What are State Sponsored Cyber Attacks? - Detailed Guide

By SentinelOne

Published: 2023-08-16 · Archived: 2026-04-02 10:39:22 UTC

The rise of nation-state cyber attacks has become a defining feature of modern geopolitics. With blurred lines between advanced persistent threats (APTs) and cybercrime, understanding this complex landscape has become a critical element in building a strong cybersecurity strategy. According to recent reports on the rise of state-sponsored cyber attacks, nation-state actors targeting critical infrastructures have doubled from 20% to 40% in the past two years alone. As for the costs? Organizations are estimating a total of $1.6 million per cyber incident.

Not only is the frequency and financial consequences of such attacks accelerating, the threat landscape in which these nation-state actors now operate is also shifting. Cyber warfare and the use of cyberweapons in the ongoing Russo-Ukrainian war, for example, have magnified the intersection of conflict across geopolitical and digital surfaces.

The challenge is that nation-state threat actors are well-funded and possess specialized skills, focusing their attacks on high-value targets including government and military entities, think tanks, universities, and those providing critical infrastructure services.

This post explores how nation-state sponsored attacks have evolved over recent years to become a threat not just to individual targets but to all organizations, as well as to the civil, economic and political fabric of our society. Sharing our collective knowledge on how such groups operate and the impacts they have can help the cyber defense community better understand and mitigate these sophisticated threats.

A Shadowy Threat | A Brief History of Cyber Espionage & Nation-State Attacks

Cyber espionage, a stealthy practice dating back to the very beginnings of internet connectivity, has undergone substantial changes in recent years, fueled by rapid advancements in technology and evolving global dynamics.

The origins of cyber espionage trace back to the 1980s when the French intelligence agency, led by the "Farewell Dossier", exploited a KGB officer's computer to gather critical information on Soviet activities. At the same time, a German hacker group known as the Chaos Computer Club exposed vulnerabilities in government and military systems. These incidents marked the inception of digital espionage and highlighted the potential of exploiting interconnected networks to gather intelligence. These early instances foreshadowed the evolution of cyber espionage into a formidable global concern in the decades that followed.

Cyber espionage has since evolved into a potent tool for nation-state threat actors and a critical security issue for organizations, with implications sounding across political, economic, and societal domains.

Subsequently, state-sponsored hacking campaigns, corporate espionage, and intellectual property (IP) theft have become rampant, with the potential to disrupt critical service industries and compromise national security. The interconnected nature of the modern world amplifies this impact as a breach in one corner of the globe can trigger far-reaching consequences.

As nations, corporations, and civilians have become increasingly reliant on digital infrastructure, the stakes have escalated, making targeted, state-sponsored cyber attacks a top-tier and global security concern. To safeguard against this escalating threat, international cooperation, robust cybersecurity measures, and innovative defense strategies are crucial in this new era of digital spycraft.

The Big Players | Navigating The Complex Landscape of APTs

By some estimates, there could be over a hundred different APT groups worldwide, but when we look at where most activity that threatens our interests originates from, there are four major nation-states that have been in the game longer than the rest.

Between them, China, Russia, North Korea and Iran have developed some of the most sophisticated and comprehensive threat activity and cyber tradecraft that businesses in all sectors have to face today.

China

China's cyber threat is not only broad and persistent but also evolving. The Office of the Director of National Intelligence's 2023 Annual Threat Assessment paints a clear picture of the cyber threat posed by the People's Republic of China (PRC), noting that:

"China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."

The annual report contains a stark warning.

"China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems."

Emerging in the early 2000s, Chinese-based threat groups rapidly matured in terms of tactics, techniques, and targets. The infamous Titan Rain campaign of the mid-2000s marked a watershed moment, exposing China's cyber capabilities as it targeted U.S. defense and technology sectors. This trend continued with APT1, linked to the Chinese military, launching widespread attacks on various industries.

As time progressed, the Chinese cyber espionage ecosystem diversified. From 2006 to the present day, APT10 (*aka* Red Apollo/Stone Panda) has been reported targeting a wide-range of companies across multiple continents, including healthcare, defense, aerospace and government sectors. APT17 (DeputyDog) is a threat group sponsored by the Jinan bureau of the Chinese Ministry of State Security. First seen in 2009, it was attributed for the Operation Aurora and CCleaner supply chain attacks in 2017. APT41 (*aka* Winnti Group) was first seen in 2012 and combines financially-motivated cybercrime with information theft and espionage.

In general, Chinese APT groups have been known to use tactics like living-off-the-land (LOTL), where they abuse native tools like PowerShell and WMI to evade detection, and to develop comprehensive programs for vulnerability research and exploitation.

