2022 PRAGUE

28 - 30 September, 2022 / Prague, Czech Republic

SCRIPT KIDDY ON THE DEEP & DARK WEB: LOOKS SERIOUS? BUT EMPTY SUIT!

Dasom Kim, Yeonghyeon Jeong, Yujin Lee & Jeongyeon Lim

S2W, Korea

dasomong@gmail.com

ABSTRACT

On the deep and dark web, an increasing number of threats leading to data breaches and open-source vulnerabilities are occurring. With the emergence of LAPSUS$ this year, major companies around the world suffered damage, and confidential information was leaked.

In 2020, as remote working became normal routine around the world due to Covid-19, threat actors began to pose a greater threat to our daily lives, from corporate infrastructure to individuals. Now, it is not only large corporations, but also websites with vulnerabilities on the open web, small businesses and general community sites with low-level security that are being targeted by threat actors. In this paper we focus on analysing two threat actors that sold relatively little-known, but critical leaks.

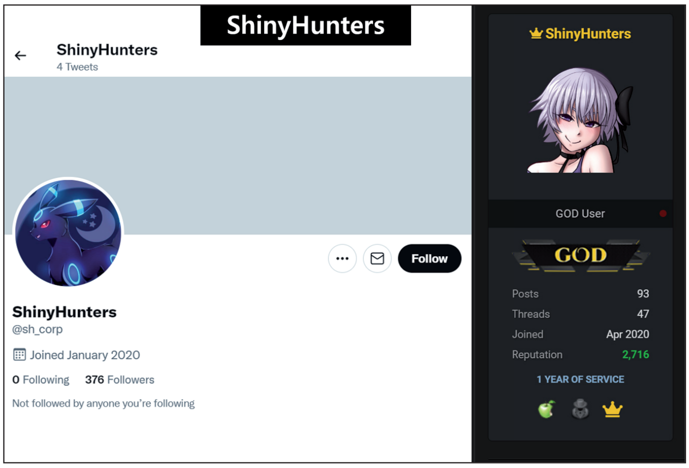
This report is based on posts and information confirmed by 25 July 2022. The times mentioned in the report are based on KST (UTC+09:00).

INTRODUCTION OF DATA BROKER & INITIAL ACCESS BROKER

We start by explaining the two threat actor roles, data broker and initial access broker. Both are mainly active in forums and markets on the deep and dark web.

Data broker

Those who specialize in collecting personal information or data about companies or institutions and users, and selling such information to third parties, are called data brokers. The most representative example is ShinyHunters, who mainly sold leaked information related to a specific website.



ShinyHunters

ShinyHunters
4 Tweets

ShinyHunters
@sh_corp
Joined January 2020
0 Following 376 Followers
Not followed by anyone you're following

ShinyHunters
GOD User
GOD

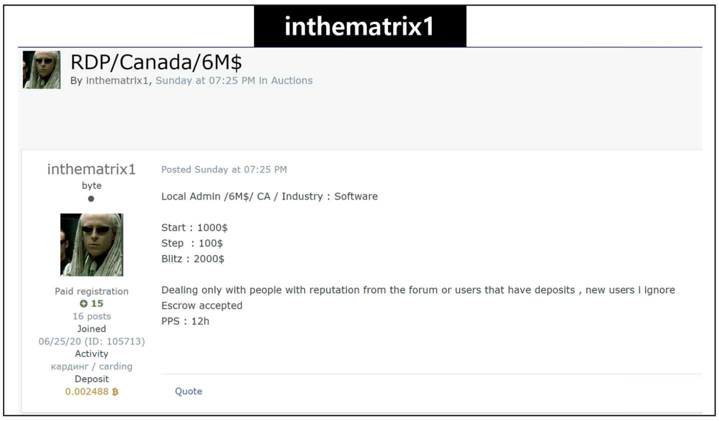
Posts	93
Threads	47
Joined	Apr 2020
Reputation	2,716

1 YEAR OF SERVICE

Figure 1: The profile of ShinyHunters.

Initial access broker

Those who sell network-related credentials such as RDP and VPN related to specific companies and institutions and access rights to databases are called initial access brokers. Inthematrix1, who is mainly active in the Exploit forum and RAMP forum, is the most active initial access broker.



inthematrix1

RDP/Canada/6M$
By inthematrix1, Sunday at 07:25 PM in Auctions

inthematrix1
byte

Paid registration
15
16 posts
Joined
06/25/20 (ID: 105713)
Activity
кардинг / carding
Deposit
0.002488 ฿

Posted Sunday at 07:25 PM

Local Admin /6M$/ CA / Industry : Software

Start : 1000$
Step : 100$
Blitz : 2000$

Dealing only with people with reputation from the forum or users that have deposits , new users i ignore
Escrow accepted
PPS : 12h

Figure 2: The post of inthematrix1.

