

An Introduction to Nation-State Cyber Threats

TLP: CLEAR B-2023-12-06a

Key Findings

- Nation states’ cyber programs often leverage a range of threat actors that can be categorized as nation-state actors, nation state-sponsored actors, and nation state-aligned actors.
- The distinctions between these three categories almost certainly varies depending on the country, and some nations are assessed to intentionally blur them.
- Advanced Persistent Threats (APTs) refer to a long-term pattern of targeted and sophisticated attack activity in which intruders gain unauthorized access, establish persistence, and remain undetected in compromised networks.
- Despite the terms often being used interchangeably, APTs are not synonymous with nation-state actors. APTs span the full range of nation-state linked threat actors, while some APTs likely lie outside nation-state programs altogether.

Nation-State Cyber Operations

Offensive cyber operations are now an established part of multiple nation states’ international strategic and operational objectives and are central to their externally-focused intelligence collection efforts. Nation states—including those adversarial to the United States, Europe, and the West more broadly—have extensive cyber programs that typically operate in four distinct tiers: influence or misinformation, cyber warfare, financial gain, and espionage. The weighting assigned to these tiers will vary according to each nation’s circumstances and strategic goals. Targets for attack include government, military, media and communications, healthcare, finance, and critical national infrastructure sectors.

Nation states’ cyber programs often leverage a range of threat actors, from operatives employed by official state apparatus to independent entities operating in alignment with state objectives. Operatives can be categorized into three overlapping buckets, which have become increasingly—and in some cases intentionally—blurred:

- Nation-State Actors
- Nation-State Sponsored Actors
- Nation-State Aligned Actors

Key Nation-State Cyber Threats

	Social Engineering Attacks		Wiper Malware
	Disinformation & Malinformation Campaigns		Backdoors / Loaders
	Trojans, Infostealers, and Spyware		Distributed Denial of Service (DDoS) Attacks
	Ransomware		

Nation-State Actors

Cyber threat operatives working entirely within—and under the direction of—official state apparatus. Attacks are typically carefully planned, with intrusions spanning months or years. Nation-state actors typically establish persistence in a network, remaining undetected while harvesting sensitive data, until objectives are met or the time arises to execute a destructive attack.

Nation-State Sponsored Actors

Collectives that are enabled by official state apparatus, typically receiving funding, technical assistance, or attack sanctioning—or partial direction—from official state sources. The distinction between nation-state actors and nation-state sponsored actors is often inconclusive and even intentionally blurred by nation-state officials as a means to maintain plausible deniability for attacks.

Nation-State Aligned Actors

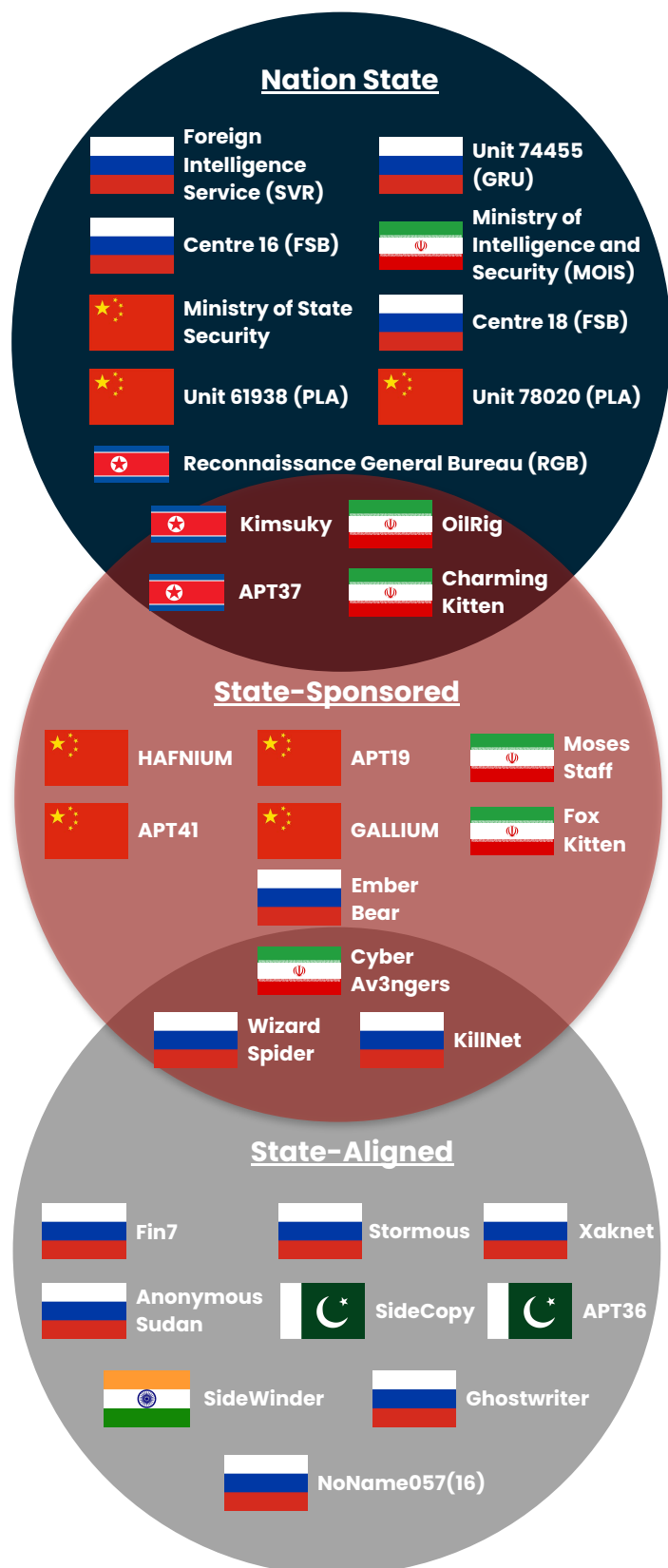
Cyber threat collectives that overtly or covertly align themselves ideologically with a nation state and act in accordance with its objectives. However, there is often insufficient evidence to suggest they receive formal financial or technical support from official nation-state apparatus. The distinction between a collective being nation-state aligned and nation-state sponsored is often unclear.