Most recently, Chinese threat groups are known to be disguising traffic to malicious servers through botnets of compromised IoT devices and to use DNS, HTTP and TCP/IP hijacking. Security researchers have found that Chinese threat groups tend to focus on security, networking and virtualization tools to obtain and maintain stealthy access to targeted organizations' internal networks.

Some notable recent case studies of Chinese-based APT groups and campaigns include:

- Aoqin Dragon – Operating since 2013, Aoqin Dragon targets government, education, and telecommunication organizations in Southeast Asia and Australia. Their tactics include document exploits and fake removable devices. They seek initial access through document exploits and use techniques like DLL hijacking and DNS tunneling to evade detection.
- WIP19 Espionage – This Chinese-speaking threat group has been targeting telecommunications and IT service providers in the Middle East and Asia, using stolen certificates to sign novel malware such as SQLMaggie and ScreenCap.
- Operation Tainted Love – An evolution of tooling associated with Operation Soft Cell, Chinese cyber espionage groups attacked telecommunication providers in the Middle East using well-maintained, versioned credential theft capability and a new dropper mechanism.

Russia

In the late 2000s, the notorious APT28 (Sofacy) and APT29 (NobleBaron, The Dukes) threat groups gained notoriety for their state-sponsored activities such as targeting government agencies, think tanks, and critical infrastructures worldwide. These groups have since been implicated in high-profile incidents, including mass supply chain attacks and interference in U.S. presidential elections. The U.S. government has noted that such activity is an extension of Russia's larger geopolitical goals.

"Moscow has conducted influence operations against U.S. elections for decades, including as recently as the U.S. midterm elections in 2022. It will try to strengthen ties to U.S. persons in the media and politics in hopes of developing vectors for future influence operations."

The Russian APT landscape evolved with groups like Turla, whose history of activity has been suggested to span almost 30 years, beginning with Moonlight Maze in 1996. Later, APT28 (linked to Russia's GRU military intelligence unit) and APT29 (now understood to be operated under the auspices of Russia's Foreign Intelligence Service, SVR) continued their activities, adapting their tactics and diversifying their targets to encompass sectors beyond politics. APT groups like Gamaredon and Sandworm have also emerged, exhibiting a blend of cyber espionage and disruptive operations.

As geopolitical tensions continue to heighten, Russian APT groups have become increasingly adept at utilizing supply chain attacks, zero-day exploits, and deception techniques. They have also exploited global events, such as the COVID-19 pandemic, to launch tailored and themed attacks.

Presently, Russian-based APT groups continue to engage in a broad spectrum of cyber operations, spanning espionage, disinformation, and potential sabotage. Russia's focus on targeting critical infrastructure, including underwater cables and industrial control systems, has been noted in intelligence assessments.

"Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."

Some notable case studies of Russian APT groups and campaigns include:

- HermeticWiper Malware – This destructive malware was used against Ukrainian organizations, manipulating the MBR to cause boot failure. This attack reflects Russia's willingness to deploy destructive tools against neighboring countries.
- APT28 (Sofacy) – Known for its espionage and influence capabilities, APT28 has been particularly focused on targeting critical infrastructure, including underwater cables and industrial control systems in the U.S. and allied countries through the use of malware like X-Agent.
- APT29 (Nobelium/NobleBaron) – Involved in the 2014 White House attack, this group has targeted various government, military, energy, and media organizations, using tools like CozyDuke. In 2021, the group was attributed with being behind the Solarwinds supply chain attack.
- Snake Implant – A sophisticated cyber espionage tool created and deployed by Russia's Federal Security Service, FSB. Found in over 50 countries including the U.S., Snake malware is used to collect sensitive intelligence from high priority targets.

North Korea

North Korea's cyber program poses a sophisticated threat, adapting to global trends in cybercrime as a whole. Their journey began in the early 2000s with the Lazarus group, which has operated since 2009 and is responsible for some of the most notorious cyberattacks in history, including the 2014 hack on Sony Pictures and the 2017 outbreak of WannaCry. They added stealing cryptocurrency to their bow in 2017. At the end of 2019, SentinelLabs

connected the Lazarus and TrickBot groups, showing how the DPRK was extending to collaborate with cybercrime groups and take over funds to support their government.

Lazarus and its subgroups like BlueNoroff, APT38 and Andariel (Silent Chollima), continue to evolve, demonstrating a growing sophistication in their tactics and techniques. They have expanded their target scope beyond high-profile attacks to include financial institutions, cryptocurrency exchanges, and global infrastructure. BlueNoroff, in particular, has become notorious for conducting large-scale heists to fund the regime's activities, with attacks on ATMs and banks using the SWIFT messaging system.

