TLP : CLEAR

HoldingHandsRAT Attacks against Japanese company

Toshiki Takeuchi
NEC Cyber Security Technical Division
Cyber Intelligence Group

What is HoldingHandsRAT

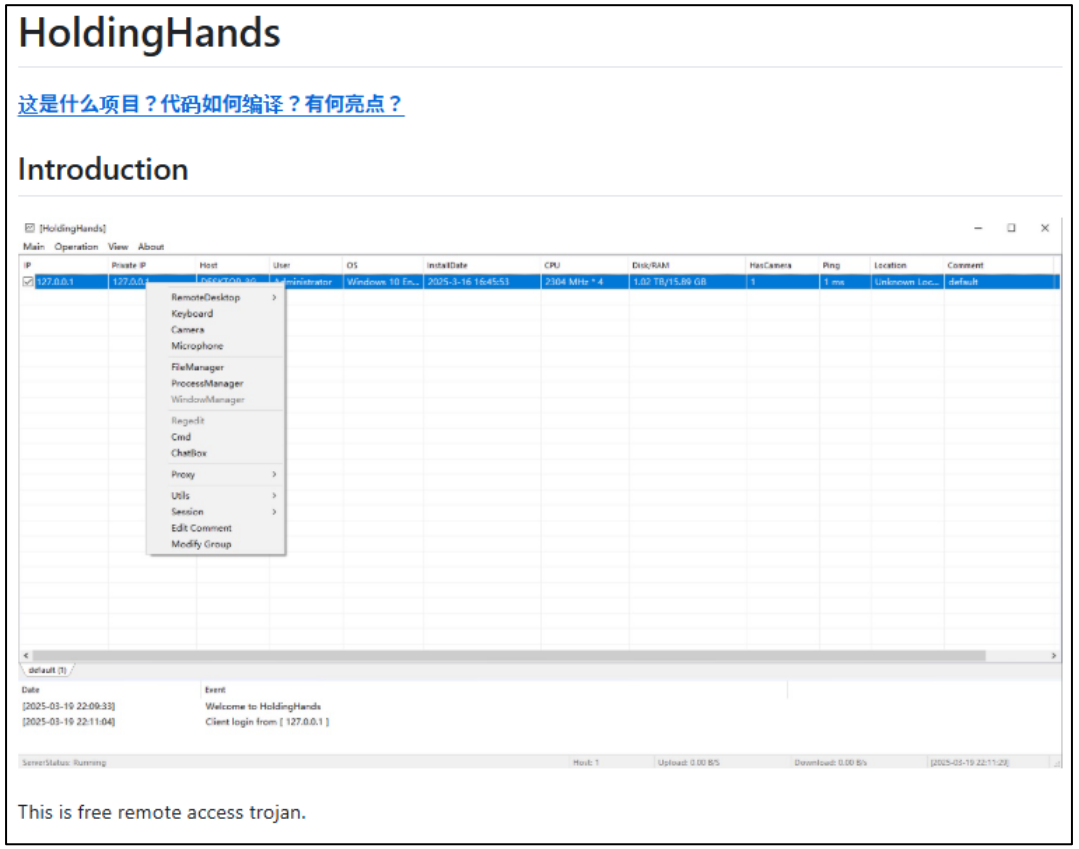
- HoldingHandsRAT was used in attacks against Taiwan, Japan, and Malaysia [1][2].

- The PDB path contains the words “HoldingHands-develop” and “BackDoor”.

```
D:¥Workspace¥HoldingHands-develop¥HoldingHands-develop¥Door¥x64¥Release¥BackDoor.pdb
```

