变脸, Teng Snake (a.k.a. Code Core)

medium.com/s2wblog/变脸-teng-snake-a-k-a-code-core-8c35268b4d1a

S2W July 9, 2022

S2W

Jul 6

.

12 min read

Author: HOTSAUCE | S2W TALON

> *: July 6, 2022. : July 8, 2022.*

The profile picture of Teng Snake on Twitter

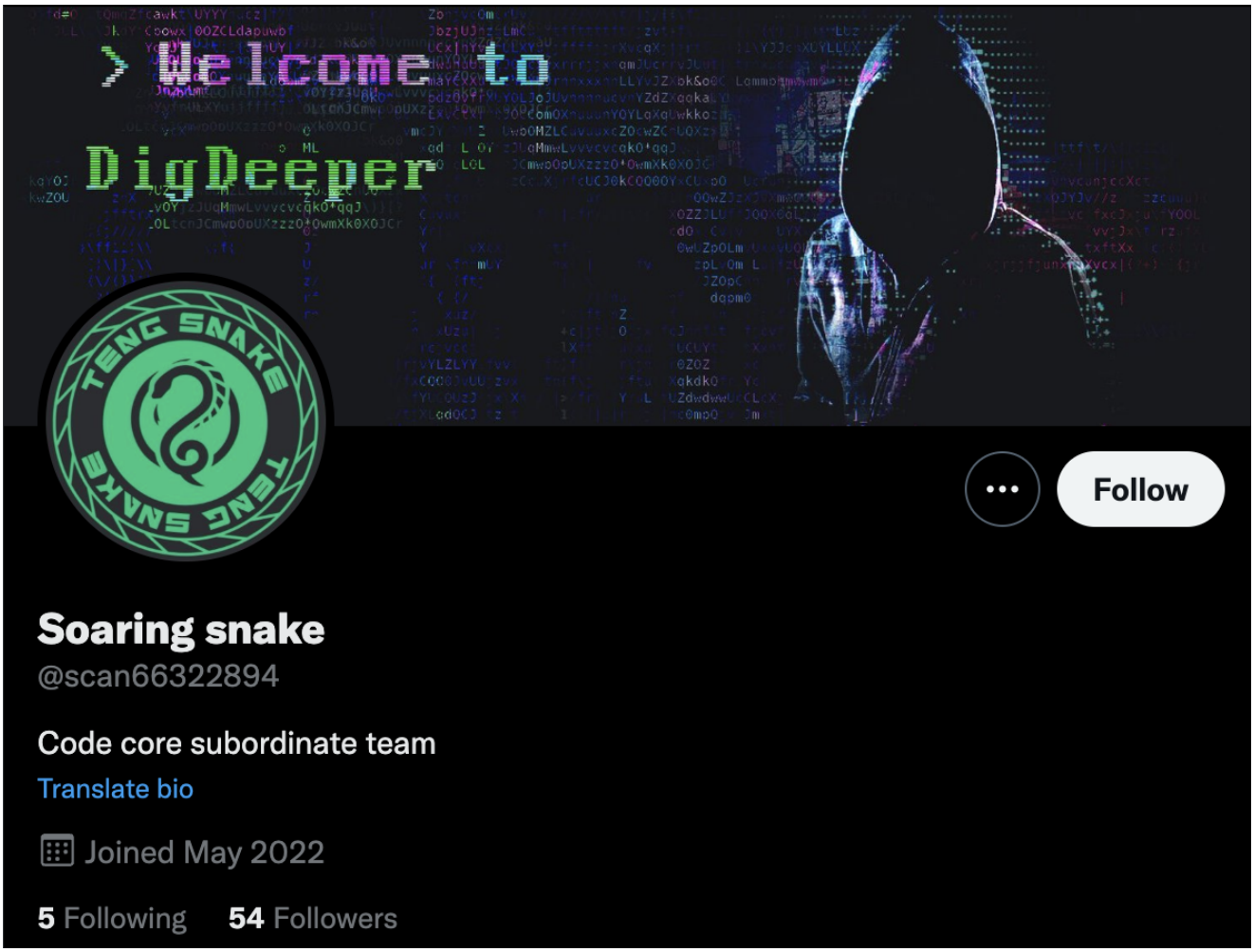
> As @CrazymanArmy and @ShadowChasing1 pointed out, our conclusion is also same that there is no concrete evidence to connect Teng Snake with the previously known APT-C-61.

Executive Summary

The “**Teng Snake**” team has created Telegram channels and group chats from October 2021. At the time, the team consisted of 4 core members and 7 sub-teams, and systematically operated channels and group chats. They claimed that they were APT-C-61, promoted provocatively, operated study teams, and recruited team members. However, there is no clear evidence that they are related to APT-C-61.

- (2022–02–10) Claimed to be APT-C-61 and started full-fledged activities.
- (2022–03–19) Shared the information about a Korean website vulnerability and a list of 97 websites that may have the same vulnerability in one of the Teng Snake-managed group chats.
- (2022–04–07) Started selling PII(Personal Identifiable Information) and chemicals, and receiving hacking requests.
- (2022–05–02) A user named , who claimed to be team, uploaded a post on an underground forum titled “South Korean health department invades” that was selling AD server privileges from an association.

— The same post was uploaded to the newly opened **Code Core** Telegram channel on May 6 and **Soaring Snake** Twitter account on May 7 and 13.



(2022–05–20) Declared the suspension of for-profit activities and shut down Telegram channels including several group chats except one channel.