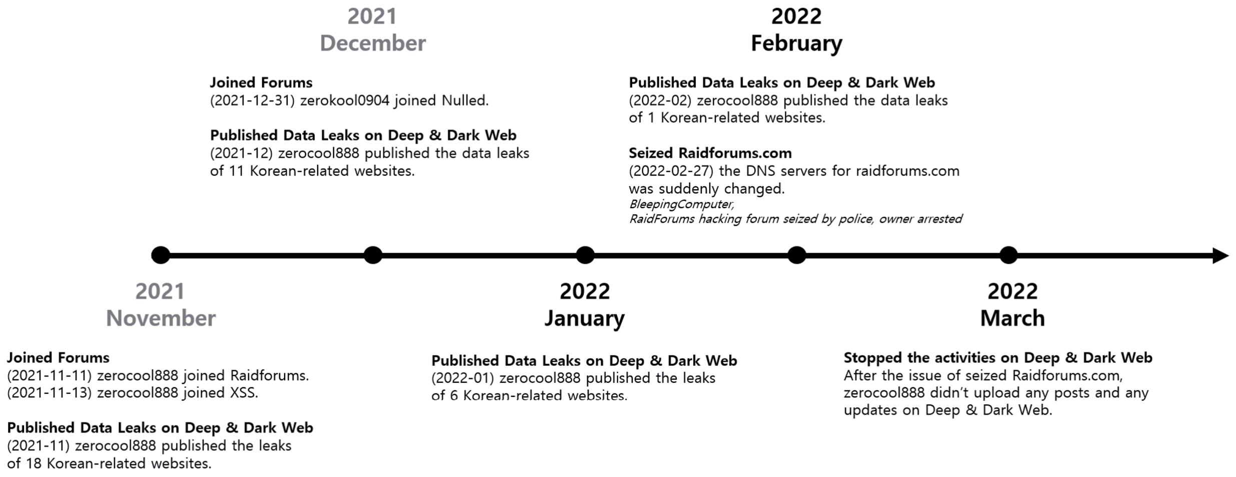
DATA BROKER @ZEROCOOL888

Overview

First, we analysed @zerocool888, which sold personal information and corporate accounts related to Korean websites. @zerocool888, which was active in RaidForums in 2021, sold a total of 35 cases of Korean company information and Korean personal information.

Timeline

Figure 3 shows a timeline of the activities of @zerocool888 from 2021 to 2022.



2021 November

Joined Forums
(2021-11-11) zerocool888 joined Raidforums.
(2021-11-13) zerocool888 joined XSS.

Published Data Leaks on Deep & Dark Web
(2021-11) zerocool888 published the leaks of 18 Korean-related websites.

2021 December

Joined Forums
(2021-12-31) zerokool0904 joined Nulled.

Published Data Leaks on Deep & Dark Web
(2021-12) zerocool888 published the data leaks of 11 Korean-related websites.

2022 January

Published Data Leaks on Deep & Dark Web
(2022-01) zerocool888 published the leaks of 6 Korean-related websites.

2022 February

Published Data Leaks on Deep & Dark Web
(2022-02) zerocool888 published the data leaks of 1 Korean-related websites.

Seized Raidforums.com
(2022-02-27) the DNS servers for raidforums.com was suddenly changed.
BleepingComputer,
RaidForums hacking forum seized by police, owner arrested

2022 March

Stopped the activities on Deep & Dark Web
After the issue of seized Raidforums.com, zerocool888 didn't upload any posts and any updates on Deep & Dark Web.

Figure 3: The activities of @zerocool888 from 2021 to 2022.

The activities of @zerocool888

@zerocool888 is active on RaidForums, XSS and Nulled and, based on the joining date, started fully fledged activities around November 2021. From 11 November to 31 January 2021, @zerocool888 uploaded a total of 35 posts on RaidForums, and sold about 31,000,000 cases of Korean-related personal information and account information. The types of sites affected by data sold by @zerocool888 are shown in Figure 4.