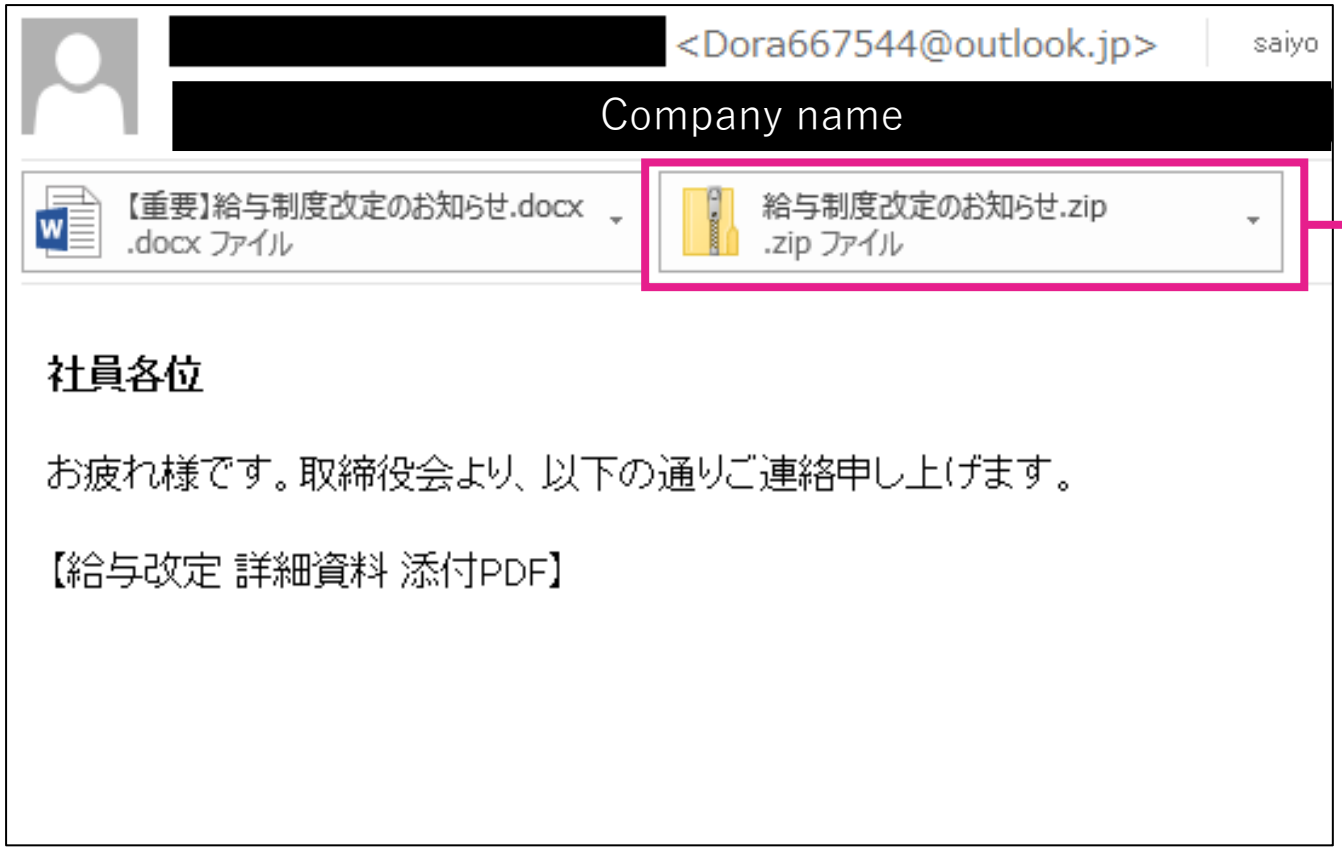
  We have found a GitHub repository for a RAT called HoldingHands [3]. The final payload is similar the one in this repository.

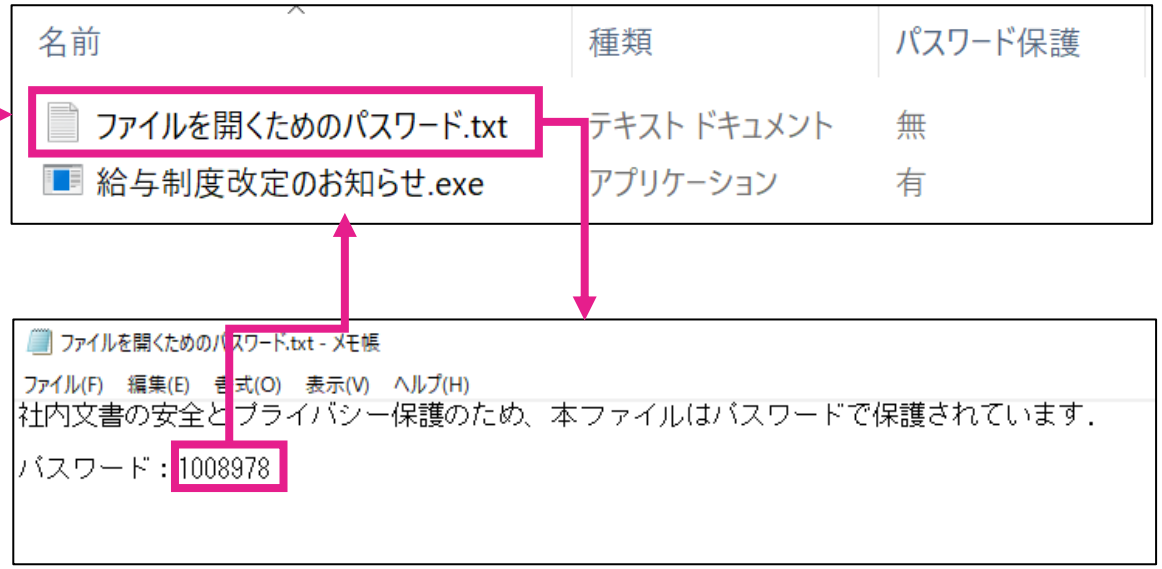
- In May 2025, we observed attack emails in Japanese aimed at infecting Japanese company with HoldingHandsRAT.