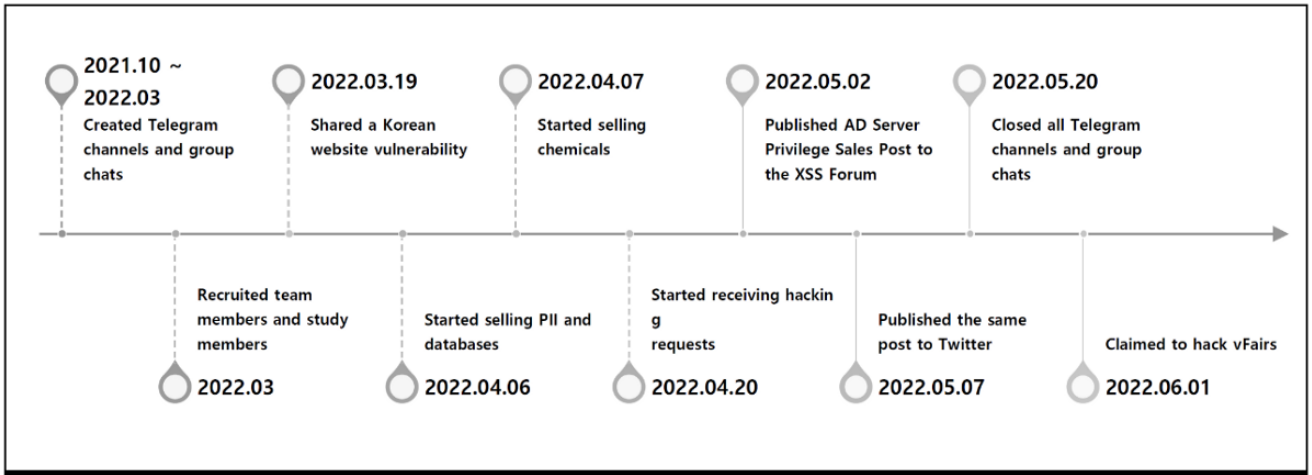
— **Mekimer** started using **CodecoreSET** account on Telegram from this point.

(2022–06–17) Yashma-based has been discovered.

1. Abstract

The **Teng Snake** team first began opening channels and group chats in October 2021. By June 2022, we have found 7 Telegram channels, 5 group chats, 6 accounts, and a Twitter account **Soaring Snake**(@scan66322894) believed to be associated with Teng Snake. The activities of the Teng Snake team from Telegram channels and group chats conversation are listed in Figure 1.

1.1. Timeline of Teng Snake x Code Core



Teng Snake	Code Core
(2021.10 ~ 2022.03) [Telegram] Created Telegram channels and group chats	
(2022-02-10) [Telegram] **Claimed to be APT-C-61**	**(2022.05.02) [XSS]** **Published AD server privilege sales post**
(2022.03) [Telegram] Recruited team member and study member	(2022.05.06) [Telegram] Created Code Core channel
(2022.03.19) [Telegram] **Shared Korean website vulnerability**	(2022.05.07) [Twitter] Created “Soaring Snake” account
(2022.04.07) [Telegram] Started selling PII and databases	(2022.05.07) [Telegram] Published AD server privilege sales post
(2022.04.20) [Telegram] Started receiving hacking requests	(2022.06.01) [Twitter] Claimed to hack vFairs
(2022.05.02) [Telegram] Declared suspension of data selling and receiving hacking requests	**(2022.06.17)** **Code Core Ransomware discovered on VT**
(2022.05.07) [Telegram] **Recruited team member and mention NATO**	

Figure 1. Timeline of Teng Snake and Code Core

2. Core members of Teng Snake

The ID of Telegram channels and group chats, which were directly managed by the Teng Snake team, were composed in form of APT{2,3 digits}. The full list of Telegram channels and group chats can be found in Appendix A.

The Teng Snake team revealed that the team had 4 core members and mentioned their roles as shown below.

Nick name	Role
Mekimer	Pentesting and APT
安赛克斯	Pentesting and APT
十七	Reversing and cracking
Skull Killer	Pentesting, OSINT, Vulnerability research

Figure 2. Core members of Teng Snake
We were able to find information about two of these members.

2.1. Mekimer: Head of Teng Snake

Mekimer is the leader and seems to be the keyman of the Teng Snake team. Most of the critical information shared in all Teng Snake group chats is forwarding Mekimer's messages. The vulnerability information of the Korean website was also shared by forwarding a Mekimer's message.

We found 2 blogs that are believed to be managed by Mekimer, in which he listed some of his personal information.

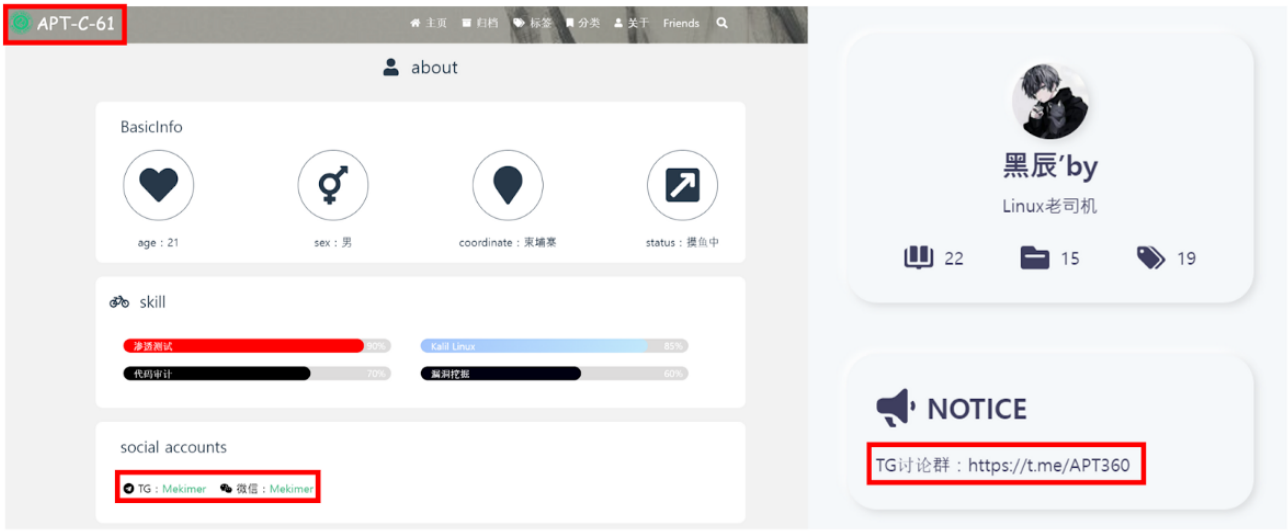


Figure 3. Two blogs of Mekimer
According to the information posted, he is a 21-year-old man and currently resides in Cambodia.

At first, we assumed that Mekimer was living in China, but in the group chats, he steadily appealed that he was abroad. It is difficult to confirm as there is no proof to back this up.

We also found that the nickname he used before working as alias Mekimer, **anqusec**.

Figure 4. Footer of Mekimer's blog

By clicking on the word "回忆", which means memories, at the bottom of Mekimer's blog, it is redirected to the **anqusec** blog. The blog posts also show that Mekimer continued to attack websites in China and other overseas countries. Also, we found articles on how to use hacking tools such as Nessus and AWVS, and articles on the use of 1-day vulnerabilities. In particular, he had written articles about the website infiltration periodically, and we also found that he infiltrated a Chinese coin exchange server using log4shell exploit.

