Phish and Chips: China-Aligned Espionage Actors Ramp Up Taiwan Semiconductor Industry Targeting

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

July 11, 2025

Key findings

- Between March and June 2025, Proofpoint Threat Research observed three Chinese state-sponsored threat actors conduct targeted phishing campaigns against the Taiwanese semiconductor industry. In all cases, the motive was most likely espionage.
- Targets of these campaigns ranged from organizations involved in the manufacturing, design, and testing of semiconductors and integrated circuits, wider equipment and services supply chain entities within this sector, as well as financial investment analysts specializing in the Taiwanese semiconductor market.
- This activity likely reflects China's strategic priority to achieve semiconductor self-sufficiency and decrease reliance on international supply chains and technologies, particularly in light of US and Taiwanese export controls.

Overview

Analyst note: Proofpoint uses the UNK_ designator to define clusters of activity that are still developing and have not been observed for long enough to receive a numerical TA designation.

China-aligned threat actors have routinely targeted the semiconductor industry for many years. This activity likely aligns with China's internal strategic economic priorities, which have increasingly emphasized the importance of semiconductor technologies in successive national economic development initiatives, including the Five-Year Plans. A growing focus on ensuring strategic self-reliance for semiconductor technologies, accelerated by external pressures from export controls, has likely reinforced the priority of intelligence collection operations directed at this industry. This is reflected in China-aligned espionage activity tracked by the Proofpoint Threat Research team, where we are currently observing an elevated level of targeting of the industry by China-aligned groups compared to historical activity.

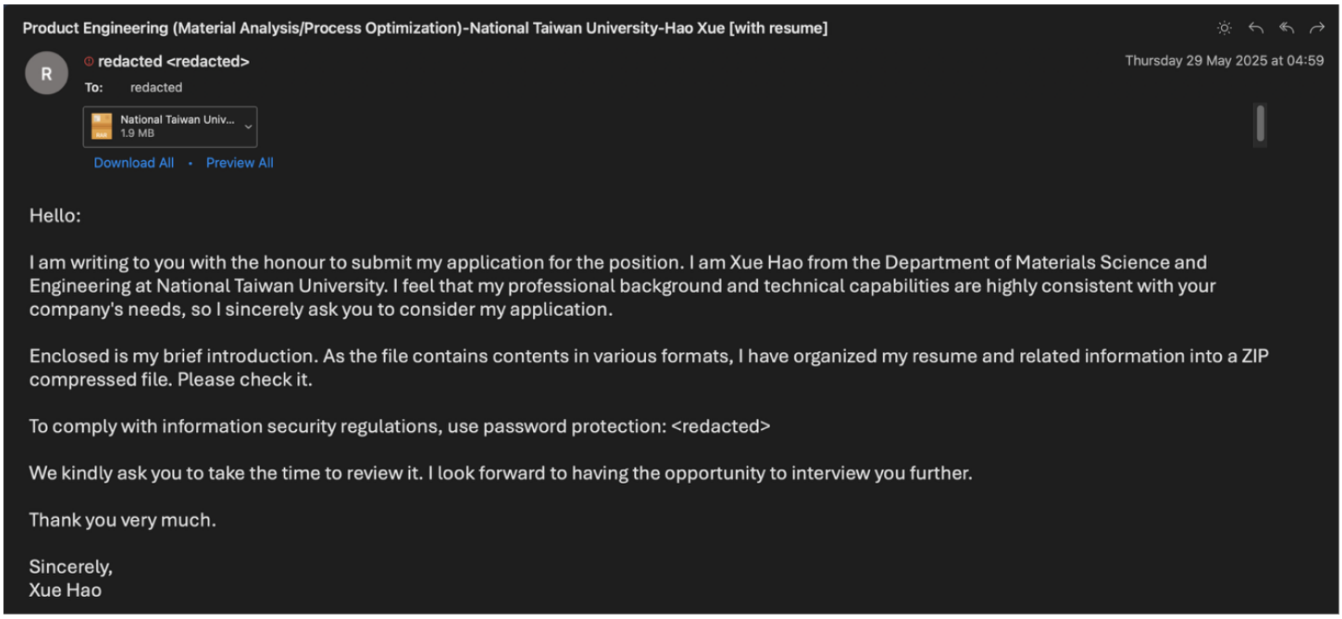
Between March and June 2025, Proofpoint identified multiple China-aligned threat actors specifically targeting Taiwanese organizations within the semiconductor industry. This included a China-aligned threat actor tracked as UNK_FistBump targeting semiconductor design, manufacturing, and supply chain organizations in employment-themed phishing campaigns resulting in the delivery of Cobalt Strike or the custom Voldemort backdoor.

Additionally, Proofpoint observed another China-aligned threat actor tracked as UNK_DropPitch targeting individuals in multiple major investment firms who specialize in investment analysis specifically within the Taiwanese semiconductor industry. This UNK_DropPitch targeting is exemplary of intelligence collection priorities spanning less obvious areas of the semiconductor ecosystem beyond just design and manufacturing entities. Finally, we also observed an actor tracked as UNK_SparkyCarp conducting credential phishing activity against a Taiwanese semiconductor company using a custom Adversary in the Middle (AiTM) phishing kit.

UNK_FistBump targets semiconductor manufacturing and supply chain with job seeking lures

In May and June 2025, Proofpoint observed UNK_FistBump conducting multiple spearphishing campaigns targeting Taiwan-based semiconductor manufacturing, packaging, testing, and supply chain organizations. Posing as a graduate student seeking employment, the actor used compromised Taiwanese university email addresses to send their phishing email to recruitment and HR personnel. Subject lines observed across this activity include the following:

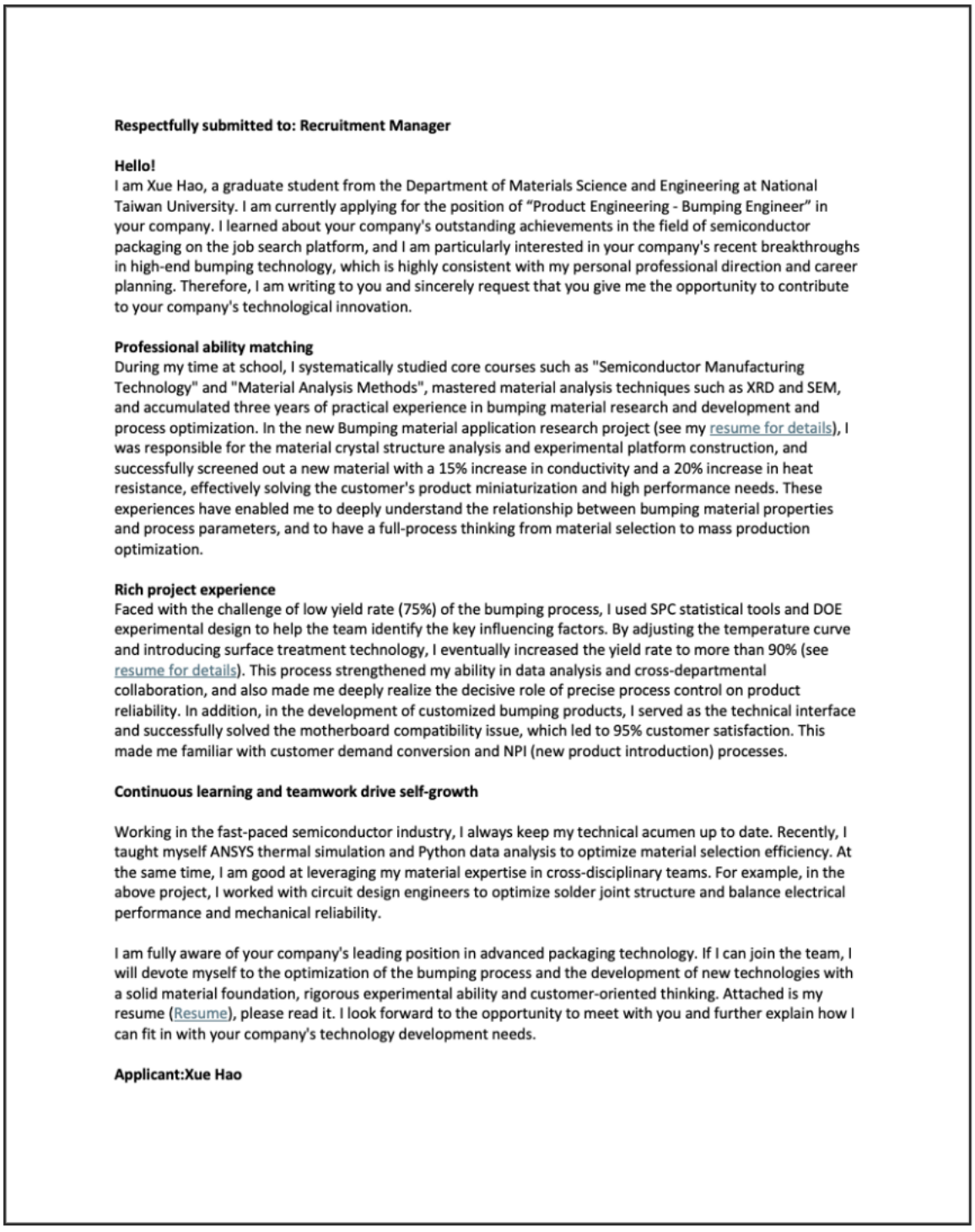
- 產品工程（材料分析/製程優化）-台灣大學-薛豪 [附履歷] (Machine Translation: Product Engineering (Material Analysis/Process Optimization) - National Taiwan University - Xue Hao [with resume])
- Bumping工程師-台灣大學-材料工程學類-薛豪 (Machine Translation: Bumping Engineer-National Taiwan University-Material Engineering-Xue Hao)
- 【重要】麻煩協助確認 (Machine translation: [Important] Please help confirm)



Example UNK_FistBump job application phishing email (machine translated from Traditional Chinese).

Delivery

UNK_FistBump phishing emails were sent via a likely compromised account and contained either a password-protected archive attachment or a PDF attachment. The PDF attachments contained URLs leading to an archive file hosted on either a Zendesk instance or the Filemail file sharing service. Earlier UNK_FistBump campaigns delivered a Cobalt Strike Beacon payload, but the group shifted to delivery of the custom Voldemort backdoor in late May 2025.



Respectfully submitted to: Recruitment Manager

Hello!
I am Xue Hao, a graduate student from the Department of Materials Science and Engineering at National Taiwan University. I am currently applying for the position of "Product Engineering - Bumping Engineer" in your company. I learned about your company's outstanding achievements in the field of semiconductor packaging on the job search platform, and I am particularly interested in your company's recent breakthroughs in high-end bumping technology, which is highly consistent with my personal professional direction and career planning. Therefore, I am writing to you and sincerely request that you give me the opportunity to contribute to your company's technological innovation.

Professional ability matching
During my time at school, I systematically studied core courses such as "Semiconductor Manufacturing Technology" and "Material Analysis Methods", mastered material analysis techniques such as XRD and SEM, and accumulated three years of practical experience in bumping material research and development and process optimization. In the new Bumping material application research project (see my resume for details), I was responsible for the material crystal structure analysis and experimental platform construction, and successfully screened out a new material with a 15% increase in conductivity and a 20% increase in heat resistance, effectively solving the customer's product miniaturization and high performance needs. These experiences have enabled me to deeply understand the relationship between bumping material properties and process parameters, and to have a full-process thinking from material selection to mass production optimization.

Rich project experience
Faced with the challenge of low yield rate (75%) of the bumping process, I used SPC statistical tools and DOE experimental design to help the team identify the key influencing factors. By adjusting the temperature curve and introducing surface treatment technology, I eventually increased the yield rate to more than 90% (see resume for details). This process strengthened my ability in data analysis and cross-departmental collaboration, and also made me deeply realize the decisive role of precise process control on product reliability. In addition, in the development of customized bumping products, I served as the technical interface and successfully solved the motherboard compatibility issue, which led to 95% customer satisfaction. This made me familiar with customer demand conversion and NPI (new product introduction) processes.