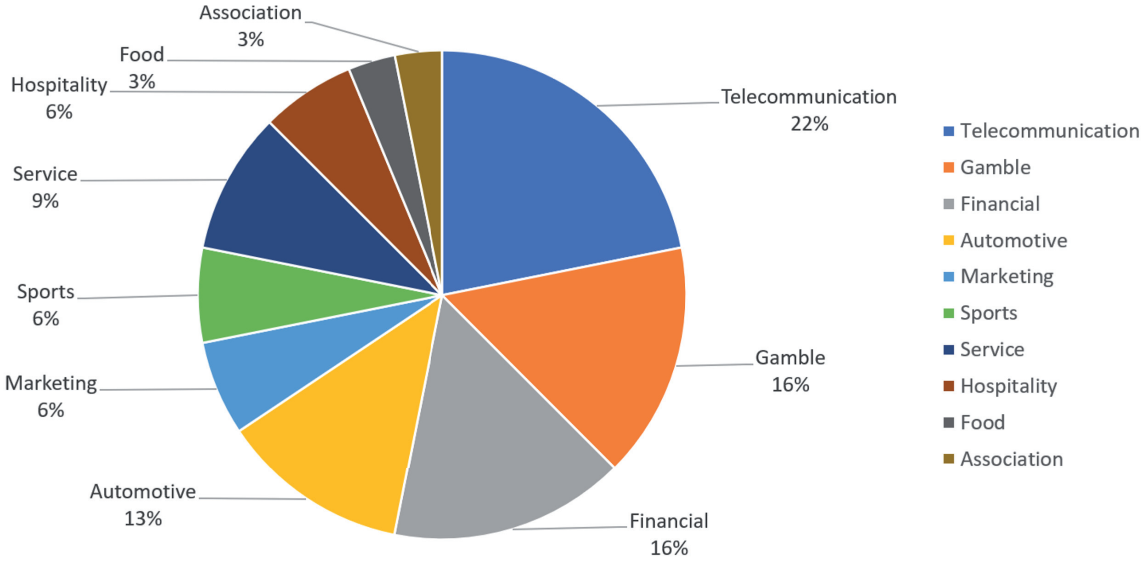


Figure 4: The sectors attacked by @zerocool88.

@zerocool888 not only sells account information, but also personally identifiable information that includes website users' home addresses, phone numbers, and subscriber information. Table 1 shows @zerocool888's posts on RaidForums (data leaked from forums and channels related to the deep & dark web is greyed out).