After the Teng Snake team shut down some of their Telegram channels and group chats, Mekimer started using the alias, **CodecoreSET**.

2.2. Activity history of anqusec in an underground forum

We found that Mekimer uploaded three posts on an underground forum using the alias anqusec from November 13 to 15, 2021. We assumed that he also participated in the chat of the forum. Mekimer introduced himself as **Thunder Domain** (or **Xunlei domain name**) team in the following three posts.

- (2021–11–13) Official Portal of Kerala Local Government Leaked
- (2021–11–15) Fulbright plan | thunder field | 2021 | data operation
- (2021–11–15) ICAT international technology center of India | Xunlei domain | 2021

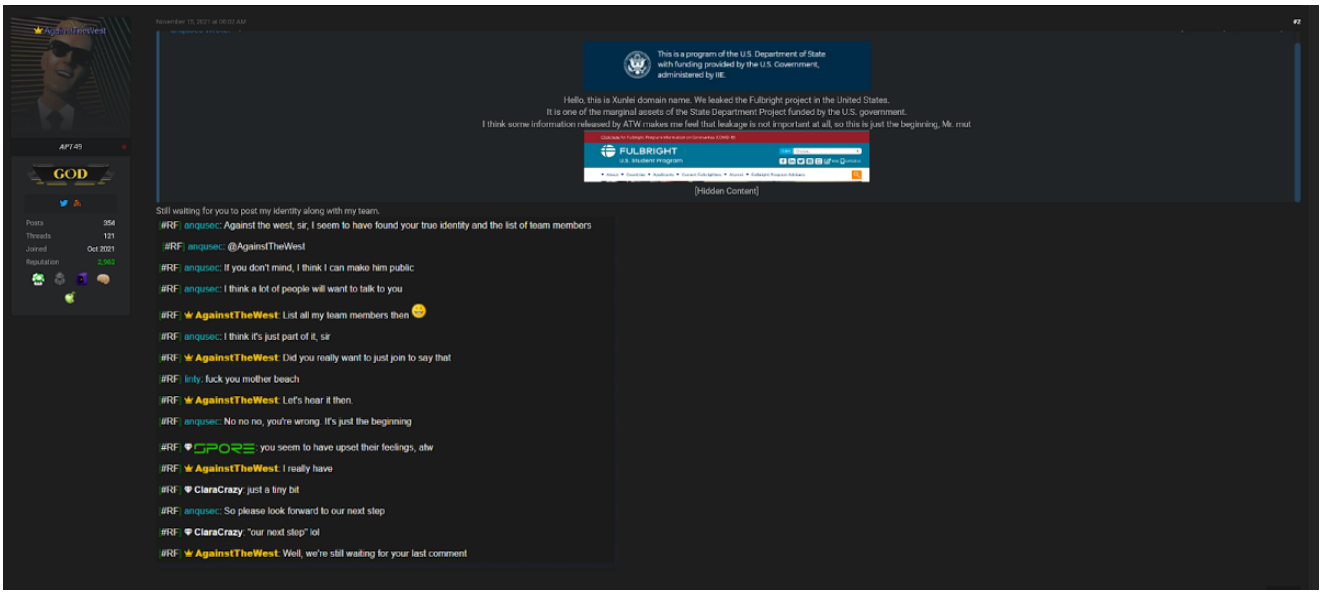


Figure 5. Mekimer talked with ATW,

Mekimer appears to have provoked ATW (Against The West) last year, saying he knew his identity. ATW responded they were still waiting for him to reveal his identity in one of the posts published by Mekimer. Mekimer has not yet released ATW's identity, and we assume that Mekimer did not actually have ATW's identity and just wanted to get attention or show off.

2.3. Skull Killer : Pentester of Teng Snake

Skull Killer is responsible for website penetration, OSINT, and vulnerability discovery in the Teng Snake team. In particular, Skull Killer is emphasized to have a large amount of personal information, which can be seen from his previous Telegram channel and group chat.

Skull Killer operated one Telegram group chat and one channel. The group chat was opened in August 2020, but it began operating in October 2021. Various personal information, hacking tools, and vulnerabilities were shared in the group chat and their channels.

On January 29, 2022, a text file named "韩国_外汇_375224 份_3月.txt" was uploaded to a chat room operated by Skull Killer. The file included 375,224 Korean account information, and consisted of e-mail, name, phone number, job information, and hashed password.

3. Mekimer + Skull Killer + α

On February 10, 2022, Teng Snake shared a screenshot that contains directories and files they used in the attack which was conducted in 2019, with the analysis report published by 360 Security about APT-C-61.

> **APT-C-61(腾云蛇) report from 360 Security [link]

According to 360 Security, APT-C-61 group primarily targeted Pakistan and Bangladesh, particularly important sectors such as government, military industry, and research centers.

APT-C-61 used spear-phishing and social engineering techniques to infiltrate, and DDE to download malware. The malware that is finally installed on the host is an executable file packaged with pyinstaller that executes commands received from the C&C server. Afterward, utilities such as 7za.exe and rclone.exe were also downloaded to exfiltrate sensitive files.

Teng Snake group claimed to be APT-C-61 group, but the screenshot they uploaded contained 2 python scripts, one suspected to be a tool. The tool has the same size (3kb) as the publicly available script on Github. Also, a directory that was suspected to be an open-source tool called is also displayed.