Continuous learning and teamwork drive self-growth

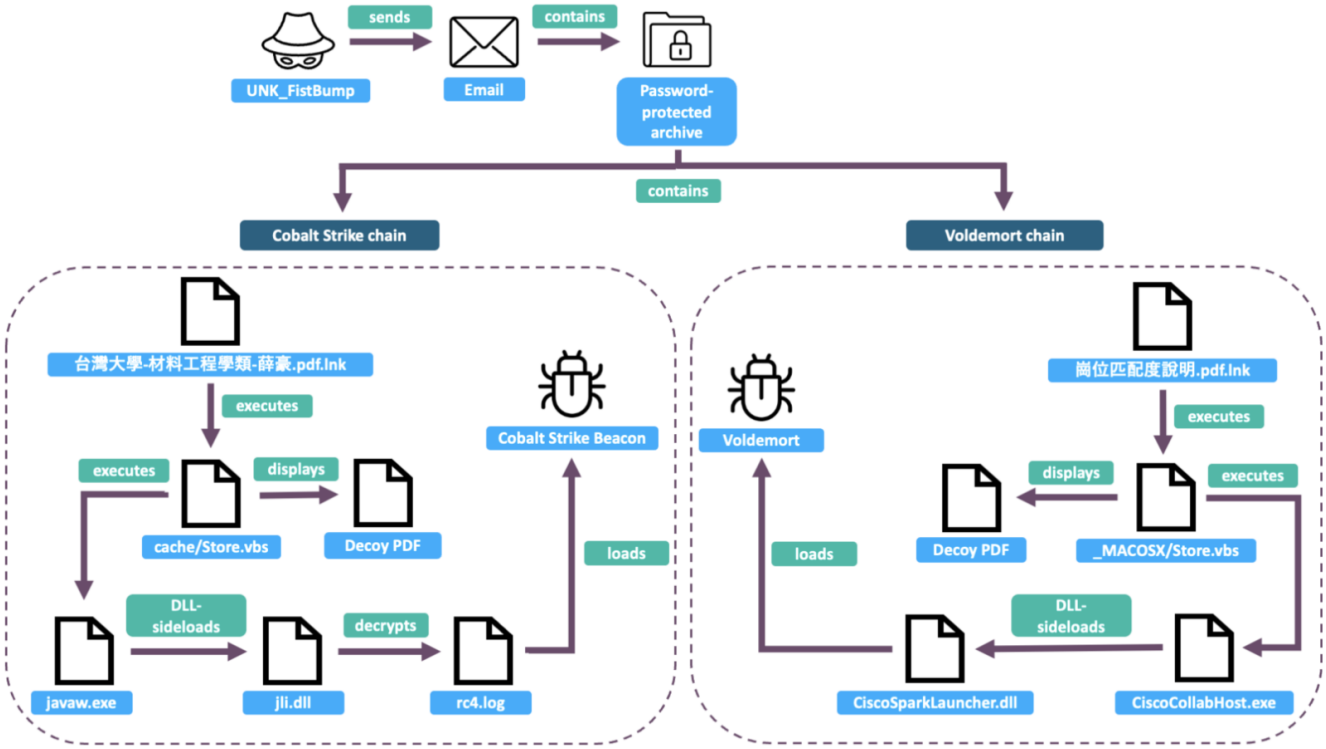
Working in the fast-paced semiconductor industry, I always keep my technical acumen up to date. Recently, I taught myself ANSYS thermal simulation and Python data analysis to optimize material selection efficiency. At the same time, I am good at leveraging my material expertise in cross-disciplinary teams. For example, in the above project, I worked with circuit design engineers to optimize solder joint structure and balance electrical performance and mechanical reliability.

I am fully aware of your company's leading position in advanced packaging technology. If I can join the team, I will devote myself to the optimization of the bumping process and the development of new technologies with a solid material foundation, rigorous experimental ability and customer-oriented thinking. Attached is my resume (Resume), please read it. I look forward to the opportunity to meet with you and further explain how I can fit in with your company's technology development needs.

Applicant:Xue Hao

UNK_FistBump PDF attachment leading to file sharing site (machine translated from Traditional Chinese).

In an unusual campaign in late May 2025, UNK_FistBump included two distinct infection chains beginning with the same password-protected archive, one of which loaded a Cobalt Strike Beacon payload, and the second loading Voldemort. These infection chains were initially triggered by distinct Microsoft Shortcut (LNK) files.



UNK_FistBump RAR archive containing two distinct infection chains.

_MACOSX	5/29/2025 7:02 AM	File folder	
cache	5/28/2025 3:58 PM	File folder	
.DS_Store	5/29/2025 7:07 AM	DS_STORE File	7 KB
im02	5/27/2025 2:55 PM	JPG File	431 KB
im03	5/27/2025 2:57 PM	JPG File	608 KB
台灣大學-材料工程學類-薛豪.pdf	5/16/2025 6:16 PM	Shortcut	2 KB
崗位匹配度說明.pdf	5/28/2025 4:18 PM	Shortcut	2 KB

Contents of job application zip containing two distinct infection chains.

Infection chain 1: Cobalt Strike payload

Execution of the first LNK file named 崗位匹配度說明.pdf.lnk runs a VBS script Store.vbs stored within the cache subfolder. This folder contains the following files:

- cache/Store.vbs
- cache/javaw.exe
- cache/崗位匹配度說明.pdf
- cache/rc4.log
- cache/jli.dll