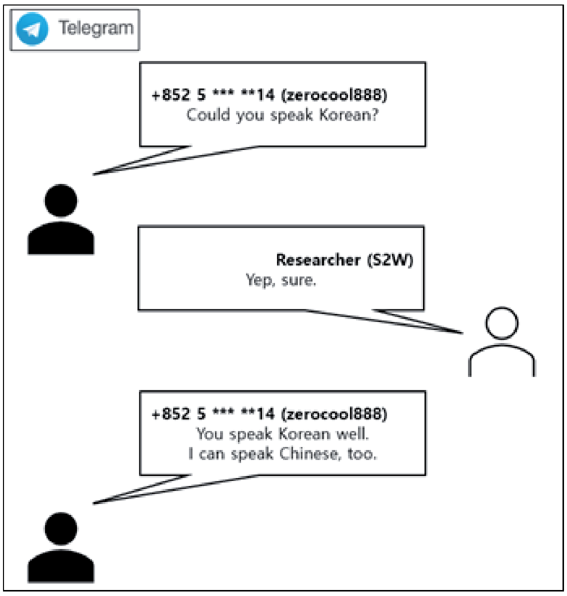
Num	Published Date	Sector	Title
01	2021.11.12 09:37PM	N/A	SELLING South Korea FULL DETAILS DATABASE
02	2021.11.13 07:46AM	Telecommunications	CSV South Korea SMS log (Name,Phonenumber)
03	2021.11.13 07:57AM	Food	CSV South Korea ifoo****.or.kr 11306 people data
04	2021.11.13 08:56AM	Gambling	TXT South Korea Gamble Site SMS Log [FREE]
05	2021.11.15 07:04AM	Telecommunications	TXT South Korea /kr****.net
06	2021.11.15 08:08AM	Telecommunications	TXT South Korea SMS site /munj****.com
07	2021.11.15 08:14AM	Marketing	TXT South Korea Web Survey replay data
08	2021.11.16 12:15PM	Sports	TXT South Korea han****.co.kr/ golf web market
09	2021.11.16 12:15PM	Sports	TXT [Sale-Sample] South Korea han****.co.kr / golf web market
10	2021.11.16 12:32PM	Gambling	TXT South Korea Gamble Site SMS Log
11	2021.11.18 01:35PM	Telecommunications	TXT South Korea www.sms****.co.kr (FREE)
12	2021.11.18 10:47AM	Services	TXT South Korea www.hel**-**.kr (FREE)
13	2021.11.19 02:43PM	Financial	TXT South Korea om**.**.kr (FREE)
14	2021.11.29 02:09AM	N/A	SELLING 31Million South Korea Database / Full Detali Data
15	2021.11.29 06:10PM	Telecommunications	CSV South Korea www.hel**-**.kr
16	2021.11.29 07:31PM	Association	CSV South Korea www.ki**.**.kr/www.ke****.kr
17	2021.11.30 10:03AM	Telecommunications	TXT South Korea Gamble Site SMS Log #2 [FREE]
18	2021.11.30 10:48AM	Services	CSV South Korea 5-website **Already leaked the same files on Telegram OpenData Channel.
19	2021.12.01 04:10PM	Gambling	TXT South Korea Gambler mail address (FREE)
20	2021.12.02 08:17AM	Telecommunications	TXT South Korea sms****.co.kr
21	2021.12.06 08:33AM	Services	South Korea -love****.co.kr
22	2021.12.07 02:10AM	Gambling	SELLING South Korea Gambler data & SMS Log/ 266k
23	2021.12.08 12:08PM	Financial	CSV South korea /sh**-**.co.kr / loan
24	2021.12.16 10:03AM	N/A	SELLING 31million South Korea Data (It's sold only to one .No resale.)
25	2021.12.16 10:03AM	N/A	SELLING 31million KR South Korea Data
26	2021.12.21 09:14PM	Automotive	CSV South Korea Used Car Dealer Data
27	2021.12.21 10:18PM	Gambling	SELLING South Korea Gamble Member / 266k+
28	2021.12.29 01:52PM	Financial	SQL South Korea insurance Customer Log
29	2021.12.30 09:47AM	Automotive	TXT South Korea Car Navigation Update Data
30	2022.01.01 03:43PM	Telecommunications	TXT South Korea Telecom Customer
31	2022.01.10 04:56AM	Automotive	CSV South Korea Car club Member
32	2022.01.15 12:52PM	Marketing	TXT South Korea blog marketer ,membership card user data
33	2022.01.17 09:19PM	Hospitality Financial	South Korea Hospital+Resort+Ars loan
34	2022.01.19 02:59PM	Financial	South Korea funeral insurance Log
35	2022.01.23 11:45PM	Automotive	TXT South Korea Car Information System Update Log
36	2022.02.24 08:49AM	Hospitality	South Korea Hotel reservation Company

Table 1: List of posts by @zerocool888.

Deep analysis of @zerocool888

@zerocool888 is Korean, living in Hong Kong

On 16 November 2021, we confirmed that @zerocool888 had signed up for a *Telegram* account (@zerocool888) with a Hong Kong number for contact with RaidForums users. @zerocool888 mainly communicated in English in RaidForums but claimed to speak Korean like a native, and also to be able to speak Chinese. The actual conversation with @zerocool888 is shown in Figure 5.



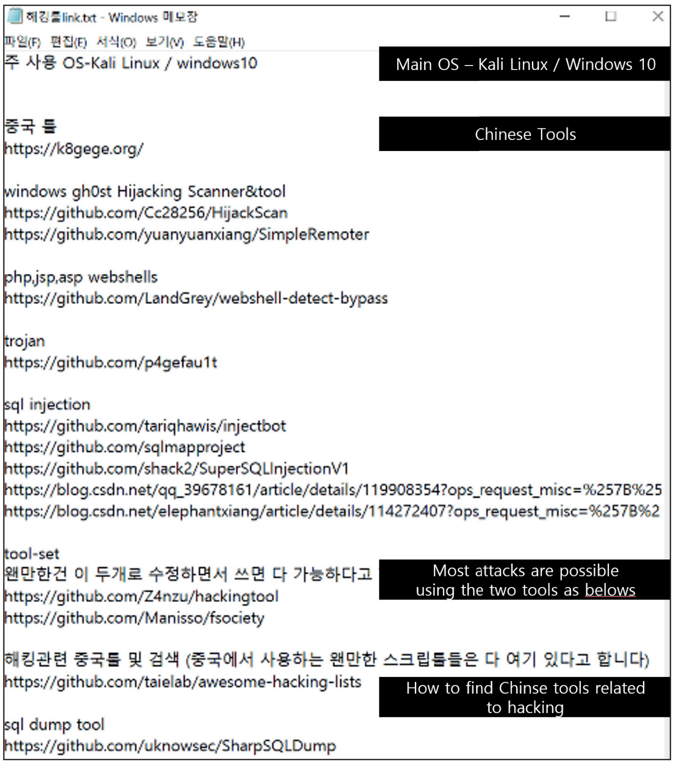
+852 5 * **14 (zerocool888)**
Could you speak Korean?