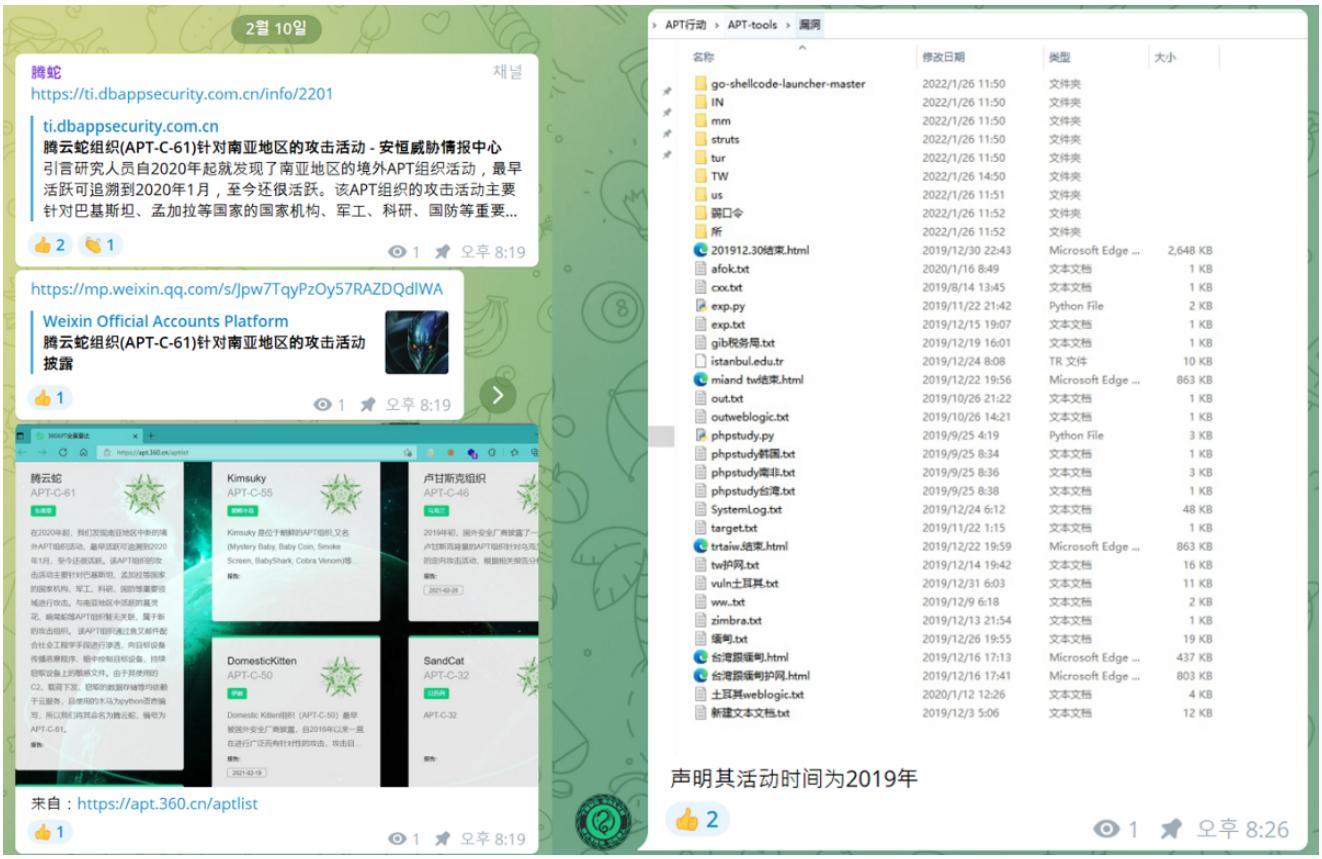


Figure 6. Teng Snake claimed to be APT-C-61

Furthermore, while APT-C-61 used Google Drive and Dropbox, Teng Snake is using Ali Cloud.

Figure 7. Screenshot of Ali Cloud

While the countries affected by APT-C-61 are located in South Asia, the countries identified in Figure 7 and their tweets are South Korea, Myanmar, Turkey, and Taiwan. It's an overstatement to call them an APT group, as they are carrying out their attacks with very obscure purposes.

As a result, when comparing the information of the APT-C-61 group with the information of Teng Snake that has been released so far, **it is hard to say that Teng Snake is an APT-C-61 group.**

4. Teng Snake started the emerging cyber threat in the real world.

4.1. Korean website vulnerability shared on a group chat

On March 19, 2022, a file named "韩国网贷.txt" was uploaded to a group chat along with several files. The message was a forwarded Mekimer's message by a user named **雷域** and he is presumed to be the manager of the group chat.

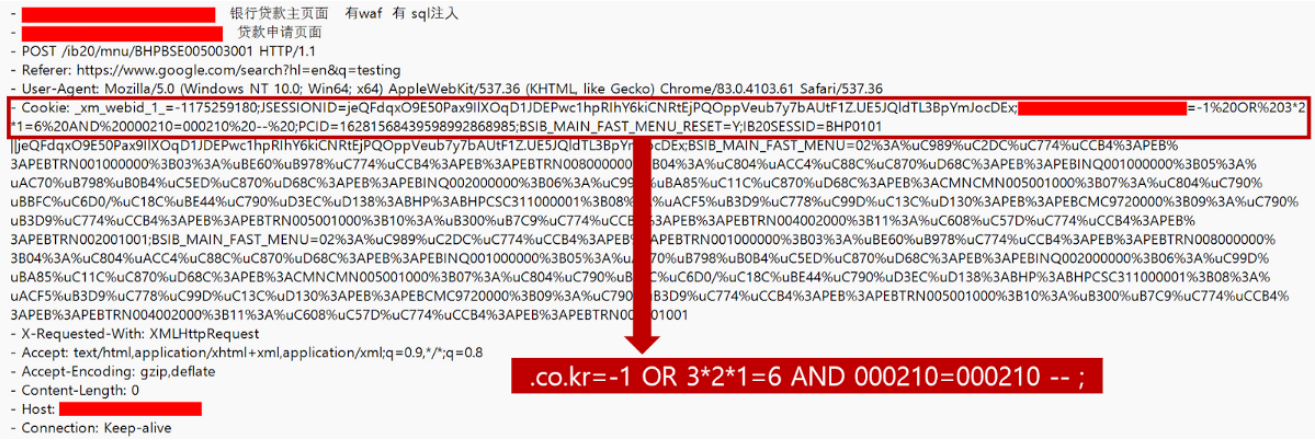


Figure 8. Exploit payload of SQL injection

In the overall context, the file appears to be educational material for users in the group chat. Hacking tools, hacking tips, a vulnerability, and a payload used to attack South Korean websites were included in the file. It also included a list of websites that showed the possibility of vulnerabilities or whether they existed.

The vulnerability was a SQL injection, and inside the file, there was an exploit payload that could be used for actual attacks, as shown in the picture above.

In addition, as shown below, we were able to check the precautions and hacking tips to be taken.

- Use Nessus or AWVS 13.14 version instead of XRAY when scanning Korean websites for vulnerabilities.
- Use dynamic IP.
- Look at the subdomains of the target website.

- Many XSS vulnerabilities are found, but few are useful.
- Social engineering, such as phishing mail, is much more useful to target administrators.