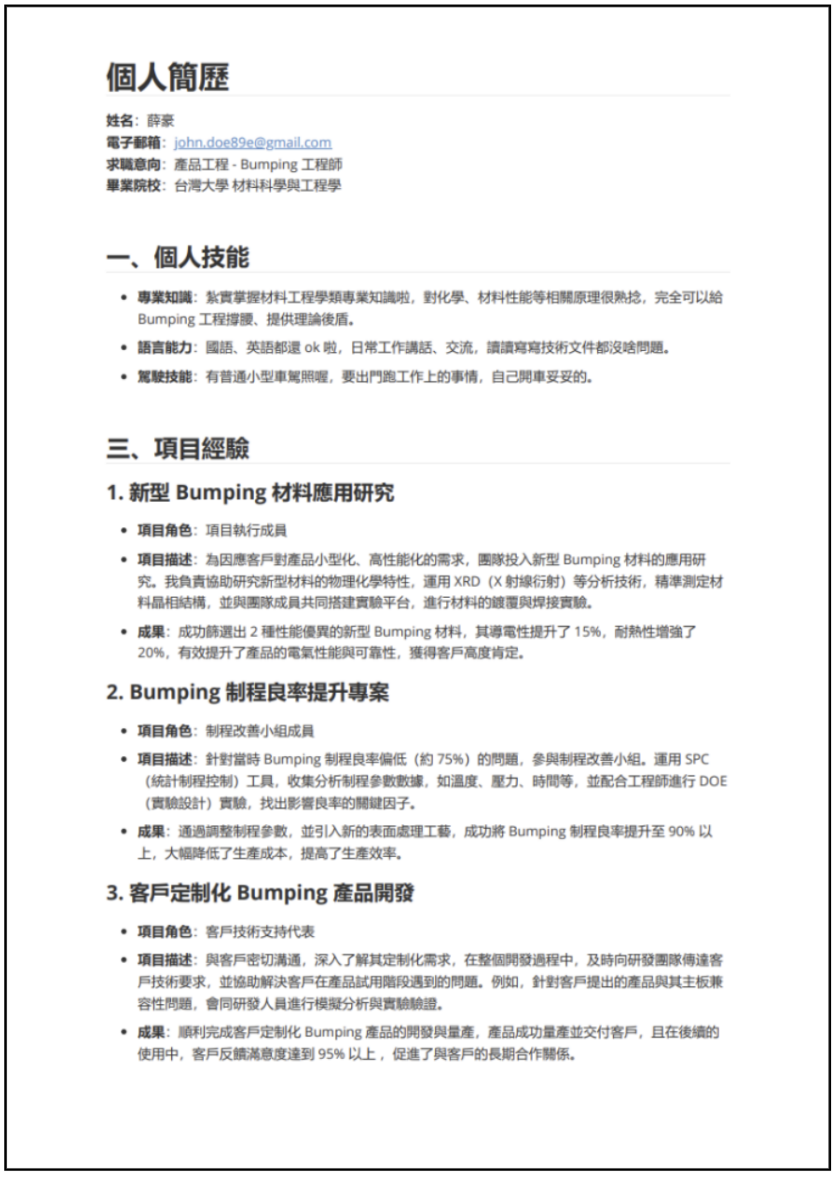
This Store.vbs script copies the files javaw.exe, jli.dll, and rc4.log to the C:\Users\Public\Videos directory and opens a decoy document named 崗位匹配度說明.pdf (machine translation: Explanation of Job Compatibility.pdf). It then executes the benign signed executable javaw.exe, which is vulnerable to DLL-sideloading. This loads the malicious DLL jli.dll, which in turn decrypts the RC4-encrypted Cobalt Strike Beacon payload from the rc4.log file using the key qwxsfvdtv and loads it into memory. The Cobalt Strike Beacon payload uses a customized GoToMeeting malleable C2 profile and communicates with the Evoxt VPS C2 IP address 166.88.61[.]35 over port TCP 443. The jli.dll loader also establishes persistence by setting a HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run key value for runs to the path of the DLL sideloading executable javaw.exe.

Infection chain 2: Voldemort payload

Execution of the second LNK named 台灣大學-材料工程學類-薛豪.pdf.lnk runs another VBS file also called Store.vbs, this time within the MACOSX subfolder. This MACOSX folder contains the following files:

- _MACOSX/Store.vbs
- _MACOSX/台灣大學-材料工程學類-薛豪.pdf
- _MACOSX/CiscoSparkLauncher.dll
- _MACOSX/CiscoCollabHost.exe
- _MACOSX/Cisco.xml

Similar to the Cobalt Strike infection chain, the Store.vbs script copies the malicious executable files to C:\Users\Public\Videos and opens a different decoy document 台灣大學-材料工程學類-薛豪.pdf (Machine translation: National Taiwan University - Materials Engineering - Xue Hao.pdf). It then executes the benign signed executable CiscoCollabHost.exe, which is vulnerable to DLL sideloading and loads the malicious DLL CiscoSparkLauncher.dll. This DLL sideloading chain results in the delivery of the custom Voldemort backdoor, which uses Google Sheets for command and control (C2).



個人簡歷

姓名：薛豪
電子郵箱：john.doe89e@gmail.com
求職意向：產品工程 - Bumping 工程師
畢業院校：台灣大學 材料科學與工程學

一、個人技能

- **專業知識**：紮實掌握材料工程學類專業知識啦，對化學、材料性能等相關原理很熟捻，完全可以給 Bumping 工程撐腰、提供理論後盾。
- **語言能力**：國語、英語都還 ok 啦，日常工作講話、交流，讀讀寫寫技術文件都沒啥問題。
- **駕駛技能**：有普通小型車駕照喔，要出門跑工作上的事情，自己開車妥妥的。

三、項目經驗

1. 新型 Bumping 材料應用研究

- **項目角色**：項目執行成員
- **項目描述**：為因應客戶對產品小型化、高性能化的需求，團隊投入新型 Bumping 材料的應用研究。我負責協助研究新型材料的物理化學特性，運用 XRD（X 射線衍射）等分析技術，精準測定材料晶相結構，並與團隊成員共同搭建實驗平台，進行材料的鍍覆與焊接實驗。
- **成果**：成功篩選出 2 種性能優異的新型 Bumping 材料，其導電性提升了 15%，耐熱性增強了 20%，有效提升了產品的電氣性能與可靠性，獲得客戶高度肯定。

2. Bumping 制程良率提升專案

- **項目角色**：制程改善小組成員
- **項目描述**：針對當時 Bumping 制程良率偏低（約 75%）的問題，參與制程改善小組。運用 SPC（統計制程控制）工具，收集分析制程參數數據，如溫度、壓力、時間等，並配合工程師進行 DOE（實驗設計）實驗，找出影響良率的關鍵因子。
- **成果**：通過調整制程參數，並引入新的表面處理工藝，成功將 Bumping 制程良率提升至 90% 以上，大幅降低了生產成本，提高了生產效率。

3. 客戶定制化 Bumping 產品開發

- **項目角色**：客戶技術支持代表
- **項目描述**：與客戶密切溝通，深入了解其定制化需求，在整個開發過程中，及時向研發團隊傳達客戶技術要求，並協助解決客戶在產品試用階段遇到的問題。例如，針對客戶提出的產品與其主板兼容性問題，會同研發人員進行模擬分析與實驗驗證。
- **成果**：順利完成客戶定制化 Bumping 產品的開發與量產，產品成功量產並交付客戶，且在後續的使用中，客戶反饋滿意度達到 95% 以上，促進了與客戶的長期合作關係。

UNK_FistBump resume decoy document.

