



| Brief |

Chinese Threat Actors Targeting Semiconductor Firms

B-2023-10-18a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Malware, Vulnerability, Geopolitical & Physical, Threat Actor Targeting

October 18, 2023

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 9:00 AM (EDT) on October 18, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Chinese Threat Actors Targeting Semiconductor Firms

› Key Findings

- ZeroFox identified recent reports of a new Chinese state-sponsored threat actor conducting cyber espionage campaigns against semiconductor firms in Taiwan, Hong Kong, and Singapore.
- ZeroFox assesses this threat actor may be sharing the sensitive data obtained with the China Communist Party (CCP) so it can be reverse-engineered and replicated.
- ZeroFox anticipates that Chinese APT groups are very likely to conduct future cyber espionage campaigns targeting the global semiconductor industry.

| Analyst Commentary

Over the past several weeks, a new Chinese state-sponsored threat actor has been observed to be conducting a cyber espionage campaign targeting semiconductor firms in Taiwan, Hong Kong, and Singapore.¹ This activity was attributed to a Chinese APT group due to the overlap in tactics, techniques, and procedures (TTPs). Specifically, the use of a HyperBro malware² variant to install Cobalt Strike beacons with a Taiwan Semiconductor Manufacturing (TSMC) PDF in a phishing lure correlates to the TTPs of Chinese threat

¹

[hXXps://blog.electiciq\[.\]com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia#a2](https://blog.electiciq[.]com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia#a2)

² [hXXps://attack.mitre\[.\]org/software/S0398/](https://attack.mitre[.]org/software/S0398/)

actor APT27.³ This activity is significant because it shows the emergence of newer China-based APT groups focused on cyber espionage in the technology sector. As part of its 14th five-year plan, China is attempting to advance its in-house manufacturing of semiconductors in order to be independent of other countries, decouple from global supply chains, and become a leader in semiconductor manufacturing.⁴

These operations are also consistent with previous activity by various Chinese state-sponsored APTs engaged in cyber espionage to infiltrate semiconductor manufacturing firms and gain access to intellectual property (IP). From February 2023 to May 2023, a separate and previously unknown Chinese APT group (now known as “Grayling”) used customized malware and open-source tools to exploit CVE-2019-0803,⁵ targeting a number of organizations in Taiwan's manufacturing sector.⁶ Taiwan's manufacturing sector focuses on semiconductor and semiconductor-related technologies manufacturing.⁷ The exploitation of CVE-2019-0803 is notable because it is listed in CISA's Known Exploited Vulnerabilities (KEV) Catalog, meaning it is still an active indicator of compromise (IOC) for a legacy Microsoft product.⁸ Separately, Chinese threat actor APT41 also targeted two subsidiaries of an unnamed Asian conglomerate earlier this year, both operating in the materials and composites sector, including the semiconductor sub-sector.⁹

Once this sensitive information is obtained, these APT groups may share it with the CCP in order for the technology to be reverse-engineered and the IP to be replicated.¹⁰ This represents a threat to the national security of Western democracies, specifically the United States. Semiconductors are essential to all technologies, especially now in the age

³ [hXXps://attack.mitre\[.\]org/groups/G0027/](https://attack.mitre.org/groups/G0027/)

⁴ [hXXps://cset.georgetown\[.\]edu/publication/china-14th-five-year-plan/](https://cset.georgetown[.]edu/publication/china-14th-five-year-plan/)

⁵ [hXXps://nvd.nist\[.\]gov/vuln/detail/CVE-2019-0803](https://nvd.nist[.]gov/vuln/detail/CVE-2019-0803)

⁶ [hXXps://symantec-enterprise-blogs.security\[.\]com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks](https://symantec-enterprise-blogs.security[.]com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks)

⁷

[hXXps://www.forbes\[.\]com/sites/katharinabuchholz/2023/01/13/advanced-microchip-production-relies-on-taiwan/?sh=488aa9da371d](https://www.forbes[.]com/sites/katharinabuchholz/2023/01/13/advanced-microchip-production-relies-on-taiwan/?sh=488aa9da371d)

⁸

[hXXps://support.microsoft\[.\]com/en-us/topic/description-of-the-security-update-for-the-win32k-elevation-of-privilege-vulnerability-in-windows-server-2008-windows-embedded-posready-2009-and-windows-embedded-standard-2009-july-10-2018-f82533d1-628f-4dcf-b05d-2990991d11f5](https://support.microsoft[.]com/en-us/topic/description-of-the-security-update-for-the-win32k-elevation-of-privilege-vulnerability-in-windows-server-2008-windows-embedded-posready-2009-and-windows-embedded-standard-2009-july-10-2018-f82533d1-628f-4dcf-b05d-2990991d11f5)

⁹ [hXXps://symantec-enterprise-blogs.security\[.\]com/blogs/threat-intelligence/blackfly-espionage-materials](https://symantec-enterprise-blogs.security[.]com/blogs/threat-intelligence/blackfly-espionage-materials)

¹⁰ [hXXps://cset.georgetown\[.\]edu/publication/chinas-progress-in-semiconductor-manufacturing-equipment/](https://cset.georgetown[.]edu/publication/chinas-progress-in-semiconductor-manufacturing-equipment/)

of artificial intelligence (AI).¹¹ With more sophisticated technology, the CCP may aim to strengthen its military and defense, have the ability to set global standards, and dominate critical supply chains.

Forward Look

ZeroFox researchers assess that the global semiconductor industry, which is estimated to be worth about one trillion dollars by 2030,¹² will very likely continue to be targeted by Chinese APT groups. High-tech ecosystems with innovative semiconductor firms (such as in Taiwan, South Korea, Singapore, the United States, and Europe) are likely to be targeted since they have the most advanced semiconductor manufacturing capabilities and a large share of IP. Verticals of the semiconductor industry—such as prominent universities and government research labs specializing in semiconductor research and development—are also likely to be targeted. Although Chinese state-sponsored APT groups have relied on certain malware families in the past, ZeroFox researchers assess that newer and lesser-known Chinese APT groups are likely to shift to different TTPs. In particular, these APT groups are likely to use open-source tools and exploit critical and widespread vulnerabilities in future cyber espionage campaigns targeting the global semiconductor industry.

To mitigate these threats, organizations should:

- Implement effective email protection solutions to mitigate phishing campaigns.
- Conduct training and awareness for employees to recognize phishing emails.
- Implement multi-factor authentication (MFA) to prevent unauthorized access to sensitive information (in the event that credentials are compromised).
- Develop and implement an effective incident response plan (IRP).
- Conduct continuous scanning and monitoring of attempted port scans, vulnerabilities, and suspicious activity on devices.
- Implement an effective anti-virus (AV) solution.

¹¹ [hXXps://www.voanews\[.\]com/a/fbi-warns-about-china-theft-of-us-ai-technology/7202760.html](https://www.voanews.com/a/fbi-warns-about-china-theft-of-us-ai-technology/7202760.html)

¹²

[hXXps://www.mckinsey\[.\]com/industries/semiconductors/our-insights/the-semiconductor-decade-a-trillion-dollar-industry](https://www.mckinsey.com/industries/semiconductors/our-insights/the-semiconductor-decade-a-trillion-dollar-industry)

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE 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.	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 MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	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.
	Green	Clear
WHEN SHOULD IT BE 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.	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 MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix C: 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 occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with 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%