Finally, a list of 97 websites (one duplicated) that can test the forementioned vulnerabilities was also shared, with more than half belonging to the financial and loan industry.

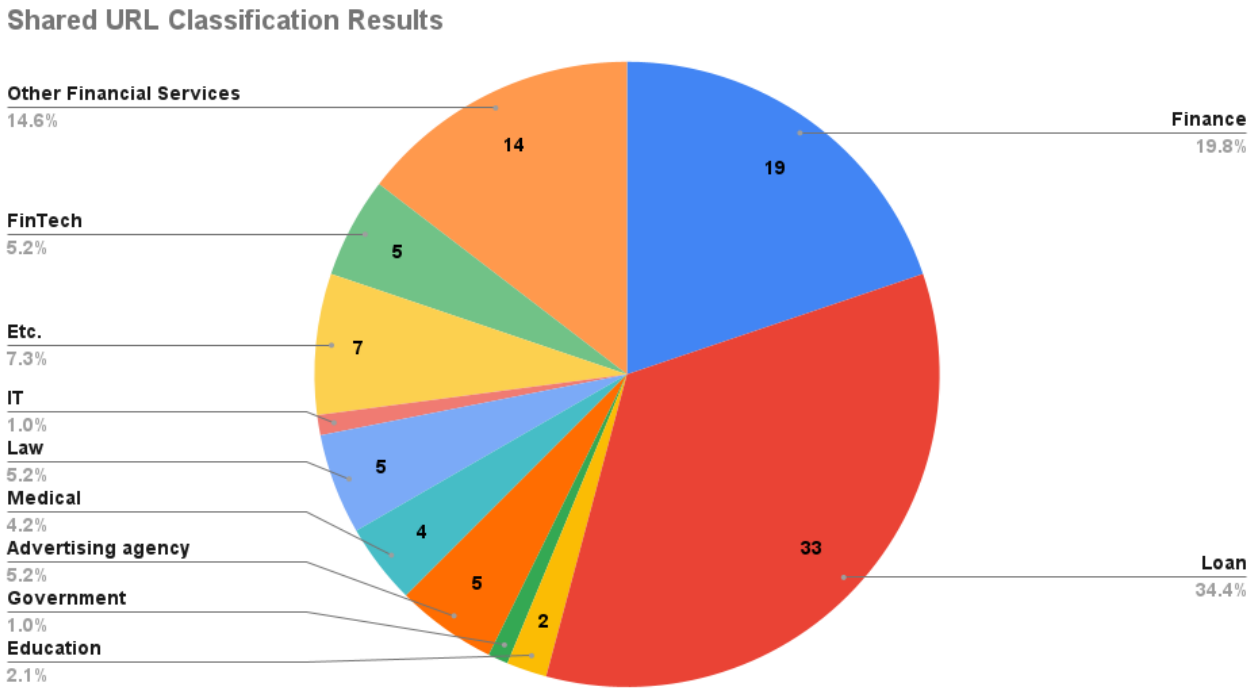


Figure 9. Classification results of shared URLs

After sending the message, the user continued to share hacking tools and vulnerabilities they used, such as uDork and CANVAS, in the group chat and kept the group chats highly active.

4.2. Start selling PII, databases, and chemicals

At the end of March, Teng Snake closed some of their Telegram group chats and channels and also stopped recruitment. At the time of recruiting, it is estimated that at least 100 people were recruited in each of 3 group chats, so it seems that enough people gathered to stop recruiting people and begin commercial activities.

On April 7, 2022, Teng Snake posted on their main channel that they started selling the following chemicals and would not sell them to China.

Figure 10. Chemicals sold by Teng Snake

And on April 20, 2022, the Teng Snake team announced that they would start receiving hacking requests and released their unit price list. The workable contents and unit price are as follows.

Work	Details	Starting price
Development	APK and program development	5,000 yuan
	Module development	5,000 yuan
	Custom development	20,000 yuan
Pentesting	Website infiltrating (Backend privilege,system privilege, shell, database privilege takeover)	20,000 yuan
	Privilege maintenance(Linux, Unix, Windows)	10,000 yuan
	Dumping database	7,000 yuan
Whatsapp user account information	-	700 yuan(100,000 each)
Interface searching	-	1,000 yuan
Website brute forcing	-	100 yuan

Figure 11. Workable unit price released by Teng Snake

After they released their unit price, they continuously promoted that they were receiving hacking requests on the Telegram channel. However, it seems that they were not paid even after the finish of some requests.

In addition, they also sold Chinese personal information. Below is a part of the sales items.

- **14w 广东驾校学员-2022.xlsx**
- **2.9w 多简介数据-2022-04-15.xlsx**
- **29w 江苏宿迁业主.xlsx**
- **650 套-未泛滥身份证正反.zip**
- **75w 山东快递职称.csv**
- **90 万 7 位 QQ 号账号密码**
- **业主**
- **城建**

tengshe staff 130K 3 11 19:25 浙江城建项目 1.9k.xlsx

- **外卖**
- **油卡**
- **教师.txt**
- **电气.txt**
- **中国 10 亿手机库**

-rwxrwxrwx 1 tengshe staff 5.0G 3 13 14:24 数据.rar

- **湖南 150w**

-rwxrwxrwx 1 tengshe staff 1.8M 3 11 19:25 中专.xlsx

-rwxrwxrwx 1 tengshe staff 37M 3 11 19:25 初中.xlsx

-rwxrwxrwx 1 tengshe staff 1.4M 3 11 19:25 大专.xlsx

-rwxrwxrwx 1 tengshe staff 95K 3 11 19:36 本科.xlsx

-rwxrwxrwx 1 tengshe staff 11M 3 11 19:44 高中.xlsx

-rwxrwxrwx 1 tengshe staff 26M 3 11 19:26 小学女.xlsx

Figure 12. Part of the Chinese PII selling list

After that, on May 2, the suspension of receiving hacking requests and data sales was announced. Some buyers had raised suspicions about the resale of data sold by the Teng Snake team, and some clients had not paid. This seems why they have declared a shutdown.

Figure 13. Declared suspension of receiving hacking request and data sales

4.3. Selling AD server privilege of South Korea health department

On May 2, 2022, a user by the name of **uteus** posted on an underground forum titled "**South Korean Health Department Invades**." Pointing out he was part of a team called **White Dawn** and sold access permission with captured photos of him accessing the AD server believed to belong to the Ministry of Health and Welfare of Korea.

