What Are Nation-State Attacks?

Nation-state attacks are sophisticated cyberthreats from adversaries working directly or indirectly for their own government. Their motivation? To place their nation in a better position against their political enemies.

Nation-state attackers target governments and businesses to steal sensitive information, disrupt enemy capabilities, grow financial power through cryptocurrency, or even sway the international balance of hard or soft power. The targets of nation-state attacks range from private hospitals and financial institutions to election infrastructures. As indicated by our Global Threat Report series, the reach and impact of these attacks are growing exponentially every year.

Because of the resources and prestige granted to nation-state actors for their attacks against high-value targets, the damage these threats can cause is extremely high. In fact, Carbon Black expert Eric O’Neill declares nation-state attacks to be the largest global security threat today.
Over the past two decades, Russia, China, North Korea, and Iran have all made massive investments in cyberespionage and the tools needed to launch disruptive and destructive cyberattacks against the critical infrastructure of rival nations.

– Eric O’Neill
National Security Strategist, VMware Carbon Black
How Do They Work?

The term “nation-state actor” only describes a category of attacker, not the means of the threat itself. A nation-state actor can use any of the attacks in our Threats on the Rise series, from spear phishing to ransomware. Additionally, these attackers are being trained in countermeasures against their targets’ defenses.

However, the methods of these attackers can extend offline into the realm of social engineering and offline spycraft. Nation-state attacks are Advanced Persistent Threats (APT), with a lifespan of five years or more. By manipulating the humans behind the computer, a nation-state attack can remain undetected for extended periods of time. The result is long-term exploitation, disruption, IP theft, and other damaging activities that can cause the targeted organization to lose trust in the public eye.
How Carbon Black Combats Nation-State Threats

The answer to combating nation-state threats lies in the problem itself; gaining awareness. We know that nation-state threats have a tendency to go “low and slow,” maintaining a light footprint in their victims’ environments for as long as possible to advance their campaign. However, even the lightest footprint will leave a trace, and that is where solutions like Carbon Black can help.

Carbon Black prioritizes visibility first. The endpoint data that we collect is continuous, so as to identify any possible suspicious or malicious activity being exhibited by any process, at any time. The raw data that we collect is overlaid with behavioral analytics, which allows us to identify attacker behaviors and patterns over time.
For example, let’s say that a nation-state campaign began with a targeted phishing attack on your organization’s HR department by attaching a PDF advertising a new piece of recruiting software containing an embedded macro within. The attacker is hoping for a couple of downloads that will launch the embedded macro and begin screen-recording all activity, continuously sending that data back to their command and control server. Carbon Black will monitor each step of that process, applying behavioral tags to indicate that a PDF is executing an embedded script that is making international network connections, and escalate this activity into an alert, allowing for your team to hop in proactively and address the situation early on.

TO LEARN MORE AND SEE HOW YOU CAN COMBAT THREATS IN YOUR ENVIRONMENT, VISIT CARBONBLACK.COM/PSC-DEMO