The specific Voldemort DLL sideloading infection chain and payload observed closely resembles one used by the China state-sponsored threat actor TA415 (APT41, Brass Typhoon), as previously documented by Proofpoint. An earlier Voldemort variation used by UNK_FistBump in May 2025 exfiltrated host information in plain text to the Google Sheets C2, while a later variation Base64-encoded and RC4-encrypted the values using the executable's filename as the RC4 key (CiscoCollabHost.exe) in an identical manner previously highlighted in TA415 activity.

Examining UNK_FistBump and TA415 attribution overlaps

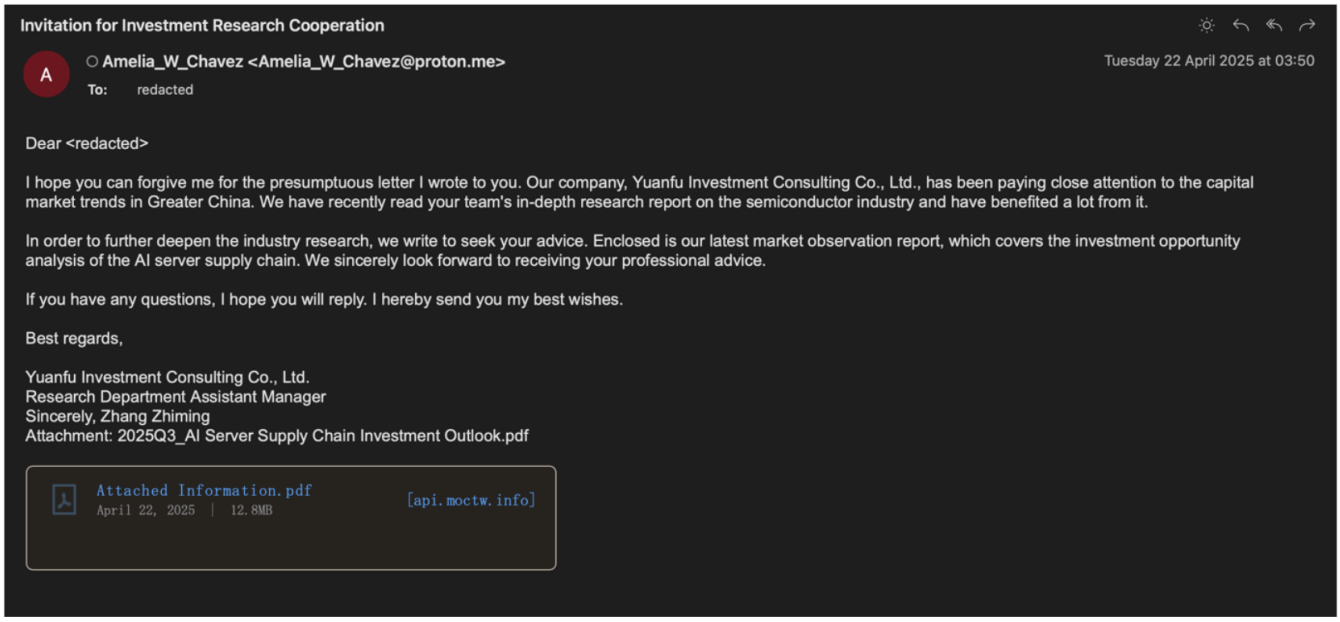
Voldemort is a custom malware family publicly reported by Proofpoint and Google that was historically only used by TA415 within Proofpoint telemetry. Proofpoint Threat Research also previously observed TA415 conducting spearphishing campaigns targeting the Taiwanese semiconductor sector using compromised Taiwanese university senders, in a similar manner to the highlighted UNK_FistBump activity.

However, the observed UNK_FistBump campaigns diverge from activity typically tracked as TA415. For example, the Cobalt Strike infection chain uses a loader not typical of TA415, which usually favors ChaCha20-based loaders rather than the more simplistic RC4 loader used by UNK_FistBump. Similarly, the use of a hardcoded IP address for a C2, rather than a Cloudflare Worker or actor-controlled domain behind Cloudflare CDN, is atypical of TA415 activity. Due to these and other divergences, coupled with the wider propensity of custom capability sharing across Chinese cyberespionage threat actors, Proofpoint is tracking UNK_FistBump activity as distinct to TA415 at this time.

UNK_DropPitch pitches semiconductor investment analysts

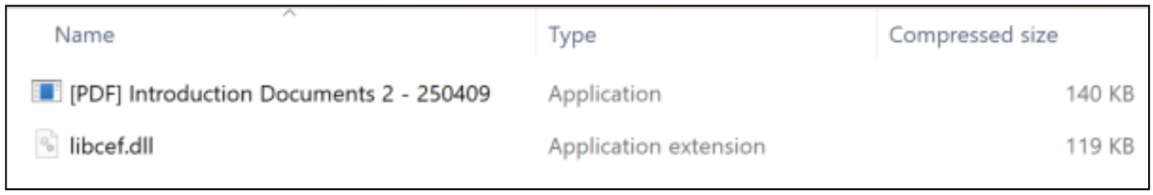
In April and May 2025, Proofpoint observed another China-aligned threat actor tracked as UNK_DropPitch conducting targeted phishing campaigns against multiple large investment banks. This activity focused specifically on individuals specializing in financial investment analysis of Taiwanese semiconductor and technology sectors. The phishing emails were sent from attacker-owned email addresses and purported to come from a fictitious financial investment firm seeking to collaborate with the individual.

Delivery



Example UNK_DropPitch investment research collaboration phishing email (machine translated from Traditional Chinese).

In a campaign observed in late April 2025, an UNK_DropPitch phishing email contained a link to hxxps://api[.]moctw[.]info/Intro.pdf. This resulted in the download of a file named Intro.zip containing both a benign executable vulnerable to DLL-sideloading and a malicious DLL libcef.dll, which are designed to load a simple custom backdoor Proofpoint tracks as HealthKick.



UNK_DropPitch Intro.zip contents.

Upon execution, both files are copied to a randomly named subfolder under the ProgramData directory and the following scheduled task named SystemHealthMonitor is created to execute [PDF] Introduction Documents 2 - 250409.exe every five minutes:

```
schtasks.exe /Create /TN "SystemHealthMonitor" /TR "\"C:\ProgramData\zumArSAB\[PDF] Introduction Documents 2 - 250409.Exe\" -run" /SC MINUTE /MO 5 /F
```

The HealthKick backdoor then attempts to create a web socket to the actor-controlled IP address 82.118.16[.]72 over TCP port 465. HealthKick employs a FakeTLS protocol and expects a response from the C2 starting with the magic bytes 0x17 0x03 0x03 (the standard header for TLSv1.2), followed by the payload size. Due to the way the malware verifies that incoming packets start with these magic bytes and

then later verifies this again, the FakeTLS header needs to be included twice for commands to be properly parsed and decoded, it is unclear if this was an intended feature or a mistake. This double FakeTLS header is then followed by a payload which is XOR encoded with the key mysecretkey.