The Teng Snake team introduced themselves as **White Dawn** only in this post, and later introduced themselves as **Soaring Snake** (or **Snakes**) team, as a part of the **Code Core** team. Currently, Teng Snake's Mekimer (a.k.a. CorecodeSET) and uteus are believed to be in the Code Core team.

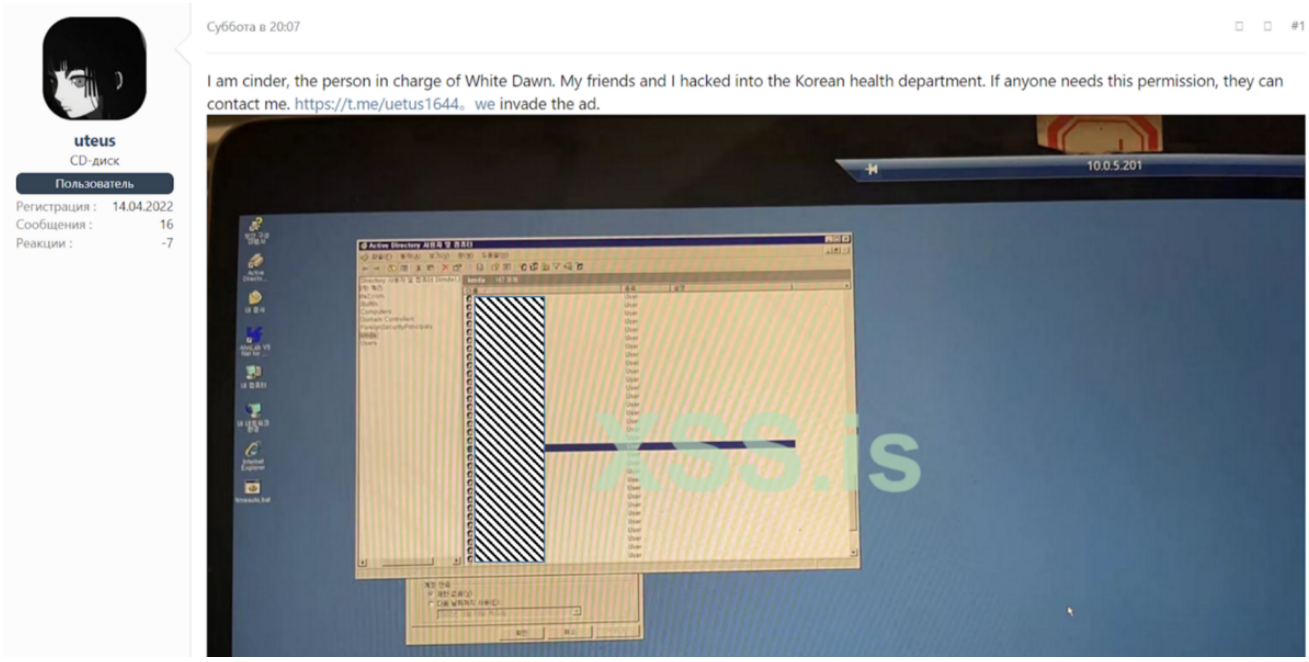


Figure 14. AD server privilege sales post by uteus,

As a result of analysis based on the username on the sample photo, it was confirmed that the actual target of the attack was a different association. We presumed that they lack an understanding of Korea.

In addition, supplementary profit-generating activities through the distribution of ransomware were not being used at that time.

4.4. Who is uteus(uetus)?

uteus is currently one of the members of the Code Core team and is believed to be responsible for planning attacks and recruiting team members. He has started activities on the forum since April 15.

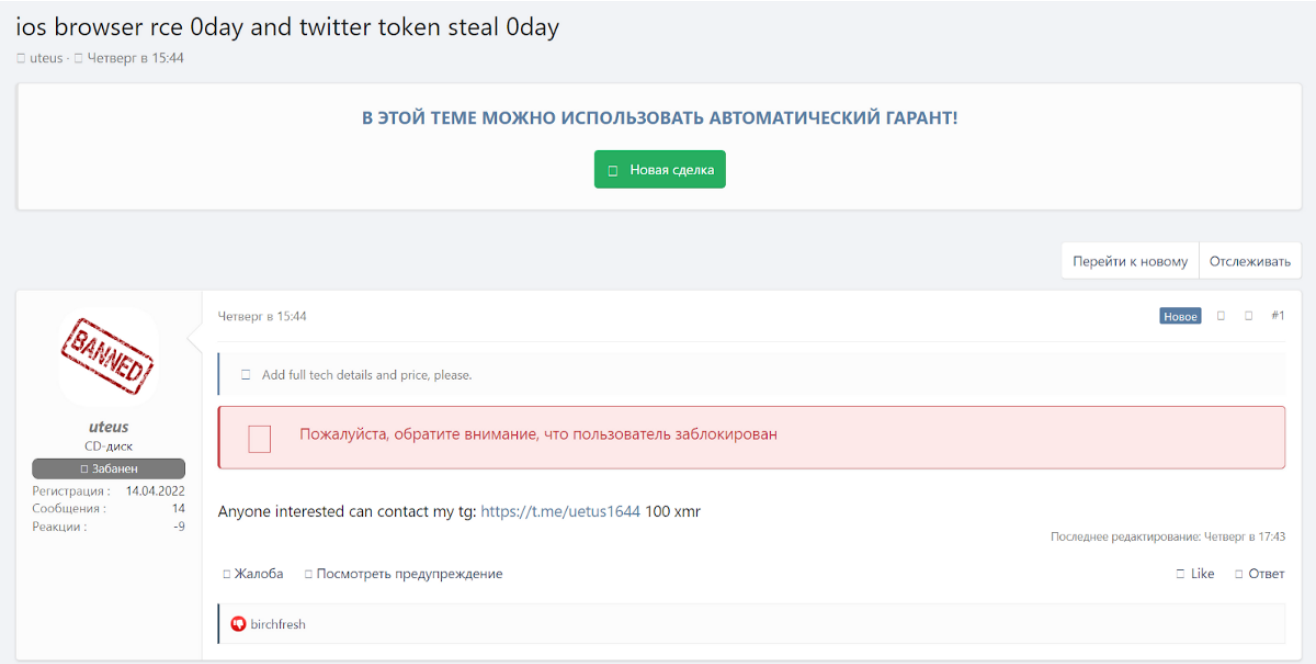


Figure 15. First post of uteus,

On April 15, 2022, when he began his activities, he posted about selling an iOS browser RCE Zero Day and Twitter Token Zero Day. But he was criticized by other users for not providing grounds for the vulnerabilities.