Researcher (S2W)
Yep, sure.

+852 5 * **14 (zerocool888)**
You speak Korean well.
I can speak Chinese, too.

Figure 5: Screenshot of the communication with @zerocool888.

Throughout the conversation, @zerocool888 seemed familiar with Korean and used the words worker, injection and hacking tool, so was judged to be a data broker selling leaked data. Figure 6 shows the content of the hacking tool link.txt text file sent by @zerocool888.


해킹툴link.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
주 사용 OS-Kali Linux / windows10


중국 툴
https://k8gege.org/

windows gh0st Hijacking Scanner&tool
https://github.com/Cc28256/HijackScan
https://github.com/yuanyuanxiang/SimpleRemoter

php,jsp,asp webshells
https://github.com/LandGrey/webshell-detect-bypass

trojan
https://github.com/p4gefau1t

sql injection
https://github.com/tariqhawis/injectbot
https://github.com/sqlmapproject
https://github.com/shack2/SuperSQLInjectionV1
https://blog.csdn.net/qq_39678161/article/details/119908354?ops_request_misc=%257B%25
https://blog.csdn.net/elephantxiang/article/details/114272407?ops_request_misc=%257B%2

tool-set
왠만한건 이 두개로 수정하면서 쓰면 다 가능하다고
https://github.com/Z4nzu/hackingtool
https://github.com/Manisso/fsociety

해킹관련 중국툴 및 검색 (중국에서 사용하는 왠만한 스크립툴들은 다 여기 있다고 합니다)
https://github.com/taielab/awesome-hacking-lists