Example Command:

17 03 03 00 20 17 03 03 00 1b 0e 14 17 4b 06 0a 00 54 44
06 59 08 1a 1b 0a 43 1a 00 18 07 0a 59 1a 16 01 09 07

Malware Response:

17 03 03 00 12 17 03 03 00 1d 05 1c 1f 09 0c 52 12 1b 19
09 1d 60 73

HealthKick TCP socket C2 communication.

HealthKick is a simple backdoor that executes commands and captures their output via a redirected anonymous pipe, which is then sent back to the C2 using the same FakeTLS and XOR-encoded payload format.

A later UNK_DropPitch campaign in late May 2025 linked to the Netlify URL https://brilliant-bubblegum-137cfe[.]netlify[.]app/files/Introduction%20Document.zip

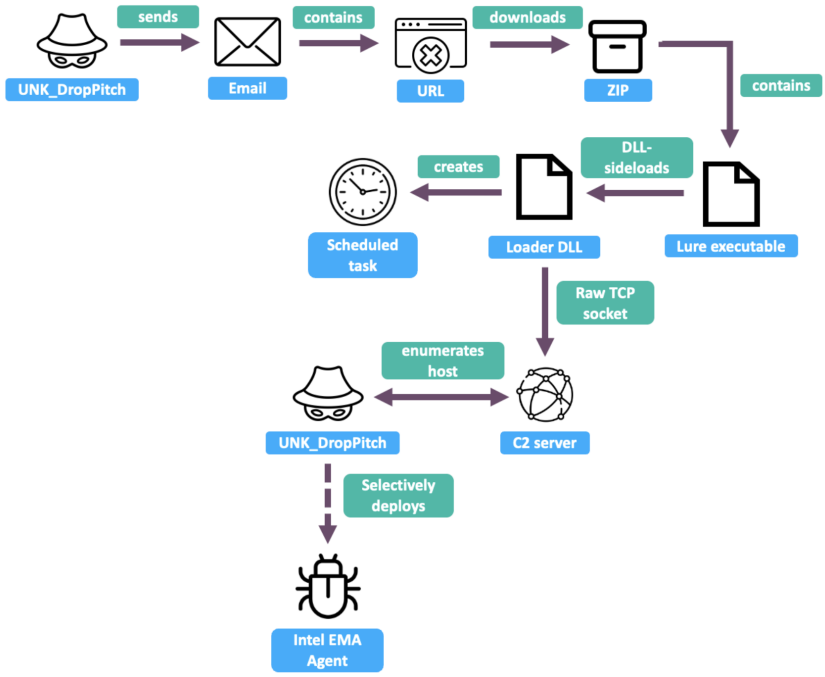
and again delivered a ZIP file containing an executable used to load a malicious DLL named pbvm90.dll. In this case, the resultant malware is a simple raw TCP reverse shell that communicates with the actor-controlled VPS server 45.141.139[.]222 again over TCP port 465 and persists via an identical scheduled task to the one noted above.

This reverse shell features minimal exception or error handling, meaning the server's response to the malware client connecting ("Server ready") is interpreted as a command by the implant. Similarly, the reverse shell sends regular "ping" messages to its C2 as a heartbeat. Similar "ping" check ins were also received back from the C2 and often concatenated with the operator's commands, resulting in errors. Proofpoint also observed typos in the command responses from the operators, indicating the commands are likely issued manually rather than in an automated fashion.

```
Client connected

Server ready

Command received
'Server' is not recognized as an internal or external command,
operable program or batch file.

<<<END>>>

ipconfig

Command received

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.160
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

<<<END>>>
ping
pingpingcd C:/

Command received
'pingpingcd' is not recognized as an internal or external command,
operable program or batch file.

<<<END>>>
ping
cd C:?

Command received
Failed to change directory. Error code: 123
<<<END>>>

cd C:/

Command received
Directory changed successfully.
<<<END>>>
```

UNK_DropPitch reverse shell errors and typos.

Proofpoint observed UNK_DropPitch using this reverse shell to conduct initial enumeration and discovery against targets. Subsequently, if the target is deemed of interest, the group dropped the Remote Monitoring and Management (RMM) tool Intel Endpoint Management Assistant (EMA), which was configured to communicate with the actor-controlled domain ema.moctw[.]info.



UNK_DropPitch infection chain.

UNK_DropPitch network infrastructure analysis

Both the 82.118.16[.]72 HealthKick backdoor C2 IP address and 80.85.156[.]234 Intel EMA C2 server used very similar reverse DNS names associated with the Russian VPS hosting provider ProfitServer and referenced the Mr. Robot character Elliot Alderson:

- elliot-alderson-971.pserver[.]space
- elliot-alderson-97.pserver[.]space

Multiple similarly named email addresses have also been used by the threat actor. Pivoting on this artifact uncovered additional likely actor-controlled servers, several of which were used as C2 servers in subsequent June 2025 UNK_DropPitch campaigns targeting US academic and think tank organizations:

- 31.192.234[.]97 (elliot-alderson-15.pserver[.]space)
- 80.85.154[.]48 (elliot-alderson-973.pserver[.]space)
- 80.85.154[.]101 (elliot-alderson-151.pserver[.]space)
- 80.85.156[.]237 (elliot-alderson-974.pserver[.]space)
- 80.85.157[.]116 (elliot-alderson-972.pserver[.]space)
- 80.85.157[.]145 (elliot-alderson-978.pserver[.]space)
- 82.118.16[.]72 (elliot-alderson-971.pserver[.]space)
- 82.118.16[.]106 (elliot-alderson-972.pserver[.]space)