He also commented on the article titled "**Отключаем Windows Defender (+ UAC Bypass, + Повышение до уровня SYSTEM)**", asking what passwords were for downloading tools for Windows EoP.

cinder, mentioned in "**South Korean health department invades**," is the alias he used on another underground forum. He has started activities on the forum since April 3.

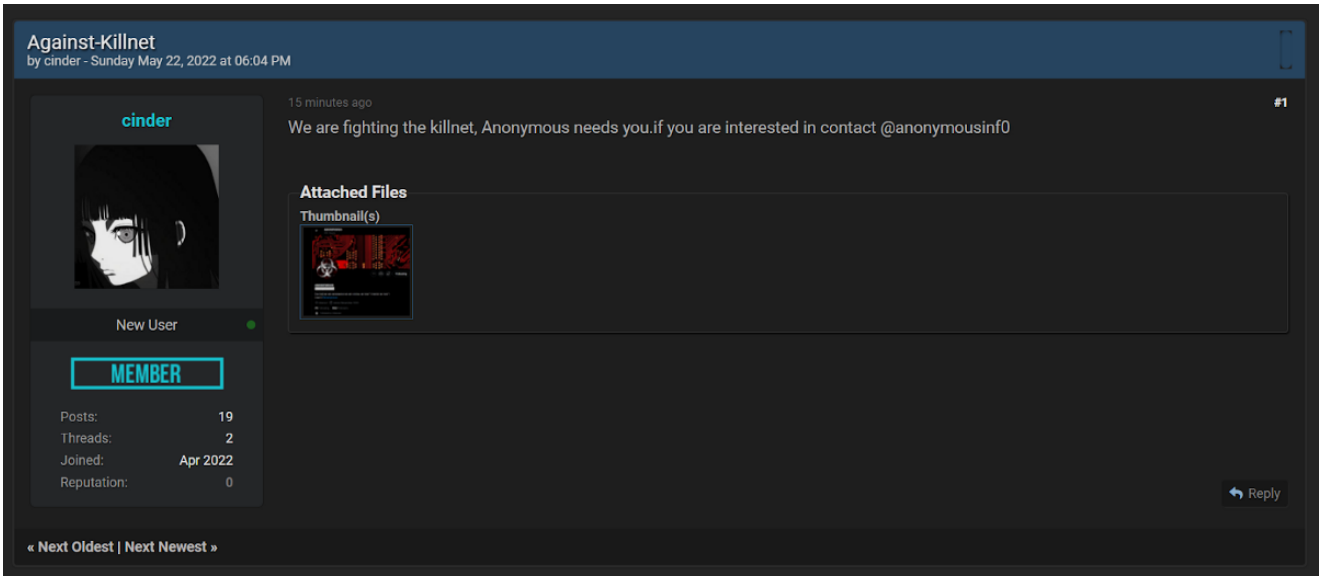


Figure 16. One of the posts by cinder,

On May 22, 2022, a post titled “Against-Killnet” was posted. He wrote to those who resisted Killnet, commenting “Anonymous needs you,” and this suggests that he is related to Anonymous.

4.5. Recruiting new team members and mentioning NATO

After announcing the suspension of receiving hacking requests and personal information sales on the Telegram channel, Teng Snake began recruiting new team members on May 7. The difference is that they started to check the hacking skills of the applicants.

Figure 17. Mentioned NATO on Telegram

The conditions for joining the Teng Snake team were stated that they should be experienced (webshell upload, high-risk vulnerabilities, penetration of internal network nodes) in taking control of the internal network of NATO allies.

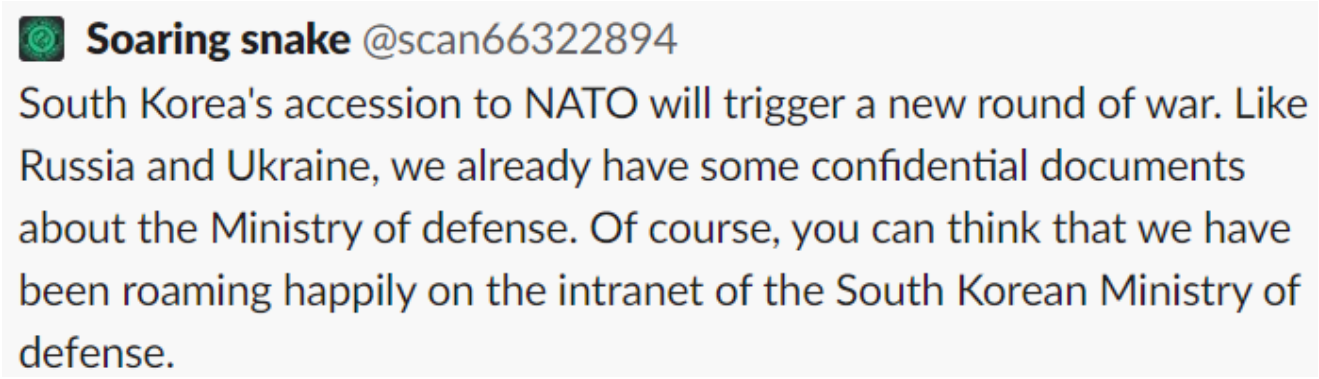


Figure 18. Mentioned NATO on Twitter

On Twitter, they claimed that South Korea’s entry into NATO would cause a new war and that they had already seized confidential data from the Ministry of National Defense. Korea joining NATO mentioned here means that Korea has joined the NATO Cooperative Cyber Defence Centre of Excellence as a regular member. Through this, it is speculated that Teng Snake lacks understanding of this case and just ostensibly mentions it to create the justification for attacks on NATO-related countries.

Figure 19. Continued to recruit new members

From this point on, May 17, they started receiving new team members who can steal server privileges for non-governmental organizations, military, and third-party supply chains.

4.6. Code Core Ransomware Detected

On June 17, 2022, **Code Core Ransomware** was uploaded to Virus Total.

The ransomware was created by the **Yashma** ransomware builder (a.k.a. **Chaos** ransomware builder), and the ransom note was customized to include their team name. For information on the Chaos ransomware, refer to Appendix D. Based on the use of minor Yashma ransomware builders rather than other famous RaaS, the Code Core team seems to lack expertise in ransomware and the ransomware ecosystem.