Increasing State Influence / Control

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 5:00 PM (EST) on December 5, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



Selected State-Linked Collectives



Source: ZeroFox Intelligence

Nation states have multiple units conducting offensive cyber operations leveraging a diverse set of cyber capabilities. These groups conduct a range of highly-sensitive activity under classified directives. Nation-state actors very likely operate—or collaborate with—a range of cybercriminal threat collectives. State employees are likely involved to varying degrees in the operations of multiple cyber collectives, including the deployment of ransomware and malware.

The degree of distinction between nation-state actors and nation-state sponsored collectives almost certainly varies depending on the country. It is likely many sponsored collectives have stronger ties to nation-state actors than have been identified. For example, DPRK-based threat actors very likely operate with little distinction between these two categories; cyber groups are tightly controlled and directed by the government's Reconnaissance General Bureau (RGB), North Korea's primary intelligence and clandestine operations apparatus. It is very unlikely DPRK-based, externally-facing cyber collectives operate outside the strict control of nation-state apparatus. Many North Korean group definitions are known to have significant overlap, very likely a result of commonality in tactics, techniques, and procedures.

Other countries, such as Russia, are assessed to have more variation in their control over threat groups. It is very likely Russia-aligned threat actors operate with at least some degree of autonomy from the state. Some hacktivist collectives are likely receive sanctioning—at most—for attacks from official state entities, with no substantiated evidence to suggest they receive resourcing or assistance; to note, this often runs contrary to the groups' claims. Russia is one of the main culprits for blurring the distinction between the three categories of threat actor. Ensuring some threat actors are overtly kept at arm's length from nation-state control is almost certainly an intentional strategy; nation-state actors are happy to let affiliates aid battlefield progress by targeting opponents, while also enabling plausible deniability for attacks against Western targets.

ZeroFox Intelligence does not provide intelligence assessments of nation-state actors, such as Russia's Foreign Intelligence Service (SVR). ZeroFox has limited insight into the short- and long-term objectives of these entities. The highly evasive nature of their operations means intrusions are unlikely to be identified in advance of attacks. However, ZeroFox Intelligence routinely provides assessments following attacks, such as SVR-attributed APT29's SolarWinds attack in 2019 / 2020.

Advanced Persistent Threats (APTs)

APTs refer to a long-term pattern of targeted and sophisticated attack activity in which intruders gain unauthorized access to a network, establish persistence, and typically remain undetected for a considerable period of time. Attacks are highly customized and are deployed against high-value, strategic targets. APTs pursue their objectives consistently over an extended period of time, adapt to circumvent defensive efforts, and are resolute in maintaining network access sufficient to execute their objectives.