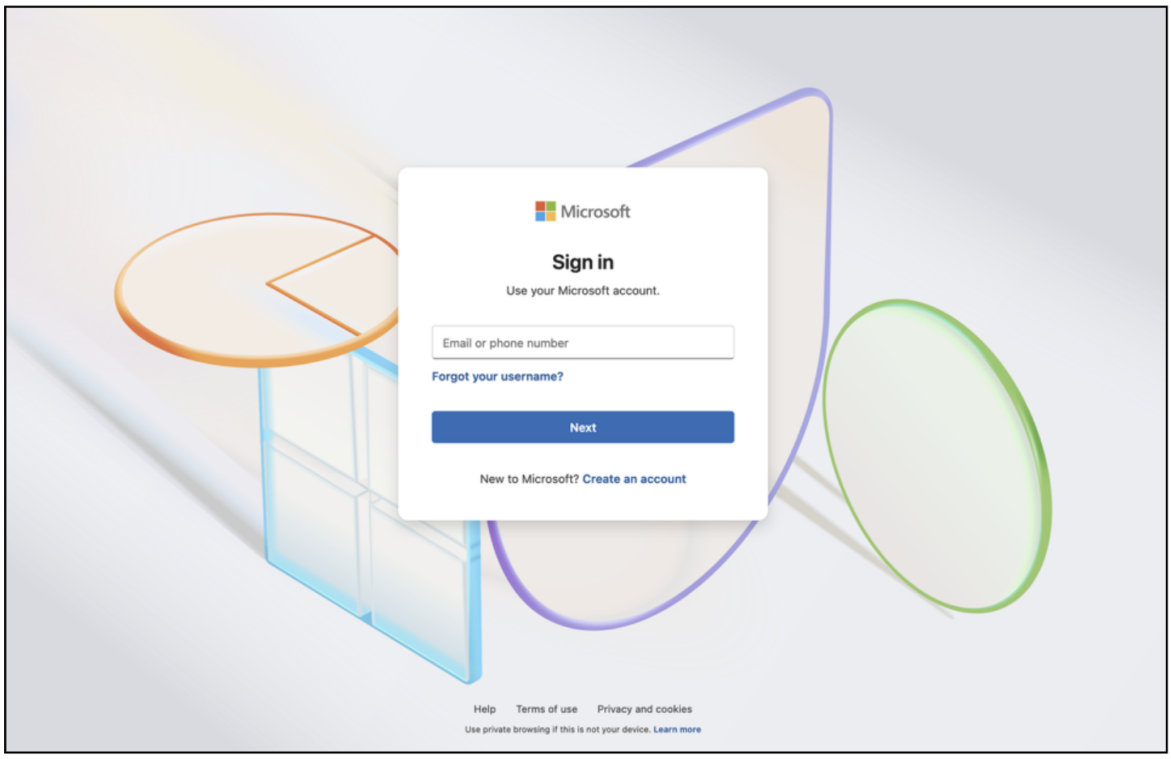
Two of these servers were concurrently configured as SoftEther VPN servers, an open-source VPN product commonly used by a range of China-aligned threat actors for both infrastructure administration and tunnelling traffic out of victim networks. The hosting IP address for the UNK_DropPitch subdomain mx.moctw[.]info (43.247.132[.]96) was also configured as a SoftEther VPN server during time of use.

The 80.85.154[.]101 IP address identified above concurrently exhibited a TLS certificate with the common name CN=AS.website (SHA256 fingerprint: 000062e9e212231328b660f759f8878ac47604b9609f71c05ad19d7ef56b17a8) on port TCP 4444. This certificate has been historically associated exhibited on C2 infrastructure associated with multiple custom malware families used by Chinese state-sponsored threat actors, most frequently the SideWalk (aka ScrambleCross) backdoor. The TLS certificate was also noted in Kaspersky reporting on the MoonBounce firmware rootkit and PWC reporting on TA415 (APT41, Brass Typhoon) activity, both in relation to SideWalk usage. At this time, Proofpoint analysts were unable to determine conclusively if the reuse of this TLS certificate is an artifact of a specific custom malware family shared across multiple China-aligned threat actors, most likely SideWalk, or of shared infrastructure provisioning across these groups.

Additional China-aligned threat actors targeting Taiwanese semiconductor industry

In addition to the highlighted UNK_FistBump and UNK_DropPitch activity, Proofpoint has also identified multiple additional Chinese state-sponsored threat actors specifically targeting organizations within Taiwan's semiconductor industry.

In March 2025, a China-aligned threat actor Proofpoint tracks as UNK_SparkyCarp conducted a credential phishing campaign using a custom adversary-in-the-middle (AITM) framework targeting a Taiwanese semiconductor industry company, which the group also previously targeted in November 2024. The phishing emails masqueraded as account login security warnings and contained a link to the actor-controlled credential phishing domain accshieldportal[.]com, as well as a tracking beacon URL for acesportal[.]com.



Typical UNK_SparkyCarp AITM phishing kit landing page.

Similarly, in October 2024 Proofpoint observed the China aligned threat actor UNK_ColtCentury (overlaps TAG-100, Storm-2077) sending benign conversation starter emails to legal personnel at a Taiwanese semiconductor organization in an attempt to engage the target. Based on related activity associated with this threat actor, this was likely an attempt to deploy the SparkRAT backdoor.

Conclusion

Within Proofpoint telemetry in recent years, traditional espionage targets – including governments, aerospace and defense companies, and non-governmental organizations – have continued to be consistently targeted by China-aligned espionage threat actors. Despite public reporting on semiconductor targeting from China-aligned threat actors, Proofpoint directly observed only sporadic targeting of this sector. Since March 2025, this shifted to sightings of multiple campaigns from different China-aligned groups specifically targeting this sector, with a particular emphasis on Taiwanese entities.

As many well-established China-aligned threat actors have shifted tactics, techniques and procedures (TTPs) towards exploitation of edge devices and other initial access vectors, Proofpoint has observed an influx of new China-aligned clusters to the phishing threat landscape, as demonstrated by the subset of activity highlighted within this report. These emerging threat actors continue to exhibit long-standing targeting patterns consistent with Chinese state interests, as well as TTPs and custom capabilities historically associated with China-aligned cyberespionage operations.

