Prepared Statement
Charles Carmakal, Chief Technology Officer
Mandiant Consulting
Before the United States House Committee on Oversight and Accountability
Subcommittee on Cybersecurity,
Information Technology, and Government Innovation

May 15, 2024

Introduction
Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thank you for the opportunity to share my observations and experiences regarding this important topic, as well as for your leadership on cybersecurity issues. My name is Charles Carmakal and I am the Chief Technology Officer of Mandiant.

Background
In my role at Mandiant, I oversee a team of security professionals that help organizations respond to complex cybersecurity breaches orchestrated by foreign governments and organized criminals. I have personally led and been involved in the responses to thousands of cybersecurity intrusions. I led the teams responsible for identifying the SolarWinds software supply chain attack in December 2020, the Colonial Pipeline disruption in 2021, and the discovery of several novel and sophisticated cyber campaigns carried out by China-nexus threat actors.

Mandiant employees are on the front lines of the cyber battle, actively responding to computer intrusions at some of the largest organizations on a global scale. We employ more than 900 cybersecurity experts in over 28 countries, with skills in digital forensics, malware analysis, intelligence collections, threat actor attribution, and security strategy and transformation. Over the last 20 years, we have responded to thousands of security incidents.

I am here to talk about Mandiant's and my personal experiences in defending against and responding to cyber threats emanating from the People's Republic of China. I will share my first-hand observations and the observations of the team that I lead.

The US / China Agreement in 2015
Before we discuss today's threats, it's important to review what's happened over the past decade.

On September 25, 2015, the United States and China agreed that neither government would "conduct or knowingly support cyber-enabled theft of intellectual property" for an economic advantage.

The following year, in 2016, Mandiant analyzed our incident response cases to assess the impact of the agreement.[1] We actually observed a reduction in cyber intrusions by China-nexus threat actors that began a year prior to the agreement. The relatively lower volume of intrusion activity continued until approximately 2020.

Government-backed China-nexus threat actors operated notably differently prior to the Agreement than they do in modern days.

1. **Email-based phishing** – They commonly sent email-based phishing emails to employees of the organizations they targeted. The emails often contained a malicious attachment or a link to a malicious website. Their goal was to deploy malicious software on the computers of their targets, which would enable them to gain deeper access into the victim's environment. Their ultimate objective was to steal data or intellectual property that would give China an economic, military, or political advantage.

2. **Backdoors** – They deployed backdoors across the environment to ensure they could maintain persistent access to the victim's environment. Backdoors were often deployed on Windows-based systems and were not commonly detected by antivirus software.

3. **Foreign IP addresses** – They would access victim environments from systems they controlled in China and other parts of the world. Organizations with mature security teams could identify evidence of compromise by identifying anomalous network connections from foreign countries.

4. **Multiple threat actors** – Multiple discrete and unrelated China-nexus threat actors would compromise the same victim environment with the objective of stealing the same data, likely without knowledge of each other in the network.

Current Advanced Tradecraft Employed by China-nexus Threat Actors

These China-nexus threat actors operate very differently today. They are more coordinated, resourced, sophisticated, and clandestine.

1. **"Zero day" vulnerabilities** – They often research and develop exploits for "zero day" vulnerabilities. A "zero day" vulnerability is when an adversary has knowledge of a vulnerability before the vendor does. The tools and knowhow to exploit these vulnerabilities are shared among multiple discrete groups that conduct cyber operations for the benefit of the PRC. Over the past few years, we've observed targeted zero day exploitation of vulnerabilities in VPN, firewall, email security gateway, hypervisors, and other technologies that do not commonly support endpoint detection and response solutions.

2. **Targeting systems without EDR** – Endpoint detection and response solutions have gotten more effective at identifying malicious software on Windows systems. China-nexus threat actors

---

1 https://www.mandiant.com/resources/reports/red-line-drawn-china-recalculates-its-use-cyber-espionage

realize most organizations largely rely on EDR detections to discover network compromises. As a result, these threat actors develop and deploy novel and advanced malware ecosystems that are specific to the technologies that they compromise.

3. **"Closed box" appliances** – Many of the systems that these actors target are considered to be "closed box," meaning the organizations using them cannot install EDR or antivirus software. This makes it very difficult for organizations to determine if they are compromised. If the organization wants to forensically examine the device to determine if it's compromised, they often need to reach out to the vendor to ask for permission to obtain access to the device to examine it. Not all vendors will provide this access to the victim.

4. **Residential IP addresses** – Over the years, these actors have compromised home and small office networking devices in an effort to build a large network of residential IP addresses that they could proxy their traffic from. That way, if they wanted to log into the VPN of a Virginia-based organization, they could appear to come in from the cable modem of someone living in Virginia, so that the network connection does not appear to be anomalous.

5. **"Living off the land"** – Nowadays, these actors try to avoid deploying malware on Windows systems, out of fear that they will be detected by modern EDR solutions. Instead, they leverage built in commands and tools on Windows and other systems within the environment. This makes it more difficult for victims to discover they are compromised.

Difficulty in Discovering Compromises

Given the advanced tradecraft leveraged by China-nexus threat actors, it is incredibly difficult for organizations to know when their environments have been compromised. Many organizations that engage Mandiant to help them investigate and respond to a China-nexus intrusion stumble upon network activity suggesting they could be compromised. My team often discovers that these intrusions began months or years ago.

Through the course of our day-to-day investigations and threat research, we often learn about other entities that have been compromised by China-nexus threat actors. We do our best to notify victims. When we have prior relationships with the victim and when they have a dedicated cybersecurity team, we often help them contain the incident and eradicate the threat actor before significant damage could be done. However, there are times where we struggle to contact smaller organizations, for example cities or municipalities that do not have dedicated cybersecurity staff.

We recommend organizations do the following to try to mitigate the risk and impact of intrusions by China-nexus threat actors:

1. Implement "zero trust" principles throughout environments to enhance preventative, detective, and response controls.
2. Deploy modern endpoint detection and response (EDR) solutions across the environment.
3. Implement multi-factor authentication across all remote access solutions and SaaS environments used.
4. Conduct regular "red team" exercises to test network defenses and measure intrusion detection efficacy.

5. Perform regular “threat hunts” of the environment to look for indicators of compromise, based on threat intelligence shared by the security community, other victims, and government partners.

Conclusion

Over the years, I have personally observed multiple China-nexus threat actors with significant access and privileges to U.S.-based technology, defense, government, energy, construction, chemical, financial services, and healthcare organizations. Fortunately, I have not yet personally observed any actions taken by these actors that I consider to be overtly and intentionally destructive that could directly lead to negative kinetic outcomes or physical harm to people.

On behalf of Mandiant, I thank you for this opportunity to testify before the Subcommittee. As we collectively consider these threats and methods to prevent attacks, reduce damages, and remediate, it’s important to realize we are no longer facing one-off cyber attacks. We are contending with long-term, persistent campaigns conducted – and at times financed – by nation states. A “whole of community” plan and response and collective defense to thwart China and other actors, which includes the private sector, is necessary to deter this behavior and to build better resiliency into our nation’s networks.