on an international body of trust to determine the culprits behind major attacks. Such a body would have to work hard to gain international trust and prove its neutrality. International action may be slow to materialise but could help reduce nation state attacks.

But who is to blame when nation-state tools get released in the wild, as happened in the Shadow Brokers case? In this case, dozens of US National Security Agency (NSA) tools were stolen and made available to the global hacker community, including the impactful WannaCry ransomware tools. These tools included dozens of so-called zero-day exploits (vulnerabilities in IT systems that are neither known nor acknowledged by the manufacturer and for which no patch exists). Military-grade weapons built by super spies ended up in the hands of common crooks.

[1] The bill names Iran, China, the Democratic People's Republic of Korea, and Russia as explicit threats.

Access Partnership Ltd
9th Floor, Southside
105 Victoria Street
London SW1E 6QT
United Kingdom

Tel : +44 (0) 20 3143 4900
Fax: +44 (0) 20 8748 8572
www.accesspartnership.com

In some cases, these tools were known to manufacturers, which chose not to address them out of support for national security. The collaborative attitude from the private-sector is rapidly changing in favour of user security.

A response from industry has been a pledge to protect consumers and not aid the offensive cyber attackers who exploit private-sector products. The Cybersecurity Tech Accord, which now has over 40 major international IT providers as signatories, is a promise to consumers that industry is committed to providing trustworthy products. But that's only one part of the equation: what should a company do when a nation-state actor attacks them? From our experience in helping victims of attacks understand their government outreach options, and years of working with global IT companies, we have identified the following optimal practices that can make the difference, whether your company is hit by common crooks or super spies:

1) Have your defensive team on speed dial:

A company that suffers an attack will ultimately need help from outsiders, such as law enforcement, homeland security, cybersecurity insurance providers, incident response and digital forensics firms, and outside legal counsel. Your moment of crisis should not be the first time you call these important members of your defence and recovery strategy. If the local FBI agent knows your business and understands what the company does, that agent can help flag pertinent information about attacks targeting your sector. If your cyber insurance provider knows your company's specific risks and you've built points of contact within them, you can speed up the claims and recovery process after a successful attack.

2) Know your game plan:

As we mentioned above, defence and recovery are a team sport, and, like any other team sport, practicing the plays in your playbook will make the difference between a smooth recovery and uncoordinated action. An important step in building a game plan, which companies all too often neglect, is to write it down and rehearse it (while we're at it, print it out in case you get locked out of all your IT systems at once). By going through the scenarios, you will learn the proper reaction to adopt given the nature of the attack. For example: will you hack back? (we think there's lots of reasons you shouldn't, but in some circumstances, this may be a viable option.) At what point in the process will you go public with the nature and impact of an attack? Will your company pay to remove ransomware from its systems? (The FBI does not encourage you to do so, and neither do we.)

3) Drill baby, drill:

Having a game plan is one thing. Testing it out, finding its weaknesses and fixing them is another. As Latin writer Publilius Syrus said it, "Practice is the best of all instructors." Once you're satisfied that the game plan provides a reaction capacity for your organisation, testing it out and continually refining it is the single best thing your company can do to reduce the impact of a cyberattack. In-house rehearsals for little cost through table-top exercises will break down silos and build confidence in the game plan across the organisation. For example, a scenario where your accounts payable team is asked to walk through the steps of responding to evidence of a hack into the company's sensitive financial data will help them understand the nature of the threat far better than reading technical reports meant for the IT department.

At a certain point, however, most organisations hire external resources to test their capabilities. This may take the form of penetration testers (technical professionals hired to probe the IT systems of an organisation) or a more thorough red-team attack. A red team attack is one in which attackers hired by

the organisation conduct a variety of attacks against it, including non-technical attacks like social engineering. Such a program is designed to test facets of the organisation's defences and response plans.

4) Sharing is caring:

Modern cyber attackers share tactics, techniques, and procedures. They have outsourced various parts of the cybercrime functions to specialists, increasing the quality and speed of their attacks. It no longer makes sense for organisations to attempt to protect themselves in isolation. Sharing information via government-led automated indicator exchanges like the CISA program in the US, or in an industry association like the sector-specific Information Sharing and Analysis Centers (ISACs), and building lines of communication with other defenders via groups like FIRST. By plugging in to information sharing groups, companies increase their own resilience and their overall industry ecosystem, making attacks less lucrative and reducing the economic incentives for attackers to ply their trade.

5) Support the adoption of norms in cyberspace:

Prosecuting criminal hackers is difficult, since they live in the shadows online and operate across borders, often from areas with no domestic law on cyber-attacks. Cross-border judicial cooperation to combat these hackers is difficult; for nation-state hackers, prosecution even rarer. The current US administration has shown considerable resolve in naming and shaming government cyber actors, but concrete legal action rarely materialises.

One resource available between states is the continued growth of norms for responsible state behaviour in cyberspace. The initial list of norms promulgated in 2015 has grown (in the report of the UN Group of Governmental Experts or UNGGE, and now includes work by the Global Commission on Stability in Cyberspace and private-sector actors like Microsoft.

While the norms for state behaviour continue to percolate, there remains significant work to be done in implementing the norms and understanding how the principles apply in real world situations. Much of this work will be done by governments, but the private-sector can help by sharing its expertise and advising governments about the situations they face as the owners and operators of most of the world's Internet infrastructure.

At Access Partnership, we've begun work in conjunction with industry partners and governments to foster the adoption of the 2015 UNGGE norms in the Southeast Asian context. Through our Coalition for Cybersecurity in the Asia Pacific (CCAPAC), we are building stronger ties between the governments in the region and global industry, aimed at securing the digital economy that is driving the region's growth. Throughout 2018 and going forward, we will continue to drive the discussion about the application and adoption of norms by the region's actors to reduce the likelihood of nation-state attacks.

About Access Partnership

Access Partnership is the world's leading public policy firm for the tech sector. We monitor and analyse global trends for the risks and opportunities they create for technology businesses and identify strategies to mitigate those risks and drive the opportunities to our clients' advantage. Our team uniquely mixes policy and technical expertise to optimise outcomes for companies operating at the intersection of technology, data and connectivity.

www.accesspartnership.com
@AccessAlerts