In recent years, North Korean APT groups have further diversified, with increasing focus on supply chain attacks, cryptocurrency theft, and the exploitation of zero-day vulnerabilities. The evolution of North Korean APTs highlights their adaptability and the intertwining of cyber operations with broader geopolitical strategies.

Other North Korean subgroups include ScarCruft (*aka* Inky Squid, APT37, or Group123) and Kimsuky. Some recent case studies of North Korean-based APT groups and campaigns include:

- ScarCruft & Lazarus Group – SentinelLabs identified a North Korean intrusion into a Russian missile engineering organization, NPO Mashinostroyeniya. This case involved two instances of compromise, including the use of a Windows backdoor dubbed OpenCarrot.
- Kimsuky's Reconnaissance Capabilities – Utilizing a new malware component called ReconShark, North Korean APT Kimsuky has targeted organizations across Asia, North America, and Europe.
- JumpCloud Intrusion – This intrusion into the cloud-based IT management service JumpCloud is linked to North Korean APT activity, showcasing the DPRK's focus on supply chain targeting.

Iran

Iran-based APT groups have steadily gained prominence in the realm of cyber espionage. Their beginnings date back to the late 2000s, when groups like APT33 (Elfin) and APT34 (OilRig) first emerged onto the scene. These early campaigns were characterized by targeting foreign governments, critical infrastructure, and regional rivals such as the Shamoon wiper attacks of 2012 conducted against Saudi Aramco and Rasgas.

As the years progressed, Iranian APT groups increased in sophistication and breadth. APT34, for instance, diversified its focus to include industrial espionage, particularly targeting sectors like energy and telecommunications. The group's activities revealed Iran's intent to bolster its domestic industries and capabilities. MuddyWater (aka TA450) likely began its earliest operations around 2017 with a focus on espionage attacks on Middle Eastern targets initially but later expanding to Belarus, Turkey and Ukraine.

In a geopolitical context, tensions spurred Iran-based APT groups to engage in more aggressive and disruptive activities. APT33, in particular, was implicated in destructive attacks against targets in the Middle East and beyond. The emergence of APT35 (Charming Kitten), for instance, signaled a shift towards influence operations and spear phishing campaigns against political dissidents, journalists, and human rights organizations.

Iranian APT groups have showcased their adaptability by incorporating innovative tactics such as domain spoofing, social engineering, and leveraging cloud infrastructure for command and control. This agility has

enabled them to effectively navigate the evolving cybersecurity landscape and continue their operations despite international scrutiny.

Today, Iran-based APT groups remain a significant player in the world of cyber espionage, with growing expertise and a willingness to conduct aggressive cyber operations. Recent Iranian state-sponsored activities include destructive malware and ransomware operations.

Some notable recent case studies of Iranian-based APT groups and campaigns include:

- APT33 – Known for destructive malware and ransomware operations on the aerospace and energy sectors, this group has used tools like DropShot to conduct campaigns against organizations in Saudi Arabia and the U.S., in particular.
- TunnelVision – An Iranian-aligned threat actor operating in the Middle-East and the U.S. using timely-exploitation of recent vulnerabilities such as Log4j and ProxyShell.
- MuddyWater – Uses a suite of open-source malware and DNS Tunneling to conduct espionage and other malicious activity. Believed to be sponsored by the Iranian Ministry of Intelligence (MOIS).

Counting the Cost | The Widespread Impact of State-Sponsored Cyber Attacks

Nation-states, driven by political agendas, have harnessed cyber espionage as a powerful tool to gather intelligence, influence events, and undermine rivals. This has led to a heightened sense of vulnerability among nations and catalyzed international tensions. Cyber attacks sponsored by nation states have had a profound impact across various aspects of global security, economy, and geopolitics.

Industry & Sector-Specific Impacts

Over the years, there have been many reported cases of government agencies, energy grids, financial institutions, and healthcare systems falling prey to targeted attacks, jeopardizing both economic stability and public safety. Some examples include:

- Healthcare – North Korean ransomware campaigns against healthcare organizations during the COVID-19 pandemic underscore the willingness of nation-state actors to target essential services.
- Telecommunications – Chinese APTs targeting telecom providers in the Middle East and Asia reveal a strategic interest in monitoring communications and gathering intelligence.
- Defense – The compromise of Russian defense companies by North Korean actors illustrates the global reach and strategic focus of state-sponsored cyber espionage.

Economic Impacts

Cyber espionage's impact on the global economy has redefined the dynamics of trade, innovation, and security. Businesses lose billions annually when intellectual property is compromised and the increasing number of supply chain attacks disrupt manufacturing and distribution networks to an alarming degree.