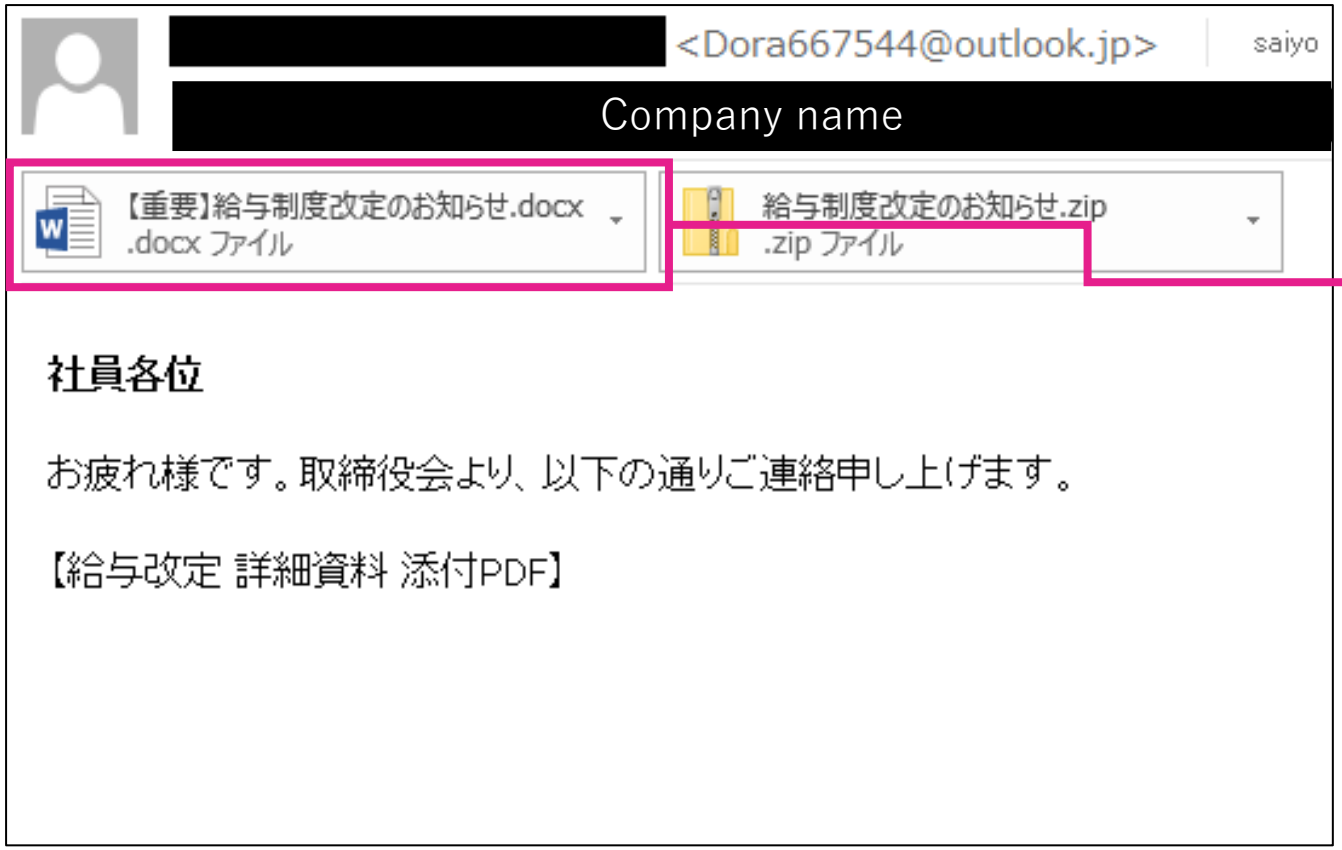
HoldingHands：https://github.com/yuanyuanxiang/HoldingHands