sql dump tool
https://github.com/uknowsec/SharpSQLDump
```

Main OS – Kali Linux / Windows 10

Chinese Tools

Most attacks are possible using the two tools as belows

How to find Chinse tools related to hacking

Figure 6: 해킹툴 link.txt.

As shown in Figure 6, the text file mentions the tools mainly used for the attack and information on the referenced community. @zerocool888 does not use RCE or zero-days, but it is presumed that use is made of the SQL injection scan tool that is open to the open web.

In fact, the following characteristics were found on the compromised website sold by @zerocool888:

- The admin login page is exposed on the main page of the website.
- An input form exists on the main page of the website.
- The vulnerability has not been patched because it has been out of operation for a long time, and an outdated version of the web framework is being used.

Bitcoin transaction analysis

@zerocool888 used Tumbler for mixing Bitcoin

Through the conversation with @zerocool888, we were able to obtain information that @zerocool888 is using a Bitcoin wallet address. The flow of funds was analysed based on the transfer transaction in the corresponding Bitcoin wallet address.

The information on @zerocool888's Bitcoin wallet address is as follows:

- Bitcoin wallet address: 3N2sZrtUFU2PguCZDYEMFKRG5DMoE4dyzA (Balance: 0 BTC)
- First seen: 24 November 2021
- Total received: 0.01006039 BTC
- Total sent: 0.01006039 BTC
- Total transactions: three

Result of Bitcoin transaction analysis

A total of two input transactions and one output transaction were confirmed in the corresponding Bitcoin wallet address, and the fund flow of the output transaction was analysed. The results of the analysis are as follows:

1. 0.01006039 BTC sent from 3N2sZrtUFU2PguCZDYEMFKRG5DMoE4dyzA goes through the following two wallet addresses and 100% of the funds are transferred:

   • bc1qcxn54fl2zrlqgwyne50afs8fmh04vsgnrm34vs

   • bc1qmgylqq8at3ju65pjk7xvvr6euava2qj3mmwldp

2. Funds were transferred from bc1qmgylqq8at3ju65pjk7xvvr6euava2qj3mmwldp to two wallet addresses as shown in Figure 7.

   As a result, it is estimated that funds were transferred by dividing the two wallet addresses after performing the Bitcoin Tumbler operation to collect funds.

   - bc1q7dmjqztn342e7qyl4tlfyqc8mju8ny7me8vm4n – Bitcoin Tumbler address.

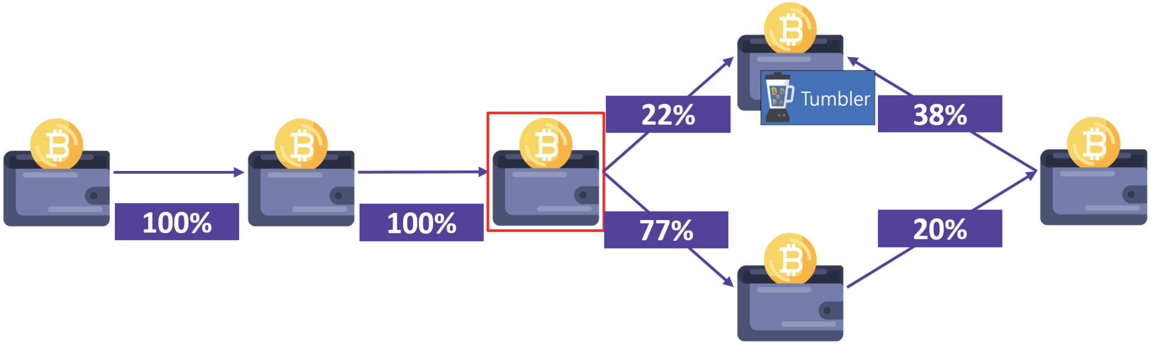


