NISOS

Webinar Brief

Nation-State Espionage Programs: An Analysis of Russian, Chinese, Iranian, and North Korean Capabilities

Executive Summary

The United States and Western allies are witnessing a full scale assault on our national security, industrial, and economic base using full spectrum cyber, signals intelligence, and human intelligence capabilities. Advanced Nation State adversaries are increasing cyber attacks against the West through computer network exploitation (CNE) and the recruitment and compromise of insiders. Targets include military, intelligence, science & technology, pharmaceutical, energy and economic sectors.

Adversaries leverage a mixture of zero day development, open-source and publicly available exploits, and a growing number of contractor or “commercial” entities to target national security and economic targets. Inadequate security controls, poor configuration and patch management, and a fundamental misunderstanding of the threat and capabilities of our adversaries creates a target rich environment across all sectors of government and business.

Attack Profiles:

Russia is a near peer adversary centered on military and political aims, with a focus on advancing regional power. Russia seeks to counter Western influence in their region and leverage strategic military, economic, and energy-based influence against EU and NATO countries. Russia possesses advanced CNE capabilities from long-term research and development efforts and a mature science and technology sector focused on national security. The recent SolarWinds attacks are largely attributed to Russian state actors and are an example of Russia’s increasingly advanced CNE tactics and capabilities and reflect an aggressive offensive operational capacity.

China is a near peer adversary with military, political and economic objectives. China seeks to replace the United States as the dominant global power and leverages all means available to counter US and Western interests. China conducts aggressive CNE operations against US and Western corporations and intellectual property (IP) seeking competitive advantage across all business lines and sectors. China leverages its unique position as the global manufacturing center to seek economic control of the global export market and its own domestic market.

The recent Microsoft Exchange Server-based attacks have been attributed to Chinese state actors and are an example of China's increasingly advanced CNE capabilities and reflect an aggressive offensive capability.

North Korea is an emerging threat actor driven by sanctions and economic dysfunction to focus on focused on regional military and intelligence aims. Sanctions and economic dysfunction have led them to focus on illicit finance and e-crime. North Korea leverages national resources and advanced CNE capabilities to counter US and Western power and target global corporate and economic entities.

Iran is an emerging threat actor focused on regional military and intelligence aims.   Sanctions and economic dysfunction have led to a focus on illicit finance and e-crime. Advanced research, development and engineering enable an   ideological base intent on countering US and Western influence. The longtime US military adversary with increasing CNE capabilities largely targets critical infrastructure and economic entities.

Insider Recruitment:

The most aggressive efforts to steal intellectual property emanate from China (ex; 1000 Talents Program) with aggressive recruitment and placement of Chinese nationals into US and Western universities, research institutions, and corporations. Russia and China also engage in advanced HUMINT espionage targeting US and Western military and intelligence officers with economic and ideological incentives Common tactics include the recruitment and development of insiders with access to proprietary information and the leveraging of supply chains and mergers and acquisitions to insert human assets into target organizations.

Defensive Actions:

The following controls should be prioritized to reduce attacker dwell time. They enable businesses to detect security events early and prevent security incidents and costly security breaches.

Comprehensive Asset Inventory:	Allows routine identification of vulnerable systems.
Effective Enterprise Configuration and Patch Management:	Ensures software updates are implemented to reduce vulnerabilities and exposures.
Email Security and Domain Intelligence:	Detects malicious email traffic and external attack campaign infrastructure creation and usage.
Enterprise Event Monitoring and Alerting:	Alerts on malicious activity to include lateral movement, administrative privilege escalation, data exfiltration, etc.

Network Segmentation with Strong Access Controls:	Reduces attacker visibility and access to critical systems and sensitive data.
Identity and Access Management (IAM):	Provides authentication, authorization and accounting and enforces policies ensuring that the proper people in an enterprise have the appropriate access to technology resources.
Enterprise Endpoint Detection and Response (EDR):	Detects malicious processes being run on endpoints and servers.
Comprehensive Third-Party Risk Management Program (TPRM):	Increases third-party risk awareness to reduce potential exposures and corporate governance issues
External Threat Monitoring:	Monitoring for malicious external threats to the organization and its employees, operating locations, infrastructure, products, etc to enable increased readiness.
Extensive Red Teaming and Attack Simulation:	Continuous adversary emulation to assess existing security controls and detection capabilities to identify vulnerabilities and allow for more robust defenses to be tested and implemented.

About Nisos

Nisos is the Managed Intelligence company. Our services enable security, intelligence, and trust & safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset delivering smarter defense and more effective response against advanced cyber attacks, disinformation and abuse of digital platforms. For more information visit: **www.nisos.com**

About Bishop Fox

Bishop Fox is the largest private professional services firm focused on offensive security testing. Since 2005, the firm has provided security consulting services to the world's leading organizations — working with over 25% of the Fortune 100 — to help secure their products, applications, networks, and cloud resources with penetration testing and security assessments. In February 2019, Bishop Fox closed $25 million in Series A funding from ForgePoint Capital, which will allow the company to continue to grow its research capabilities and develop next generation offensive security technologies like Continuous Attack Security Testing (CAST). The company is headquartered in Phoenix, AZ and has offices in San Francisco, CA and Barcelona, Spain. For more information visit: **www.bishopfox.com**