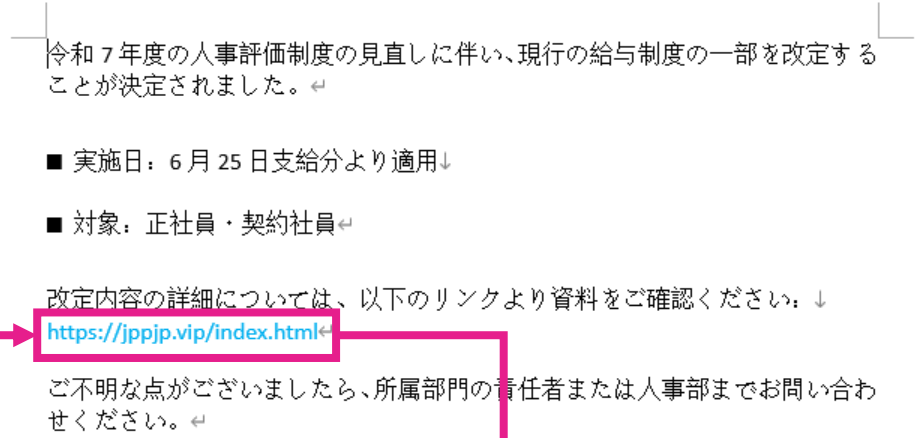
HoldingHandsRAT Attacks Against Japanese Company