Figure 7: Screenshot of the result of Bitcoin transaction analysis.

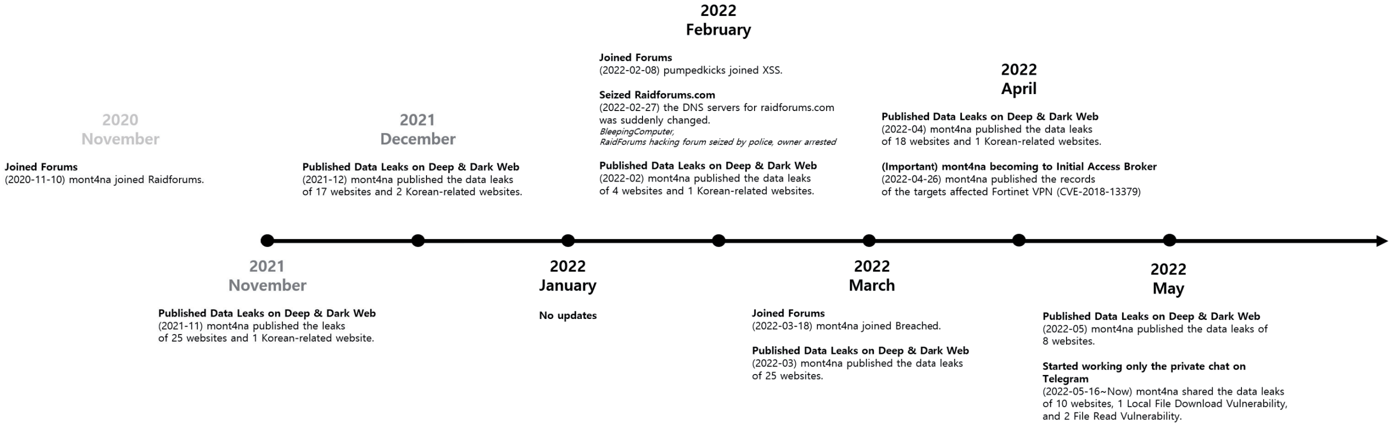
DATA BROKER & INITIAL ACCESS BROKER @MONT4NA

Overview

Next, we analysed the @mont4na user who sold a database related to the website of a large Korean company, the website of an international company, and information leaked by employees. @mont4na signed up for RaidForums on 10 November 2020, and on 22 January 2021 wrote a post on RaidForums with the title 'TXT nmmoney.xyz', selling leaked email and password information.

Timeline

Figure 8 shows a timeline of the activities of @mont4na from 2021 to 2022.



2020 November

Joined Forums
(2020-11-10) mont4na joined Raidforums.

2021 November

Published Data Leaks on Deep & Dark Web
(2021-11) mont4na published the leaks
of 25 websites and 1 Korean-related website.

2021 December

Published Data Leaks on Deep & Dark Web
(2021-12) mont4na published the data leaks
of 17 websites and 2 Korean-related websites.

2022 January

No updates

2022 February

Joined Forums
(2022-02-08) pumpedkicks joined XSS.

Seized Raidforums.com
(2022-02-27) the DNS servers for raidforums.com
was suddenly changed.
BleepingComputer,
RaidForums hacking forum seized by police, owner arrested

Published Data Leaks on Deep & Dark Web
(2022-02) mont4na published the data leaks
of 4 websites and 1 Korean-related websites.

2022 March

Joined Forums
(2022-03-18) mont4na joined Breached.

Published Data Leaks on Deep & Dark Web
(2022-03) mont4na published the data leaks
of 25 websites.

2022 April

Published Data Leaks on Deep & Dark Web
(2022-04) mont4na published the data leaks
of 18 websites and 1 Korean-related websites.

(Important) mont4na becoming to Initial Access Broker
(2022-04-26) mont4na published the records
of the targets affected Fortinet VPN (CVE-2018-13379)

2022 May

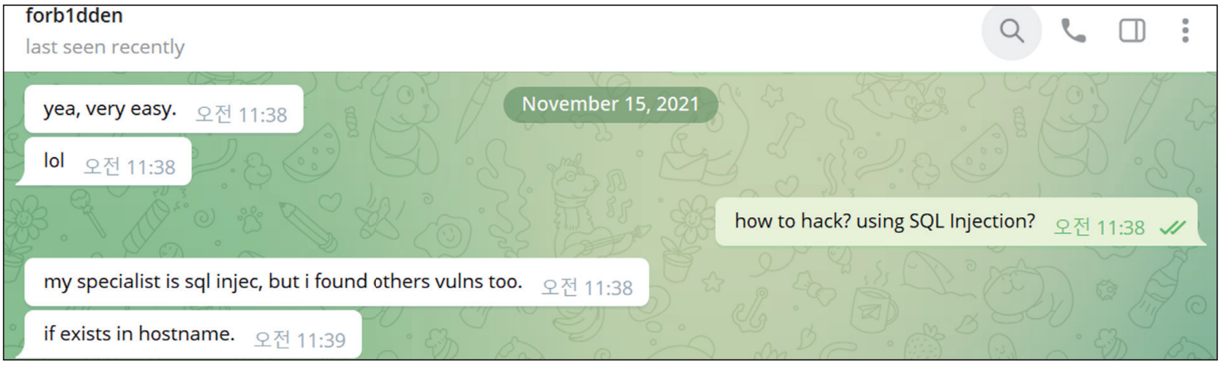
Published Data Leaks on Deep & Dark Web
(2022-05) mont4na published the data leaks of
8 websites.

Started working only the private chat on Telegram
(2022-05-16~Now) mont4na shared the data leaks
of 10 websites, 1 Local File Download Vulnerability,
and 2 File Read Vulnerability.

Figure 8: The activities of @mont4na from 2021 to 2022.

The activities of @mont4na