- Financial Losses – Cyber espionage activities have led to billions of dollars in financial losses.
- Intellectual Property Theft – China's cyber espionage campaigns have reportedly stolen intellectual property worth hundreds of billions of dollars annually from U.S. companies.

- Cryptocurrency Heists – North Korea's cybercrime activities, including cryptocurrency heists, have reportedly generated funds that support the regime's military programs.

Security & Geopolitical Impacts

Nation-states exploit digital vulnerabilities to influence elections, gather classified intelligence, and disrupt rival activities. This has blurred the traditional boundary between physical and virtual warfare and reshaped power dynamics in the cyber arena, allowing smaller nations to wield disproportionate influence far beyond their physical borders.

- Critical Infrastructure Attacks – Nation-state actors have targeted critical infrastructure, such as energy grids and transportation systems. Iran's attack on Saudi Aramco in 2012 is a prime example.
- Election Interference – Russian interference in U.S. elections through cyber means including the 2016 U.S. Presidential Election has been well-documented, highlighting the potential for cyber espionage to influence democratic processes.
- Supply Chain Compromises – The SolarWinds attack, attributed to Russia, affected thousands of organizations, including U.S. government agencies, demonstrating the vulnerability of global supply chains.

Blurring the Lines | Overlaps Between APTs & Cybercrime

The lines between APT and cybercrime have become increasingly vague. This shift has been influenced by a combination of factors, including the increasing sophistication of cybercriminals, evolving motivations, and the lucrative nature of certain cyber activities. While APTs were historically associated with state-sponsored espionage and sophisticated attacks on political or strategic targets, they now exhibit a broader range of activities resembling cybercrime tactics.

Motivations have diversified, with state-backed groups engaging in cybercriminal activities to generate revenue and fund their ongoing operations. Some APT groups have embraced ransomware attacks, sometimes exploiting the profitability of extorting victims for financial gain but also as a technique of misattribution, disguising stealthy nation-state activity behind a front of common cybercrime. In this context, it is worth noting that cyber criminals themselves have learned from the APT playbook, displaying more advanced and targeted techniques akin to APTs, reflecting their growing ability to source advanced tools and breach high-profile targets.

The availability of advanced tooling through leaks such as Shadow Brokers has also played a pivotal role, enabling cybercriminals to harness APT-like tools and tactics. Access to sophisticated malware, zero-day exploits, and advanced social engineering toolkits and services through dark markets has empowered threat actors of all stripes to execute attacks once the exclusive domain of state-sponsored actors.

The blurring of these lines underscores the complex and dynamic nature of the cyber threat landscape. Traditional distinctions between APTs and cybercrime are changing and this crystallizes the challenge of the cybersecurity community to adopt a more holistic and adaptive approach to defense.

Conclusion | Guarding Against State-Sponsored Cyber Attacks

State-sponsored cyber attacks have evolved into a critical, global issue due to their potential to disrupt economies, compromise national security, and manipulate geopolitical dynamics. A cyber attack in one corner of the world can quickly reverberate across borders, affecting governments, industries, and individuals worldwide.

In response, various international policies and agreements have been established such as the Paris Call for Trust and Security In Cyberspace. The United Nations (UN) has also discussed norms of responsible state behavior in cyberspace, encouraging cooperation and restraint. Additionally, regional organizations and alliances, such as the European Union (EU) and NATO, have developed cyber defense strategies and mechanisms for organizations to share critical information.

Governments have also intensified their efforts to prevent and mitigate cyber espionage risks. The private sectors are investing heavily in cybersecurity measures, including threat intelligence sharing and vulnerability management. Various countries have implemented laws and sanctions to deter cyber espionage, promising to take legal action against state-sponsored cyber activities.

Enterprises facing the rippling effects of cyber espionage must adopt a multi-layered defense approach. Investing in robust cybersecurity measures, such as advanced, autonomous detection and response solutions, encryption, and regular security assessments, is crucial.

Outside of choosing the right tech, collaboration with cybersecurity partners and industry peers to share threat intelligence and best practices helps to enhance the community's overall resilience. As technology continues to evolve, an adaptive mindset, continuous monitoring, and a commitment to cybersecurity readiness can safeguard enterprises against the far-reaching impacts of cyber espionage.

Enterprises worldwide have turned to SentinelOne's Singularity™ Platform to proactively resolve modern risks at machine speed. Learn how SentinelOne works to more effectively manage risk across user identities, endpoints, cloud workloads, IoT, and more. Contact us or book a demo today.
