'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