Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

# Taiwan's Semiconductor Firms Under Siege by Chinese Cyber Operations

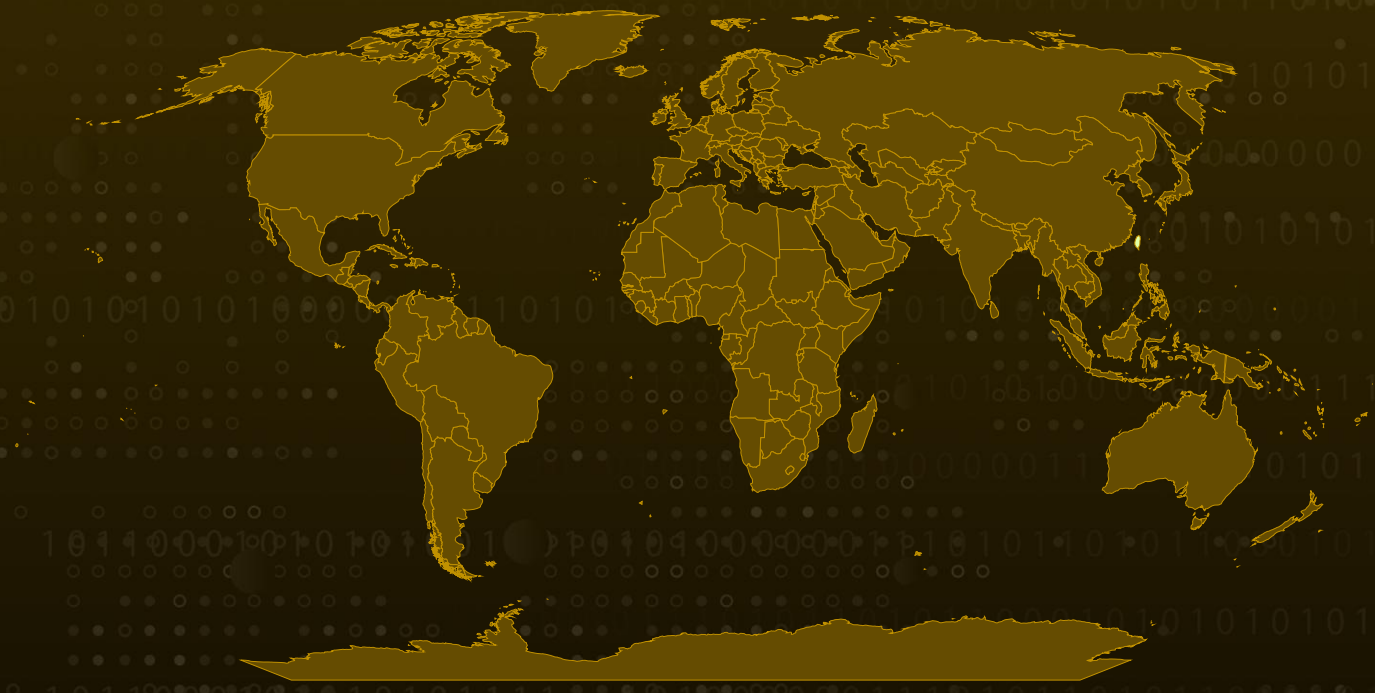

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| July 18, 2025 | A1 | TA2025225 |

# Summary

**Attack Commenced:** March 2025
**Backdoor:** Voldemort, HealthKick
**Targeted Region:** Taiwan
**Targeted Industry:** Semiconductor

**Attack:** Chinese state-sponsored threat groups launched a wave of sophisticated cyber-espionage attacks targeting Taiwan's semiconductor industry. These campaigns used spear-phishing tactics to breach firms and aimed to extract sensitive data and intellectual property. Featuring unique malware strains and deceptive lures, the operations mark a sharp escalation in China's strategic push for semiconductor dominance amid tightening global trade restrictions.