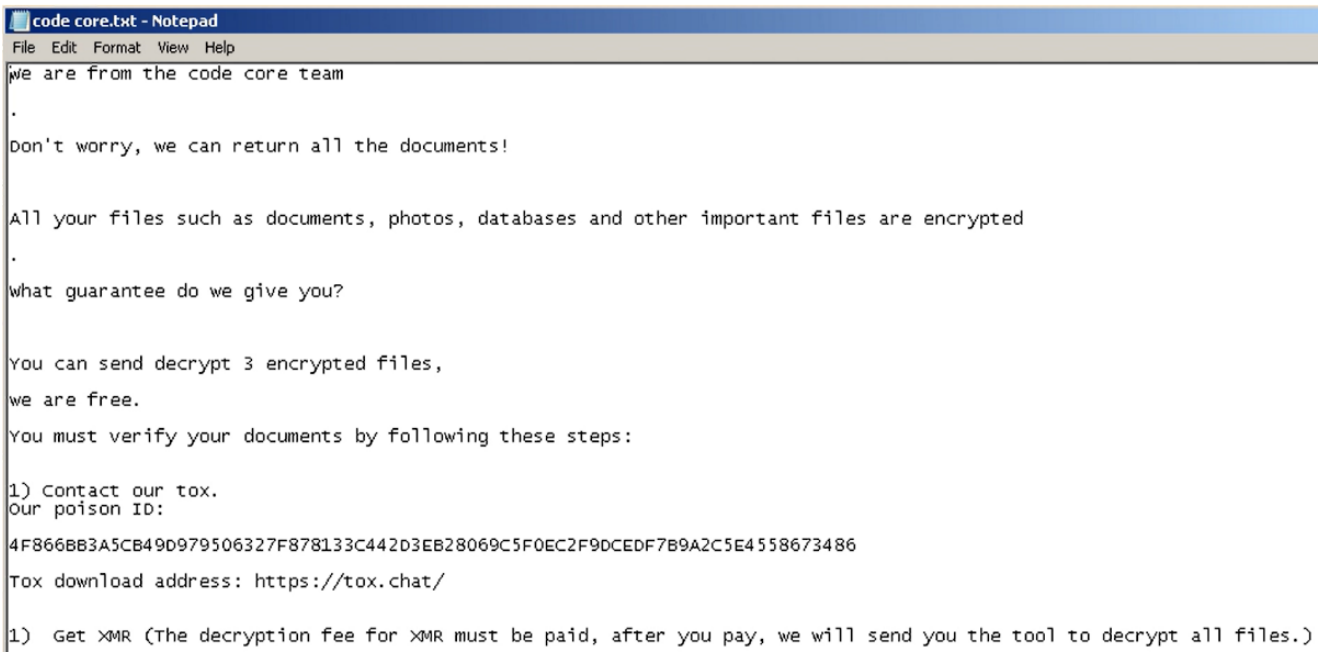


Figure 20. Ransom note of Code Core Ransomware

Conclusion

- Most of the attack methods used by the Teng Snake team have not been disclosed, but it is estimated that they are mainly focused on cloud and web servers.

- Currently, it has been confirmed that Mekimer, the team leader of Teng Snake, has joined the Code Core team and is attacking South Korea and NATO countries along with uteus and other team members.
- The Code Core team is currently developing Yashma-based ransomware, so it is expected to use the ransomware in future attacks.
- Government agencies in NATO countries need to continuously monitor their activities.

Appendix A. Teng Snake's group structure and managed Telegram channels, accounts, and group chats

Teng Snake's group structure

Team name	Role
腾蛇	External APT Attacks and Vulnerabilities Research
白阳技术团队	Attacks on Taiwanese government websites
九婴血色安全团队	Development and data acquisition
数据库渗透测试团队	Database server penetration
雷霆渗透测试团队	-
青鸾社工团队	Data collection and operation
学习组	Team recruitment and study operations

Group chats

- 【腾蛇】-技术交流群
- 九婴血色安全团队
- 雷霆渗透测试团队
- 青鸾社工团队
- 学习组

Channels and accounts

Channel/Username	Participated group chat	Notes
腾蛇	-	Presumed to have been used by Mekimer
九婴	九婴血色安全团队	
青鸾	青鸾社工团队	-
五七	雷霆渗透测试团队	-
雷域	雷霆渗透测试团队	Laundering money after changing to “Mr”
技术研讨	学习组	-
搭建 开发，逆向，查档	九婴血色安全团队	-
Mekimer	-	-
逸苏十七	雷霆渗透测试团队	-
信息情报盘点	-	-
CodecoreSET	-	Currently used by Mekimer
渗透｜数据｜脱裤｜指定站｜联盟供需频道	-	Presumed to be an external cooperation channel rather than a direct data sales channel
Code Core	-	Code Core official channel

Appendix B. Links associated with Mekimer

Surface Web

- Anqusec github:
- Anqusec blog:
- Mekimer github:
- Mekimer blog:

Deep Web

Anqusec Telegram Channel:

Appendix C. Other information sharing and sales

(2022.04.04) Shared Japanese E-mail lists

(2022.05.06) 300 million total sales of American personal information

- The data was also sold on a collaboration channel, and it is still being sold on the channel.
- The collaboration channel was initially introduced as a channel managed by the Teng Snake team, but from the end of March, it was introduced as an advertising channel. It is presumed that the Teng Snake team is operating independently even after they stopped working.

Appendix D. Code Core Ransomware

- (2021–08–25) S2W,
- Sample of Code Core Ransomware

— VirusTotal : https://virustotal.com/gui/file/3a167d1d4dfe9ba36118c816f1b73c7e

— ANY.RUN : https://app.any.run/tasks/412be530-3443-4635-80b8-992c97094576/

More from S2W BLOG

S2W is a big data intelligence company specialized in the Dark Web, Deepweb and any other covert channels.

Read more from S2W BLOG

Recommended from Medium

Rachel Janean

{UPDATE} 5 Second Rule: Drinking Games Hack Free Resources Generator

Jaclyn Supple

{UPDATE} Cop ratsastus Hack Free Resources Generator


Karnel32

Practical Malware Analysis Labs


DeFiHorse

Official Airdrop Announcement: DeFiHorse x CoinMarketCap