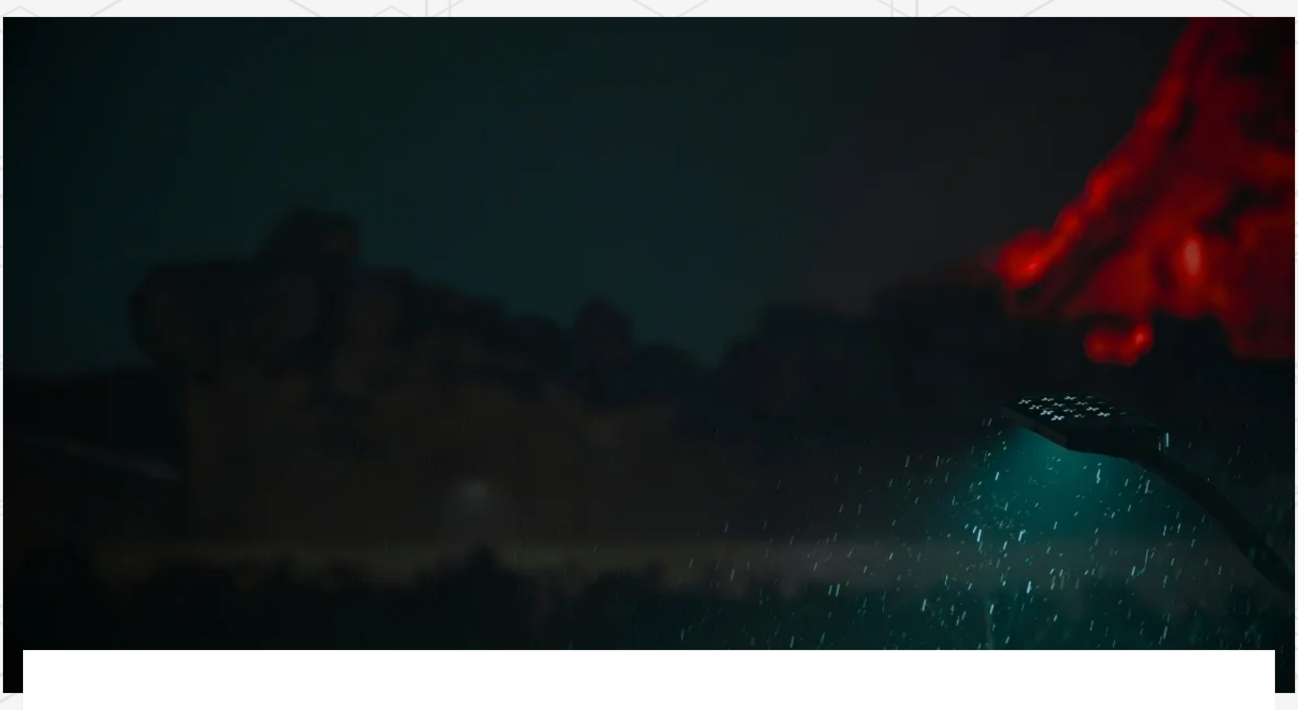

SECURITY & INTELLIGENCE

China's Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

DAKOTA CARY / OCTOBER 16, 2024

Executive Summary

- The latest CVERC report reflects China's ongoing efforts to undermine support for U.S. surveillance activities by attempting to fuel debate over Section 702.
- The CVERC report also draws Microsoft into its crosshairs as part of an ongoing push to remove foreign technology from PRC government systems.
- The report highlights previous intelligence from France and Germany regarding U.S spying in an attempt to deflect attention away from recent incidents of Chinese espionage in Europe, likely as a means to shape narratives amid ongoing political debates.

Introduction

China's Computer Virus Emergency Response Center has released part three of a running series claiming that the U.S. government is actually behind Volt Typhoon activity, rather than China. The latest CVERC report, whose front page includes an oddly edited photo with the text "Lie to Me," provides no new evidence of these claims and rehashes old leaked U.S. intelligence documents. However, this CVERC report is not useless.

The CVERC report tells us more about China's intentions than it does convince readers of the PRC's claims about Volt Typhoon. SentinelLabs has previously covered the CVERC's behavior and is issuing this report to update readers with specific takeaways based on the content of the third edition.

In our first report, we highlighted a pattern of coordination between China's cybersecurity companies, state media, the CVERC, and publications about U.S. hacking operations. We find that the pattern is thus: a cybersecurity company publishes a new report analyzing old leaked documents from the U.S. government, the CVERC picks up the piece and adds analysis–or in many cases, co-authors the report with the company–then state media regurgitate the report in English for international audiences.