Indicators of compromise

UNK_FistBump Network Indicators
Indicator
166.88.61[.]35

hxxps://sheets[.]googleapis[.]com:443/v4/spreadsheets/1z8ykHVYh9DF-b_BFDA9c4Q2ojfrgl-fq1v797Y5576Y
hxxps://sheets[.]googleapis[.]com:443/v4/spreadsheets/14H0Gm6xgc2p3gpIB5saDyzSDqpVMKGBKIdkVGh2y1bo
john.doe89e@gmail[.]com
hxxps://3008[.]filemail[.]com/api/file/get? filekey=DeHjMusPPgDt5EsWxOcgYCfRh5yI6MIIg7vvwn9yFEzh93Cts5UxrfXMYEPiMWffVCp36UCsVgYSlC47WGdjHZ7m9bAw0QWcgqQZcg&p
UNK_FistBump Malware Indicators
1a2530010ecb11f0ce562c0db0380416a10106e924335258ccbba0071a19c852
084b92365a25e6cd5fc43efe522e5678a2f1e307bf69dd9a61eb37f81f304cc6
85e4809e80e20d9a532267b22d7f898009e74ed0dbf7093bfa9a8d2d5403f3f9
338f072cc1e08f1ed094d88aa398472e3f04a8841be2ff70f1c7a2e4476d8ef7
13fad7c6d0accb9e0211a7b26849cf96c333cf6dfa21b40b65a7582b79110e4b
d783c40c0e15b73b62f28d611f7990793b7e5ba2436e203000a22161e0a00d0e
1016ba708fb21385b12183b3430b64df10a8a1af8355b27dd523d99ca878ffbb
13fad7c6d0accb9e0211a7b26849cf96c333cf6dfa21b40b65a7582b79110e4b
1016ba708fb21385b12183b3430b64df10a8a1af8355b27dd523d99ca878ffbb
bab8618bc6fc3fdfa7870b5fe0f52b570fabf0243d066f410a7e76ebeed0088c
0d992762c69d624a1f14a8a230f8a7d36d190b49e787fd146e9010e943c5ef78
ec5fef700d1ed06285af1f2d01fa3db5ea924de3c2da2f0e6b7a534f69d8409c
82ecfe0ada6f7c0cea78bca2e8234241f1a1b8670b5b970df5e2ee255c3a56ef

cd009ea4c682b61963210cee16ed663eee20c91dd56483d456e03726e09c89a7
bbdad59db64c48f0a9eb3e8f2600314b0e3ebd200e72fa96bf5a84dd29d64ac5
fc8f7185a90af4bf44332e85872aa7c190949e3ec70055a38af57690b6604e3c

UNK_DropPitch Network Indicators

Indicator	Type	Description	First Seen
amelia_w_chavez@proton[.]me	Email	Malware delivery	April 2025
lisan_0818@outlook[.]com	Email	Malware delivery	May 2025
moctw[.]info	Domain	Malware delivery	April 2025
hxxps://api[.]moctw[.]info/Intro.pdf	URL	Malware delivery	April 2025
hxxps://api[.]moctw[.]info/Document-2025.4.25.pdf	URL	Malware delivery	April 2025
hxxps://api[.]moctw[.]info/Install.zip	URL	Malware delivery	April 2025
hxxps://brilliant-bubblegum-137cfe[.]netlify[.]app/files/Introduction%20Document.zip	URL	Malware delivery	May 2025
ema.moctw[.]info	Domain	C2	April 2025
www.twmoc[.]info	Domain	C2	June 2025
80.85.156[.]234	IP Address	C2	April 2025
82.118.16[.]72	IP Address	C2	April 2025
45.141.139[.]222	IP Address	C2	May 2025
80.85.156[.]237	IP Address	C2	June 2025
80.85.154[.]48	IP Address	C2	June 2025

UNK_DropPitch Malware Indicators

7bffd21315e324ef7d6c4401d1bf955817370b65ae57736b20ced2c5c08b9814	SHA256	Intro.zip	April 2025
9b2cbcf2e0124d79130c4049f7b502246510ab681a3a84224b78613ef322bc79	SHA256	libcef.dll	April 2025
4ee77f1261bb3ad1d9d7114474a8809929f4a0e7f9672b19048e1b6ac7acb15c	SHA256	libcef.dll	April 2025
d3a71c6b7f4be856e0cd66b7c67ca0c8eef250bc737a648032d9d67c2c37d911	SHA256	[PDF] Introduction Document-2025.4.25.lnk	April 2025
366d7de8a941daa6a303dc3e39af60b2ffacaa61d5c1fb84dd1595a636439737	SHA256	Introduction Document.zip	May 2025
d51c195b698c411353b10d5b1795cbc06040b663318e220a2d121727c0bb4e43	SHA256	[PDF]Taiwan-Cooperation-Introduction-Document-20250521.exe	May 2025
ffd69146c5b02305ac74c514cab28d5211a473a6c28d7366732fdc4797425288	SHA256	pbvm90.dll	May 2025

UNK_SparkyCarp Network Indicators			
accshieldportal[.]com	Domain	UNK_SparkyCarp credential phishing domain	March 2025
acesportal[.]com	Domain	Tracking pixel domain	March 2025
hxxps://ttot.accshieldportal[.]com/v3/ls/click/?c=b5c64761	URL	Credential phishing URL	March 2025
hxxps://aqrm.accshieldportal[.]com/v2/account/validate/?vid=35f46f46	URL	Credential phishing URL	March 2025
hxxps://acesportal[.]com/T/bfzWhb	URL	Tracking pixel URL	March 2025
hxxps://acesportal[.]com/T/KRfzAH	URL	Tracking pixel URL	March 2025
menglunwuluegg226@proton[.]me	Email	Malware delivery	March 2025
lonelyboymaoxcz231@proton[.]me	Email	Malware delivery	March 2025

ET rules

2063450 - ET HUNTING GoogleSheets API V4 Activity (Fetch Single Cell with A1 Notation)

2063451 - ET HUNTING GoogleSheets API V4 Response (Single Cell with UUID)

2063452 - ET HUNTING GoogleSheets API V4 Activity (Possible Exfil)

2063453 - ET MALWARE Voldemort System Info Exfil

2063454 - ET PHISHING Observed DNS Query to UNK_SparkyCarp Domain

2063455 - ET PHISHING Observed DNS Query to UNK_SparkyCarp Domain

2063456 - ET PHISHING Observed UNK_SparkyCarp Domain in TLS SNI

2063457 - ET MALWARE Observed DNS Query to UNK_DropPitch Domain

2063458 - ET MALWARE Observed UNK_DropPitch Domain in TLS SNI

2063459 - ET PHISHING Observed UNK_SparkyCarp Domain in TLS SNI

2063460 - ET MALWARE Observed DNS Query to UNK_DropPitch Domain

2063461 - ET MALWARE Observed UNK_DropPitch Domain in TLS SNI