## Attack Regions



# Attack Details

**#1** A wave of cyber-espionage campaigns targeted Taiwan's semiconductor industry between March and June 2025, orchestrated by three Chinese state-sponsored threat actors. These operations, attributed to clusters tracked as UNK_FistBump, UNK_DropPitch, and UNK_SparkyCarp, mark a significant escalation in China's covert efforts against one of Taiwan's most strategically vital economic sectors.

**#2** The attacks extended beyond semiconductor manufacturers to encompass a broader range of entities across the industry's ecosystem. This included organizations involved in design, testing, and equipment supply, as well as financial analysts with expertise in the Taiwanese semiconductor market.

**#3** Driven by China's pursuit of semiconductor self-sufficiency particularly in response to increasing U.S. and Taiwanese export restrictions these campaigns demonstrated a high degree of precision and technical sophistication. UNK_FistBump, employed employment-themed phishing emails targeting human resources personnel at Taiwanese semiconductor firms. These messages, sent from compromised university accounts, carried password-protected archives containing malware.

**#4** Victim systems were typically infected with either Cobalt Strike Beacon or a custom backdoor known as Voldemort, deployed through dual infection chains. UNK_DropPitch focused its efforts on financial analysts by impersonating fictitious investment firms.

**#5** Through social engineering, the group distributed weaponized documents that launched either the HealthKick backdoor or basic reverse shells communicating with attacker-controlled infrastructure. Obfuscation techniques such as FakeTLS headers were used to evade detection and complicate attribution.

**#6** UNK_SparkyCarp leveraged an Adversary-in-the-Middle (AitM) phishing kit to harvest login credentials, underscoring a focus on credential theft as a means of establishing deeper access. In a related campaign traced to October 2024, another China-aligned group, UNK_ColtCentury, deployed benign-looking emails likely intended to deliver SparkRAT malware.

**#7** Collectively, these operations reflect a clear advancement in both the capabilities and strategic intent of Chinese cyber threat actors. While several tactics resembled those employed by established groups such as TA415 (APT41), the campaigns also featured distinct methods that set these newly identified clusters apart.

# Recommendations

**Enhance Email Security:** Deploy advanced filtering and sandboxing to detect spearphishing, especially emails with spoofed domains or password-protected attachments. Keep detection rules updated to reflect emerging threats.

**Adopt Zero Trust Security Models:** Apply a Zero Trust approach to user access and network segmentation, ensuring that even if credentials are compromised, lateral movement is limited. Use multifactor authentication and restrict access to sensitive design, IP, and financial systems.

**Monitor and Control Command and Control Traffic:** Detect beaconing patterns, especially HTTP/S traffic mimicking FakeTLS or covert channels. Block outbound connections to known malicious C2 domains and IPs.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0001** Initial Access | **TA0002** Execution | **TA0003** Persistence | **TA0004** Privilege Escalation |
| **TA0005** Defense Evasion | **TA0006** Credential Access | **TA0007** Discovery | **TA0008** Lateral Movement |
| **TA0009** Collection | **TA0011** Command and Control | **TA0010** Exfiltration | **T1566** Phishing |
| **T1566.001** Spearphishing Attachment | **T1566.002** Spearphishing Link | **T1557** Adversary-in-the-Middle | **T1078** Valid Accounts |
| **T1059** Command and Scripting Interpreter | **T1203** Exploitation for Client Execution | **T1053** Scheduled Task/Job | **T1543** Create or Modify System Process |
| **T1055** Process Injection | **T1068** Exploitation for Privilege Escalation | **T1027** Obfuscated Files or Information | **T1555** Credentials from Password Stores |