APTs are not synonymous with nation-state actors, despite the terms often being used interchangeably. APTs span the full range of nation-state linked threat actors, with some activity attributed to nation-state apparatus and others spanning nation-state sponsored and nation-state aligned entities. They are often embedded in a complex web of political, economic, and strategic motivations. It is also more likely than not that some APT operations lie outside alignment with nation states altogether. Nation-state actors are very likely responsible for multiple APT operations.

APTs consist of highly capable threat actors launching complex, customized, and stealthy attacks. APT operations are typically backed by significant resources, which enable them to achieve their aims. While objectives can vary, typically APTs aim to establish a foothold within a target network to conduct cyber espionage (including theft of sensitive information, intellectual property, or state secrets), for financial gain, to disrupt critical system functions, or to destroy a network entirely. Infiltrating their adversaries networks and systems; threat actors are able to gain valuable knowledge, obtain blackmail against high ranking members of society, disrupt operations and even influence global events. It is likely that some highly-skilled operatives are involved in more than one APT operation.

Selected APT Groups & Assessed Links to Nation-State Operations

APT1 Comment Panda		A Chinese threat group that has been attributed to the People's Liberation Army (PLA) Unit 61398
Sandworm		Attributed to Russia's General Staff Main Intelligence Directorate (GRU) Unit 74455
Gamaredon Group		Reportedly operating under FSB direction and staffed by FSB members
MuddyWater		Conducts cyber operations as part of Iran's Ministry of Intelligence and Security (MOIS)
Lazarus Group Labyrinth Chollima		Defined as an agency or controlled entity of the DPRK's Reconnaissance General Bureau (RGB)
APT10 menuPass Cicada		Individual members known to have acted in association with the Chinese MSS Tianjin State Security Bureau
APT32 Ocean Lotus		A Vietnamese cyber military operation that targets entities considered hostile to Vietnamese nationalist interests
APT28 Fancy Bear Tsar Team		Reportedly attributed to Russia's GRU Unit 26165
APT29 Cozy Bear Nobelium		Reportedly attributed to the Russian government's Foreign Intelligence Service (SVR)
Turla Team Venomous Bear Snake		Turla's operations reportedly linked to Center 16 of the Russian FSB
APT34 OilRig		Focused on efforts to benefit Iranian nation-state interests and assessed to likely work on behalf of the Iranian government
APT41 Winnti Group Wicked Panda		A Chinese state-sponsored espionage group that also conducts financially-motivated operations
APT19 Deep Panda Shell Crew		A hacking collective, likely with some degree of sponsorship by the Chinese government

Source: ZeroFox Intelligence

ZeroFox Intelligence provides threat assessments of APT operations, including identified campaigns and trends. Analysis of sustained targeting and trends in methodologies can provide reliable and useful insight for defenders.

The modus operandi and trends in APT attacks are more easily discernible than the objectives of nation-state actors that often sit behind them.

Recommendations

- Critical data should be backed up regularly, including password-protected backup copies kept offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, or the cloud).
- Ensure proper network segmentation.
- Never download email attachments from unknown senders or click links from untrusted sources. Provide user-training programs to fight against phishing or social engineering attacks used to obtain critical information that can lead to attacks.
- Enable multi-factor authentication wherever possible.
- Patch disclosed vulnerabilities with updated software versions as quickly as practical.
- Perform regular audits of identity access management tools or systems to ensure user accounts are secured.
- Disable PowerShell wherever possible to limit the possibility of operators employing lateral movement modules.
- Employ behavior-based malware detection as well as signature detection to address the use of commodity tools.
- Leverage ZeroFox Intelligence’s Attack Surface Assessment to understand the threats faced.
- Utilize the ZeroFox Platform’s Intelligence Search interface to investigate Indicators of Compromise (IOCs) and metadata related to Malware and Ransomware.

APPENDIX A: ZeroFox Intelligence Probability Scale

All ZeroFox Intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

APPENDIX B: Traffic Light Protocol for Information Dissemination

TLP:RED

HOW IT IS USED
Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party’s privacy, reputation, or operations if misused.

HOW IT IS SHARED
Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP:AMBER

HOW IT IS USED
Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED
Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that TLP:AMBER+STRICT restricts sharing to the organization only.

TLP:GREEN

HOW IT IS USED
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED
Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP:CLEAR

HOW IT IS USED
Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED
Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform. With complete global coverage across the surface, deep, and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

Ready to See for Yourself?

- › **Request a Demo:**
Sign up on zerofox.com/request-a-demo
- › **Learn More:**
Visit zerofox.com
Contact us at sales@zerofox.com / 855.736.1400