U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

Adam Meyers
Sr. Vice President, Counter Adversary Operations
CrowdStrike

"Big Hacks & Big Tech: China's Cybersecurity Threat"
November 19th, 2024

Chairman Blumenthal, Ranking Member Hawley, members of the Subcommittee: thank you for the opportunity to testify today. My name is Adam Meyers, and I serve as Sr. Vice President for Counter Adversary Operations at CrowdStrike. For over a decade, I've led the company's practice area on monitoring and disrupting cyber threats. An overwhelming share of my attention over this period has focused on the People's Republic of China.

As a leading U.S. cybersecurity company, CrowdStrike has a useful vantage point on China's malicious activities in cyberspace. Protecting organizations with our cybersecurity technology, threat intelligence, and incident response services, we confront a full range of cyber threats. We defend many components of the U.S. Federal government and serve as a commercial cybersecurity provider for major technology companies, 8 of the top 10 financial services firms, thousands of small- and medium-sized businesses, as well as all manner of critical infrastructure entities and many foreign companies. Chinese threat actors target each of these sectors heavily.

We started CrowdStrike in large part due to the growing impact of unchecked Chinese cyber threats, and the inability of existing security tools to meet this challenge. In 2011, it wasn't uncommon to see Chinese campaigns spanning scores of victims, with a multi-year duration, using extremely basic tools, tactics, techniques, and procedures. Back then, cybersecurity was focused on preventing the most prevalent threats, rather than the most impactful ones. Moreover, it was considered impolite, or even counter to one's economic interests, to call out this activity directly. I'm proud of the work our team–and the cybersecurity community more broadly–has done over the intervening years to change this perception. I'm grateful for the work this Committee is doing now to stay focused on this critical problem.

CrowdStrike does address Chinese cyber threats directly, including attributing adversaries to specific government, military, and intelligence organizations. We utilize a cryptonym-based naming convention to describe these threats in order to permit the flexibility to update attribution, account for reorganizations, and manage multiple actors with the same institutional affiliation. We assign a cryptonym once we achieve a reasonably robust confidence level in our attribution, and designate

China-based actors as “PANDAs.”[1] At present, we track 63 distinct PANDA adversaries, 31 of which have been recently observed, as well as a large number of other “activity clusters” with likely ties to China, but lower fidelity on their attribution.

Today’s hearing provides a unique opportunity to discuss recent China-nexus intrusions into our critical infrastructure, but I’ll begin with a brief overview of how we got here.

Evolution of the China Cyber Threat

Over the two decades I’ve assessed the China cyber threat across the public and private sectors, I’ve witnessed a marked evolution from simplistic–though often effective–“smash and grab”-type campaigns to much more sophisticated activity like that which we’ll discuss today. These changes span operational advancements, technical capabilities, and considerably greater alignment to formal national political aims. These changes also belie an increase in funding, training, and resources. For context, I’ll briefly summarize this evolution.

A reorganization of China’s cyber-focused institutions in approximately 2015 upleveled the threat. In that timeframe, we observed a notable shift away from the use of military institutions and toward the use of commercial contractors affiliated with the Ministry of State Security (MSS), China’s primary foreign intelligence organization. These shifts coincided with broader reforms of China’s defense and security complex, consistent with Chairman Xi’s consolidation of political power. High-capability China-nexus targeted intrusion adversaries like AQUATIC PANDA, WICKED PANDA, and the recently-indicted JUDGMENT PANDA are attributed to private sector contractors supporting the MSS. These adversaries and contracting organizations also have deep connections to Chinese universities, and likely draw talent from the cybersecurity training pipeline prioritized and funded by the Chinese Communist Party (CCP). People’s Liberation Army (PLA)-aligned groups remain active threats, but focus on cyber operations supporting near-abroad intelligence collection and domestic security functions.

A series of laws and regulations advanced in China since the 2017 timeframe support a national approach to developing cyber capabilities. A 2018 national security law effectively nationalized vulnerability research in China. Under China’s 2021 Regulations on the Management of Security Vulnerabilities in Network Products—an addition to the 2017 Cybersecurity Law—zero-day vulnerabilities discovered in hacking competitions must be disclosed within 48 hours of discovery via the Ministry of Industry and Information Technology (MIIT) to government authorities. In the aggregate, China’s vulnerability exploitation ecosystem and pipeline is becoming more professional and reflects increasing ties to state-intelligence. Once disclosed, knowledge of these vulnerabilities is likely disseminated to relevant agencies for further research and exploit development. Industry researchers speculate that Chinese intelligence and public-security agencies use this knowledge to develop mitigations for securing internal critical infrastructure and to support development of operational zero-day exploits used to target U.S. and other entities.