| | | | |
|---|---|---|---|
| **T1083** File and Directory Discovery | **T1046** Network Service Discovery | **T1005** Data from Local System | **T1071** Application Layer Protocol |
| **T1071.001** Web Protocols | **T1105** Ingress Tool Transfer | **T1041** Exfiltration Over C2 Channel | **T1574.001** DLL |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| IPv4 | 166[.]88[.]61[.]35,<br>80[.]85[.]156[.]234,<br>82[.]118[.]16[.]72,<br>45[.]141[.]139[.]222,<br>80[.]85[.]156[.]237,<br>80[.]85[.]154[.]48 |
| URLs | hxxps[:]//sheets[.]googleapis[.]com[:]443/v4/spreadsheets/1z8ykHVYh9DF-b_BFDA9c4Q2ojfrgl-fq1v797Y5576Y,<br>hxxps[:]//sheets[.]googleapis[.]com[:]443/v4/spreadsheets/14H0Gm6xgc2p3gpIB5saDyzSDqpVMKGBKIdkVGh2y1bo,<br>hxxps[:]//3008[.]filemail[.]com/api/file/get?filekey=DeHjMusPPgDt5EsWxOcgYCfRh5yI6MIIg7vvwn9yFEzh93Cts5UxrfXMYEPiMWffVCp36UCsVgYSlC47WGdjHZ7m9bAw0QWcgqQZcg&pk_vid=007318ac7ca53d8717482475404ed5a2,<br>hxxps[:]//api[.]moctw[.]info/Intro[.]pdf,<br>hxxps[:]//api[.]moctw[.]info/Document-2025[.]4[.]25[.]pdf,<br>hxxps[:]//api[.]moctw[.]info/Install[.]zip,<br>hxxps[:]//brilliant-bubblegum-137cfe[.]netlify[.]app/files/Introduction%20Document[.]zip,<br>hxxps[:]//ttot[.]accshieldportal[.]com/v3/ls/click/?c=b5c64761,<br>hxxps[:]//aqrm[.]accshieldportal[.]com/v2/account/validate/?vid=35f46f46,<br>hxxps[:]//acesportal[.]com/T/bfzWhb,<br>hxxps[:]//acesportal[.]com/T/KRfzAH |
| Email | john[.]doe89e[@]gmail[.]com,<br>amelia_w_chavez[@]proton[.]me,<br>lisan_0818[@]outlook[.]com,<br>menglunwuluegg226[@]proton[.]me,<br>lonelyboymaoxcz231[@]proton[.]me |
| Domains | moctw[.]info,<br>ema[.]moctw[.]info, |

| TYPE | VALUE |
| --- | --- |
| Domains | www[.]twmoc[.]info, accshieldportal[.]com, acesportal[.]com |
| SHA256 | 1a2530010ecb11f0ce562c0db0380416a10106e924335258ccbba0071a19c852, 084b92365a25e6cd5fc43efe522e5678a2f1e307bf69dd9a61eb37f81f304cc6, 85e4809e80e20d9a532267b22d7f898009e74ed0dbf7093bfa9a8d2d5403f3f9, 338f072cc1e08f1ed094d88aa398472e3f04a8841be2ff70f1c7a2e4476d8ef7, 13fad7c6d0accb9e0211a7b26849cf96c333cf6dfa21b40b65a7582b79110e4b, d783c40c0e15b73b62f28d611f7990793b7e5ba2436e203000a22161e0a00d0e, 1016ba708fb21385b12183b3430b64df10a8a1af8355b27dd523d99ca878ffbb, 13fad7c6d0accb9e0211a7b26849cf96c333cf6dfa21b40b65a7582b79110e4b, 1016ba708fb21385b12183b3430b64df10a8a1af8355b27dd523d99ca878ffbb, bab8618bc6fc3fdfa7870b5fe0f52b570fabf0243d066f410a7e76ebeed0088c, 0d992762c69d624a1f14a8a230f8a7d36d190b49e787fd146e9010e943c5ef78, ec5fef700d1ed06285af1f2d01fa3db5ea924de3c2da2f0e6b7a534f69d8409c, 82ecfe0ada6f7c0cea78bca2e8234241f1a1b8670b5b970df5e2ee255c3a56ef, cd009ea4c682b61963210cee16ed663eee20c91dd56483d456e03726e09c89a7, bbdad59db64c48f0a9eb3e8f2600314b0e3ebd200e72fa96bf5a84dd29d64ac5, fc8f7185a90af4bf44332e85872aa7c190949e3ec70055a38af57690b6604e3c, 7bffd21315e324ef7d6c4401d1bf955817370b65ae57736b20ced2c5c08b9814, 9b2cbcf2e0124d79130c4049f7b502246510ab681a3a84224b78613ef322bc79, 4ee77f1261bb3ad1d9d7114474a8809929f4a0e7f9672b19048e1b6ac7acb15c, d3a71c6b7f4be856e0cd66b7c67ca0c8eef250bc737a648032d9d67c2c37d911, 366d7de8a941daa6a303dc3e39af60b2ffacaa61d5c1fb84dd1595a636439737, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | d51c195b698c411353b10d5b1795cbc06040b663318e220a2d121727c0bb4e43, ffd69146c5b02305ac74c514cab28d5211a473a6c28d7366732fdc4797425288 |