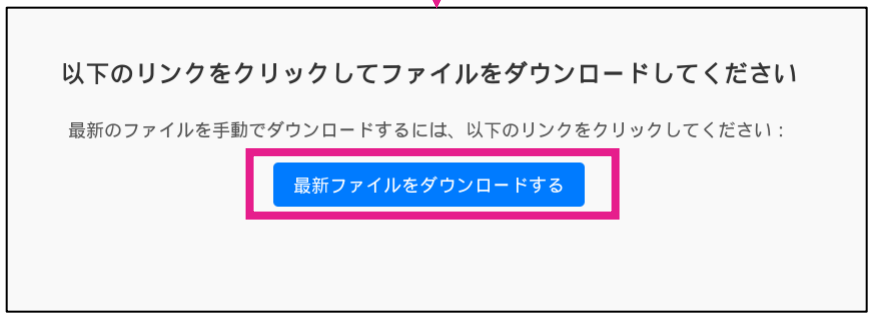




HoldingHandsRAT Attacks Against Japanese Company

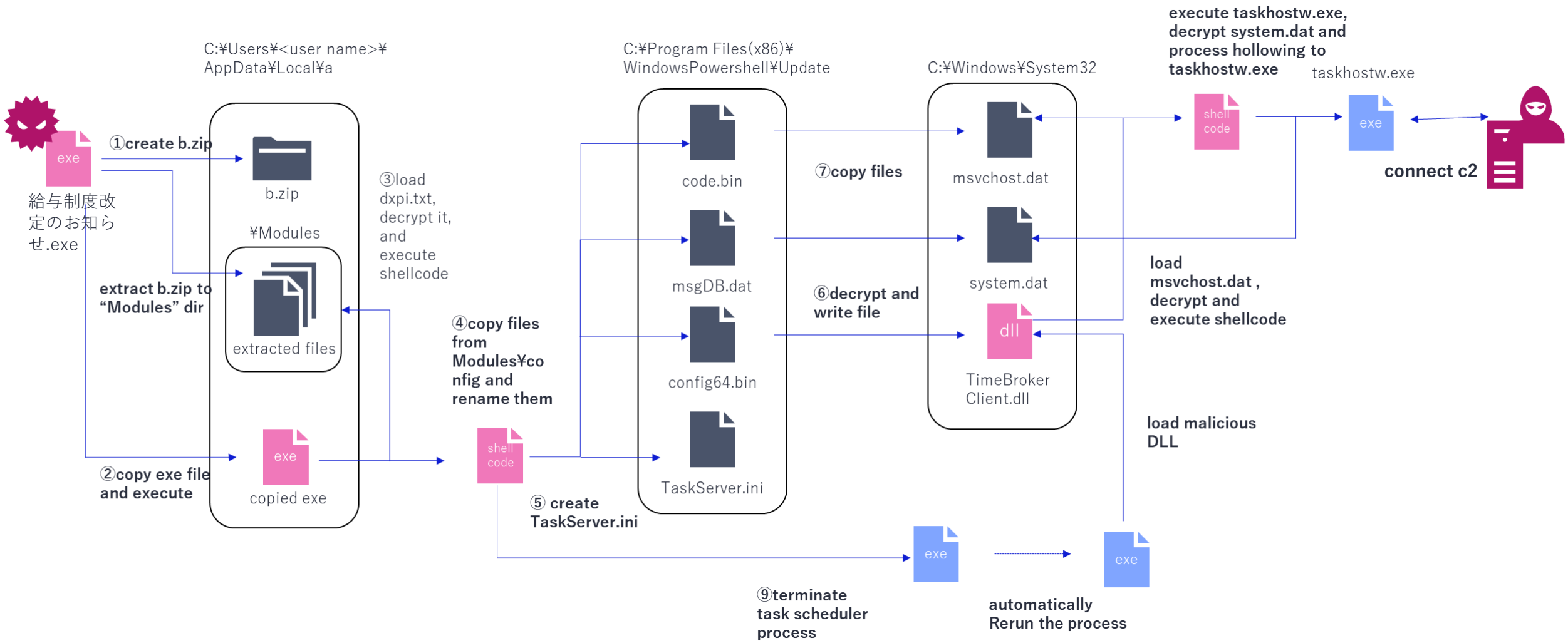






Download “給与制度改定のお知らせ.zip”
same as attached ZIP file.

The attack flow



Variant of HoldingHands

- The samples considered to have been used in the attacks on Japan had the following characteristics:
  - PDB：D:¥Workspace¥HoldingHands-develop¥HoldingHands-develop¥Door¥x64¥Release¥BackDoor.pdb
  - Signatures stolen from legitimate companies ：Sid Narayanan Ltd, ZELCORE TECHNOLOGIES INC.
  - Dropped files： C:¥Users¥<USER>¥AppData¥Local¥a¥b.zip

file name	SHA256	Signature	PDB
給与制度改定のお知らせ.exe	7102e9a86b47b65aeebc1bef98abe0928388f122af98eb62bf61622a42303f67	Sid Narayanan Ltd	D:¥Workspace¥HoldingHands-develop¥HoldingHands-develop¥Door¥x64¥Release¥BackDoor.pdb
異動一覧および配置図.exe	63c6d24be4e9d3da368c432ad15cb14be41f55cd33fc61119b8e036b9f0d1158		
異動のお知らせ.exe	6e71d405e1fed788fe5f31684711113ba1dcd52f8902fea1a4dcb659b635a2c0		
人事異動リスト.exe	5dc95bb3219bcebe86370c0a50e39ec4bafc5b1f25ac721010469a532d22a92e		
納税申告.exe	eb70f340769ad88c7a20679472b00389a760c4356ce1e1fb99e488bbeda1667c	ZELCORE TECHNOLOGIES INC.	

Related Domain & IP Addresses

- Obtaining a domain with the same name in a different TLD, or a similar domain with only one letter difference.
  - Attacks on Taiwan
    ex) twnic[.]ink, twnic[.]xin / twsww[.]xin, twswzz[.]xin
- Many of the resolved IP addresses for domains are in Japan

domain	Domain Create Date	Resolved IP Address	Autonomous System Label	Country
jppjp[.]vip[2][4]	2025/04/22 00:00:00	154.205.139[.]223	Kaopu Cloud HK Limited	JP
jppjp[.]xin	2025/04/22 00:00:00	38.60.212[.]39	Kaopu Cloud HK Limited	JP
jppjp[.]cc[4]	2025/04/22 03:47:43	107.148.0[.]149	PEG-TY	JP
jpjpz1[.]vip[4]	2025/04/22 00:00:00	154.205.139[.]195	Kaopu Cloud HK Limited	JP
jpjpz1[.]top[2][4]	2025/04/22 00:00:00	38.54.88[.]103	Kaopu Cloud HK Limited	JP
jpjpz1[.]cc[2]	2025/04/22 00:00:00	38.54.50[.]212	Kaopu Cloud HK Limited	US

What we learned

- In May 2025, an email attack was carried out against Japanese companies.
- Regarding the attached ZIP file, the EXE file is password protected, which is thought to be an attempt to avoid detection by security software.
- The signatures used may have been stolen from legitimate companies.
- Attackers acquire multiple domains with similar patterns at the same time. In addition, many of the resolved IP addresses are Japanese IP addresses, which is thought to be an attempt to avoid detection.

References

[1] Threat Group Targets Companies in Taiwan
https://www.fortinet.com/blog/threat-research/threat-group-targets-companies-in-taiwan
[2] Tracking Malware and Attack Expansion: A Hacker Group’s Journey across Asia
https://www.fortinet.com/blog/threat-research/tracking-malware-and-attack-expansion-a-hacker-groups-journey-across-asia
[3]HoldingHands
https://github.com/yuanyuanxiang/HoldingHands
[4] Multilingual ZIP Phishing Campaigns Targeting Financial and Government Organizations Across Asia
https://hunt.io/blog/multilingual-zip-phishing-campaigns-asia-financial-government

\Orchestrating a brighter world