HOW NATION-STATE ACTORS CAN UNDERMINE YOUR ORGANIZATION

What is a nation-state actor?

A nation-state actor is a government-sponsored group that forcefully targets and gains illicit access into the networks of other governments or industry groups with the intention to steal, damage, and/or change information.[1]

Nation-state actors often operate as though they maintain a 'license to hack'. They may participate in underground 'cyber armies' or 'hackers for hire' that operate within the interests of specific geopolitical environments.

Nation-state actors distinguish themselves from regular hackers in that they're uniquely persistent, and have a 'stop-at-nothing' mentality. They're are aware of the destruction that they're precipitating.

That said, some may not recognize some of the downstream or "domino" effects that can occur when targeting interconnected infrastructure. While a victim's system breach may be intentional, a third-party breach may not be.

Motives:

Nation-state actors are ultimately motivated by a sense of allegiance to their geographic locale. The governments supporting nation-state actors range in terms of interests; some seek corporate sabotage, some desire financial gain, others maintain interests in espionage, while others yet wish to advance specific political agendas. The latter is particularly common in regions that are prone to conflict.

In North America, 36% of cyber attacks were attributed to nation-state actors in 2019.

Given our interconnected online environments, sophisticated nation-state attacks represent a serious and credible threat. In 2019, in North America, 36% of cyber attacks were attributed to nation-state actors.[2] In 2020, a hack into the IT firm known as SolarWinds is thought to have emanated from a nation-state backed group.[3]

Is there a cyber arms race among nations and nation-states?

Whether or not a cyber arms race is under way remains an open question. An academic study produced by Cardiff University finds that state leaders have indeed induced a cyber arms race. Mathematical modeling points to state increases in spending and actions in response to those of other nation-states. However, the researchers posit that determining precisely how to measure a state's military build-up requires new evaluative methodologies.

"Cyber weapons are essentially 'computer codes' used to inflict meaning, that unlike [in] the physical domain the virtual nature of malware makes it very difficult for states to gain an accurate picture of one another's capabilities," or for researchers to gain similar insights.[4]

[1] Geopolitical Cyber Security: Nation-state Actors and How to Prevent a Breach, Cyber Talk, February 9th, 2021

[2] Concerned about Nation State Cyberattacks? Here's how to Protect Your Organization, Security Magazine, March 26, 2020

[3] The Nation State Threat to Business, Kate O'Flaherty, Computer Weekly, January 8, 2021

[4] Conceptualizing Cyber Arms Races, Anthony Craig and Dr. Brandon Valeriano, NATO CCD COE Publications, Tallin, 2016

Nation-state actors, attacks

According to a study that investigated over 200 cyber security incidents attributed to nation-state hackers across 11 years, researchers identified escalating tensions among participants in the cyber criminal economy. A “worrying escalation” of tensions was observed during 2020, as the coronavirus pandemic expanded opportunities for nation-states to exploit.

“Attempts to obtain IP data on vaccines and attacks against software supply chains demonstrate the lengths to which nation states are prepared to go to achieve their strategic goals,” says the University of Surrey’s Mike McGuire.[5]

And the fact that computer system patching, scaling and upgrades were often delayed due to new remote working patterns and staffing changes only encouraged hackers to advance their pursuits.

How else are nation-state actor attacking?

Nation-state attackers may leverage assorted sophisticated techniques. These include the use of proxy layers, the avoidance of attribution through the manipulation of data, and the use of novel toolkits and other tactics to divert the attention of forensics teams. These attack methods are extremely concerning, as they can potentially result lost business capabilities and/or in lost lives.

And right now, cyber weapons developed by government agencies are appearing on the black market. These include the infamous EternalBlue exploit deployed in the WannaCry attacks.

The regulatory environment?

In the US, in 2019, a Bureau of Cyberspace Security and Emerging Technologies was proposed. Its objectives would center around forging new cyber agreements. As of early 2021, the Bureau remains in a conceptual stage. Says the Biden administration regarding emerging technologies, “[they] remain largely ungoverned by laws or norms designed to center rights and democratic values…”[6]

In 2020, the European Leadership Network (ELN) produced a pan-European proposal for controlling cyber arms. “…the cupboard remains bare when it comes to outlining any significant and long-lasting successes”, said the ELN in reference to proposals.[7]

Pillars of the Nuclear Non-proliferation Treaty and the Strategic Arms Reduction Treaty will likely retain “limited applicability” in relation to the cyber realm. Cyber arms control requires ‘out of the box’ thinking, as cheating the system would be notably easier than with nuclear arms.

And unlike bombs or physical weaponry, multiple individuals or nations can often leverage the same cyber capability simultaneously. They’re dual-use systems.

Further, cyber warfare technologies differ from traditional weapons in that they’re continually changing and evolving. For example, an increasing number of cyber weapons include artificial intelligence (AI) mechanisms. One interesting form of AI-based cyber weaponry includes the ‘boomerang’ malware, which is off-the-shelf malware that suddenly turns against its operators. Is that a government-made weapon designed to target other nation-state actors? It’s unclear.

[5] Nation-state Cyber Attacks Double Every Three Years, Alex Scroxton, Computer Weekly, April 8, 2021

[6] State Reviews Plans for New Tech Bureau, Shannon Bugos, Arms Control Association, April 2021

[7] What Does Cyber Arms Control Look Like? Four Principles for Managing Cyber Risk, European Leadership Network, Andrew Futter, June 2020

The future:

Our infrastructure is vulnerable. "We have to stop leaving gaping holes in software that could be used by adversaries to pull off some of these attacks," says renowned cyber security reporter, Nicole Perlroth. Composing perfect code may be an impossible ask. In the interim, security and mitigation strategies are must-haves.[8]

Livelihoods and enterprise survival are at stake. Lives may be on the line too. It's time to take action.

Cyber security recommendations:

There are no easy answers. Organizations must maintain vigilance when it comes to thwarting cyber attacks, including adversarial nation-state threats. Tactics that can backstop existing security measures include isolating internal networks from the internet, sharing cyber threat intelligence with public and private sector groups, and enhancing cyber security training programs. But some enterprises may not survive state-sponsored cyber attacks...

Robust planning and the right cyber security architecture are key. Ensure that your organization can prevent, respond to, and easily recover from unexpected nation-state threats.

[8] Inside the Cyber Weapons Arms Race, National Public Radio, February 10, 2021

*Disclaimer: This content does not and is not intended to replace federal, legal, or professional advice. This document is for general informational purposes only.