[1] These names generally take the form of a community- or researcher-derived codeword with some significance, followed by an animal type determined by the actor’s geography or motivation. This name scheme is designed to be somewhat more descriptive than others, and can simplify communication and information sharing with government and industry counterparts, as well as assist clients’ threat modeling process. For more detail, see: “Global Threat Landscape,” https://www.crowdstrike.com/adversaries/.

If these targeted laws and regulations explain "how" China has augmented its cyber capabilities, broader and more deeply-rooted national plans explain "what" Chinese entities leverage these capabilities to achieve. National efforts like the Belt and Road Initiative (BRI), Made in China 2025 (MIC2025), the 2035 Vision, and the forthcoming 2049 Centennial are driving factors. Longstanding Five Year Plans (FYPs) provide a window into the CCP's strategy for economic development in the short- and medium-term. While a full discussion of these documents is beyond the scope of this testimony, such plans can highlight key technological gaps perceived by China's economic and security planners and Party figures. This, in turn, drives intelligence collection priorities and subsequent offensive operations by Chinese security services, including cyber espionage and theft of intellectual property (IP). Unfortunately, IP theft remains a relatively low-cost solution with scarce direct consequences.

Emerging focus on Critical Infrastructure & Telecommunications

Today, Chinese threat actors operate complex, sophisticated, meaningfully obfuscated,[2] and often highly effective cyber operations campaigns targeting every region and every industry vertical. Recent campaigns demonstrate the ability to compromise large, well-resourced, and well-defended enterprises that operate as providers for the rest of the technology ecosystem. These examples highlight a growing emphasis within Chinese operations on "upstream" or "bulk" collection, which is notable for its efficiency, scale, and potential for impact. I'll provide a brief overview of a few recent and notable campaigns.

Over the past year, VANGUARD PANDA (*Volt Typhoon*) has targeted ubiquitous unmanaged or perimeter (edge) devices and infrastructure. This is consistent with other China-nexus adversaries increasingly moving away from the use of low-sophistication methods for initial access like spear-phishing, weaponized USBs, and credential harvesting, instead favoring specific exploitation of vulnerabilities in edge devices like firewalls, gateways, or enterprise proxies to achieve initial access.[3] These same edge devices that are integral to connecting networks to devices provide a ripe attack surface for adversaries. Targeting these systems is fruitful because they are critical components for authentication and provide a pathway to compromise identities. These attacks are also relatively stealthy on account of reduced visibility from third-party security providers, minimal telemetry generated by system access and use, and limited forensic artifacts. Use of these techniques further limits the detection capabilities of defenders and the capacity to track adversary operations by researchers.

VANGUARD PANDA's targeting, which largely focused on critical infrastructure providers, drew significant attention from U.S. policymakers due to its potential application for "preparation of the

[2] As of today, CrowdStrike tracks 17 Operational Relay Box (ORB) networks leveraged by China-nexus adversaries to obfuscate and hide their activity. These ORB networks are extensive, some consisting of thousands of compromised small-office/home-office (SOHO) routers. China-nexus adversaries, including VANGUARD PANDA, leverage the ORB networks in all aspects of their operations, including to compromise U.S. based entities, conduct reconnaissance and manage their infrastructure.

[3] When traditional Remote Access Tools (RATs) are observed, Crowdstrike overwhelmingly sees China-nexus adversaries use closed source but shared tools unique to China-nexus actors. Tooling frequently proliferates from high-capability adversaries to lower tier operators over time, either through affinity groups or formalized training or technology transfer programs.

battlespace." That is, potential use of disruptive or destructive attacks preceding or coinciding with military hostilities.

Recent reporting about another threat actor, *Salt Typhoon*, depicts active targeting of telecommunications infrastructure. This is consistent with targeting and tradecraft we have observed over time (including a notable campaign I describe below). I expect we will have additional commentary on this actor as more public details emerge.

Another marker of maturation is the complexity of successfully exploited systems.[4] Advanced adversaries such as LIMINAL PANDA demonstrate extensive knowledge of telecommunications networks, including understanding interconnections between providers and the protocols that support mobile telecommunications.[5] Recently, this adversary compromised these networks by exploiting trust relationships between telecommunications organizations and poor security configurations, allowing them to create footholds to install multiple redundant routes of access across the affected organizations. The adversary ultimately emulated the global system for mobile communications (GSM) protocols to enable Command and Control (C2) and developed tooling to retrieve mobile subscriber information, call metadata and text messages, and facilitate data exfiltration. Actions on objectives indicated additional adversary aims of surveilling targeted individuals by gathering metadata about their cellular devices.