In some cases, these reports make their way into official PRC government press briefings. In one instance, a PRC embassy abroad re-hosted the report's content. It is a full court-press to point the finger at U.S. hacking efforts without providing new or substantiated claims.

It is clear that such efforts are state-directed, not merely by association of the organizations involved, but by the steady recurring drumbeat of publications. However, such a directive to produce more when there is nothing to be written is hard for writers and researchers. When writers are forced to fill a page count, they inevitably drift towards their own intentions as evidence of their claims run dry. The CVERC's latest report falls victim to this trap.

What follows is our distillation of what we believe analysts can learn from the latest CVERC report about China's posture in geopolitics, cybersecurity, and hacking operations.

Targeting Section 702

The authors mention Section 702 authorities 13 times across 60 pages, and it is a clear focal point. Compromised devices in the U.S. and abroad constitute the botnets that Chinese operations rely on for obfuscation. Section 702 very likely enables U.S. collection of Chinese activities on these devices that are located in the US. Without Section 702, tracking Chinese hacking operations would be very difficult.

However, Section 702 in the United States is controversial. Reviving the 702 debate is clearly in China's interest and is their intent, as shown by how China highlighted "impacts to ordinary Americans." No doubt that China hopes a policy move against potent U.S. counterintelligence tools would be in its interest. Will PRC influence ops push such narratives? Already, The Register's cybersecurity editor wrote a piece arguing the line that China clearly hoped to promote–that Volt Typhoon is an excuse to continue Section 702.

The CVERC publication may be motivated by previous potential Russian successes in changing U.S. policy. Following Russian abuse of leaked NSA vulnerabilities and tools that caused massive economic losses (NotPetya), the U.S. policy community debated the curtailing of these tools. Committees held public hearings and the DNI suggested that if the U.S. could not control such capabilities, perhaps they should not be developed.

This period coincides with what Ben Buchanan notes as the end of the NOBUS era. The result of Russia's operations, which were cemented by DPRK bumbling a global ransom op (WannaCry), was the creation of the Vulnerabilities Equities Process (VEP), a process through which the majority of U.S. vulnerabilities discovered are burned and given to their manufacturer. China may hope to achieve a sunset to 702, just as the Russians—intentionally or not—instigated the VEP.

Pushing Foreign Tech Out of China

The CVERC report also draws Microsoft into its crosshairs and tracks the movement of former U.S. government officials to MSFT-related entities. Underpinning CVERC's concern is CCP Document Number 79, which pushes for the removal of all foreign technology from PRC government systems. China's efforts to create its own tech ecosystem, including a domestic operating system, epitomize the effort. CVERC is in no position to signal intent about stopping MSFT's operations in China.

Still, the report suggests the organization is emboldened in its stance on the company. More sure of itself than ever, the CCP seems ready to hit foreign firms that have long remained key IT providers in its ecosystem. Eventually, successful implementation of Document 79 will push MSFT almost entirely from the PRC technology ecosystem.

Shifting the Narrative in Europe

Finally, the CVERC's mentions of France and Germany arrived at a time of intense infighting over the future of Europe and its relationship with China. Until recently, German and French firms had been making hay of U.S. firms leaving the PRC. Buying assets on discount and doubling down with its in-country partners. Now, the sands are shifting.

Germany arrested Chinese spies earlier this year. The Dutch publicly attributed hacking campaigns to China. In France, the police stopped Chinese diplomats from forcibly repatriating a dissident and asked two PRC spies to leave the country. Who knows what happens behind closed doors in Brussels, but suffice to say that the CVERC doesn't like what it sees in public.

Highlighting what those governments already know about past leaks of USG/FVEY spying is likely aimed at shaping narratives, but says more about CVERC's intent than anything the report may achieve.

As usual, and as SentinelLabs has previously written, the report is paired with propaganda coverage but, for the first time, has also been published in Japanese, French, and German, in addition to English and Chinese.

CHINA

DAKOTA CARY

Dakota Cary is a China-focused consultant at SentinelOne and a nonresident fellow at the Atlantic Council's Global China Hub. Dakota previously was a research analyst at Georgetown University's Center for Security and Emerging Technology on the CyberAI Project. He focuses on China's efforts to develop its hacking capabilities. His reports examine artificial intelligence and cybersecurity research at Chinese universities, the People's Liberation Army's efforts to automate software vulnerability discovery, China's vulnerability collection system, and policies to improve the country's cybersecurity-talent pipeline. He has been featured and quoted on his expertise in a variety of outlets, including The Economist, MIT Technology Review, Associated Press, Financial Times, and Wired. Cary has also testified before the US-China Economic and Security Review Commission.