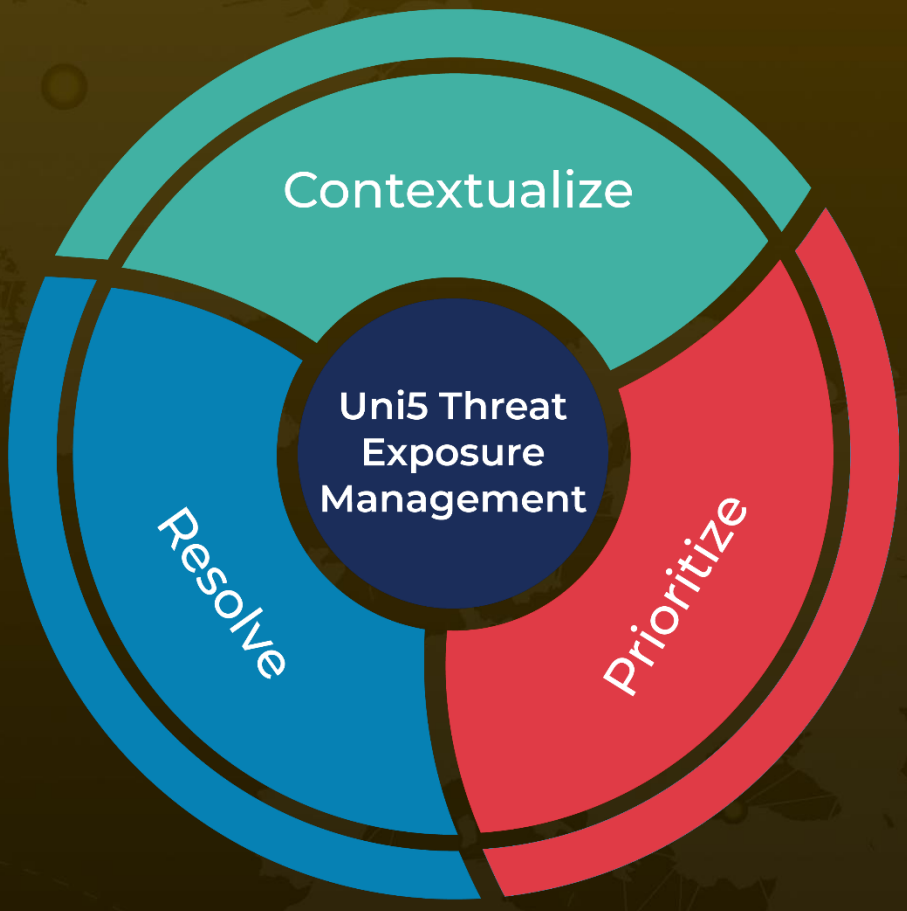
## References

https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**July 18, 2025 • 10:30 AM**



More at www.hivepro.com