Recommendations

These are just a few examples of contemporary campaigns from Chinese threat actors. I could go on about separate efforts targeting government entities or other sectors, but hopefully this summary effectively illustrates the nature and severity of the problem we face. I'd now like to turn to a few policy recommendations I think are worth our collective consideration.

Enterprises. Defenders need deep insight into the threatscape to protect against malicious activity. The security community should continue to monitor China-nexus adversaries and actively hunt for them. The more we understand about these groups, their targeting practices, their resources, and their constraints, the more accurate a threat model we can develop to help defend targeted industries, organizations, and individuals.

Defenders should also take increasing care to defend identity[6] across the enterprise. Compromised identities are at the core of most of the threat activity CrowdStrike has observed and responded to over the past several years. Better identity security enables a radical reduction in threats.

[4] China-nexus adversaries continue to increase their stealthiness and knowledge of the environments they are operating in, using novel techniques to move quickly, move laterally and escalate privileges, and remain undetected. Notably, a widely-reported 2023 breach of a major software provider demonstrated the ability to manipulate encryption systems to arbitrarily mint keys to grant the threat actors access to sensitive systems. See https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

[5] "Unveiling LIMINAL PANDA: A Closer Look at China's Cyber Threats to the Telecom Sector" CrowdStrike Blog, November 19, 2024. www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/.

[6] In cybersecurity, identity encompasses the diverse methods of representing, authenticating, and authorizing humans, devices, applications, and systems—ranging from usernames and biometrics to machine certificates and behavioral patterns as well as tokens—ensuring secure access and interaction across digital ecosystems.

Enterprises must also maintain visibility across increasingly complex, distributed, and federated networks. Today, that requires instrumenting and monitoring traditional endpoints like laptops and desktops, network infrastructure, cloud environments, mobile and IOT devices, and increasingly, Software-as-a-Service (SaaS) applications. Such monitoring generates valuable security telemetry, designed to alert defenders to threats across each of these vectors. In the face of today's cross-domain threats, it's vital to connect the dots across all of these domains to obtain a full picture and identify multi-faceted adversary intrusions. Use of technologies like Next-Generation Security Information and Event Management (NextGen SIEM) tools can help make this duty more straightforward for organizations of all sizes.

Security Industry. Threat actors are increasingly looking to leverage AI for malicious purposes, such as vulnerability discovery, exploit development, and conducting intrusions at scale. The security industry must focus on AI innovation in order to prevent these threats. It's important to recognize the significant, current benefits AI is driving in cybersecurity tools, which overperform by a wide margin legacy tools that do not leverage AI. As an AI-native company, CrowdStrike has for over a decade used Machine-Learning (ML)-based prevention, and we're increasingly leveraging Large Language Models (LLMs) to make security work more efficient and accessible to more security professionals. Further, AI is essential to achieve unified cross-domain visibility. It's essential to remember that adversaries will continue to leverage AI to innovate, regardless of the "rules of the road" for defenders.

Executive Branch. Key U.S. federal departments and agencies have come a long way on cybersecurity over the past number of years, but there's still progress to be made. The U.S. government itself faces among the most severe threat environments of any organization globally. There is ample opportunity to lead by example here by ensuring Federal departments and agencies have the best tools, best training, and most informed concepts of operations for defense available. Moreover, findings from successfully defending Federal agencies can support the development of best practices of value to other sectors, like academia, commercial enterprises, and nonprofits.[7]

Several key departments can also do more to proactively meet and defeat cyber threats. This includes increasing collaboration with industry on threat hunting practices and particularly on performing threat actor infrastructure takedowns. Efforts along these lines do take place periodically. But regrettably, from my vantage, the threat environment has worsened more rapidly than our capacity to execute such operations has increased. It's now worth asking: in collaboration with international partners, what might we do to increase the tempo of disruptions by 5x? Or by 10x? It may take that scale to impact threat actors' operations sufficiently to raise their cost of doing business and offer meaningful relief to victims.

[7] For specific recommendations on improving federal cybersecurity, *see Rob Sheldon, Testimony on "Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs"* U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection (September 19, 2023). https://www.crowdstrike.com/wp-content/uploads/2023/11/9.19-CHS-Federal-Cyber-Testimony.pdf.

Legislative Branch. For Congress' part, it's appropriate to perform oversight to ensure Federal agencies are actively pursuing the objectives outlined above. Further, to the extent that some of the responsibilities for enterprises I've outlined above appear out of reach for the average small business in your state, it's appropriate to engage in a more meaningful conversation than we as a community have had to date on the use of tax credits, rebates, or other incentives to make best-in-class cybersecurity tools and training more accessible.

Thank you again for the opportunity to testify today, and I look forward to your questions.

###