From 28 October 2021, @mont4na started selling website-related databases and employee-leaked information in earnest, selling a total of 42 corporate-related databases and various employee-leaked information in 2021. We confirmed that the actor mainly sells SQL injection vulnerability information and features of using sqlmap when attacking websites.



forb1dden
last seen recently

November 15, 2021

yea, very easy. 오전 11:38

lol 오전 11:38

how to hack? using SQL Injection? 오전 11:38

my specialist is sql injec, but i found others vulns too. 오전 11:38

if exists in hostname. 오전 11:39

Figure 9: Screenshot of the communication with @mont4na.

Figure 9 shows a conversation with @mont4na through *Telegram*. @mont4na claimed to be confident in SQL injection, and the data sold on dark web forums mainly sold SQL injection vulnerability information. The following is sample information shared by @mont4na for database sales:

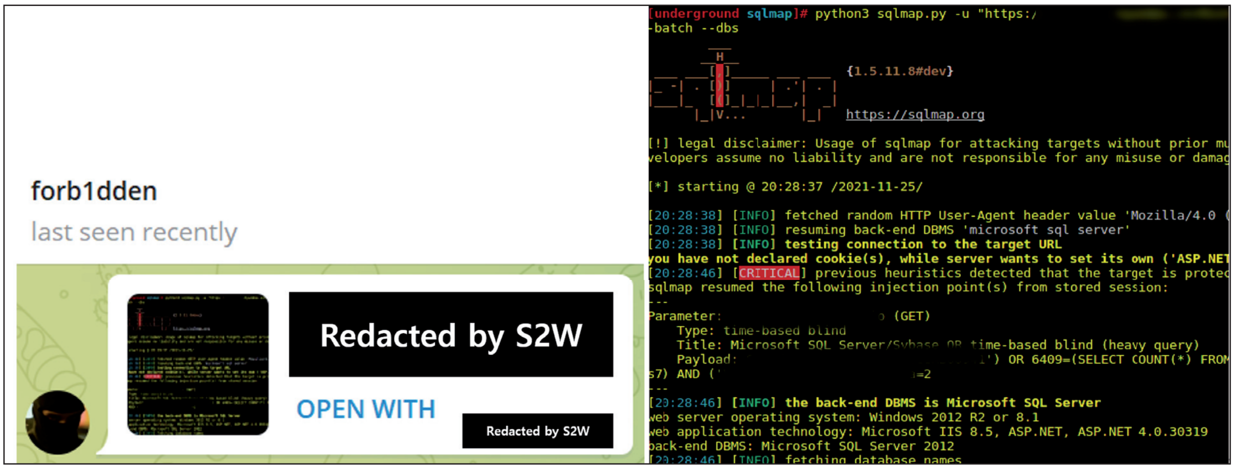
```
SQLi // AVAILABLE
{Redacted by S2W}
--is-dba = root@localhost
DB NAMES:
available databases [10]:
{Redacted by S2W}
```

Sample 1: Information shared by @mont4na for database sales.

Deep analysis of @mont4na

@mont4na usually uses sqlmap

On 26 November 2022, @mont4na shared with potential buyers some samples of SQL injection vulnerabilities related to specific companies. Figure 10 shows a screenshot of an attempt to perform an SQL injection attack using the sqlmap received from @mont4na.



forb1dden

last seen recently

Redacted by S2W

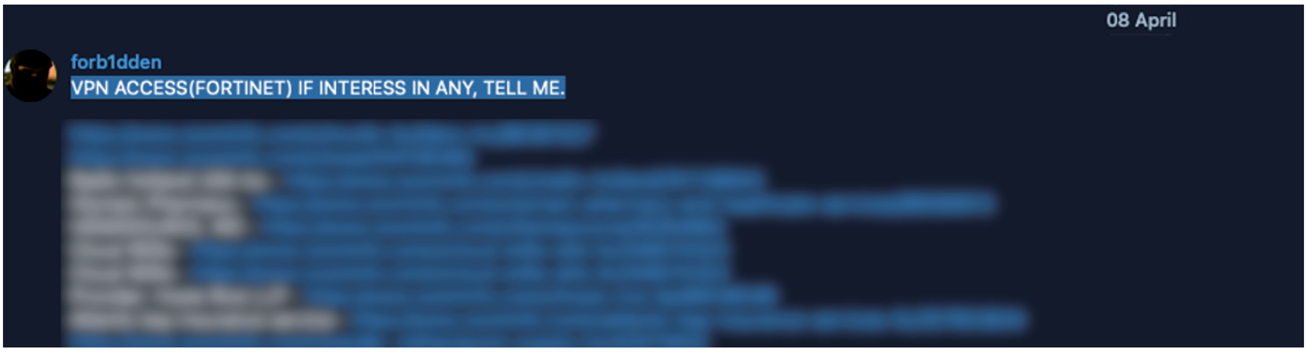
OPEN WITH

Redacted by S2W

```
[underground sqlmap]# python3 sqlmap.py -u "https:/ [redacted]
-batch --dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.11.8#dev}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
velopers assume no liability and are not responsible for any misuse or damag

[*] starting @ 20:28:37 /2021-11-25/

[20:28:38] [INFO] fetched random HTTP User-Agent header value 'Mozilla/4.0 (
[20:28:38] [INFO] resuming back-end DBMS 'microsoft sql server'
[20:28:38] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('ASP.NET
[20:28:46] [CRITICAL] previous heuristics detected that the target is protec
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: [redacted] (GET)
    Type: time-based blind
    Title: Microsoft SQL Server/Sybase OR time-based blind (heavy query)
    Payload: [redacted]') OR 6409=(SELECT COUNT(*) FROM
s7) AND ([redacted]=2
---
[20:28:46] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2012 R2 or 8.1
web application technology: Microsoft IIS 8.5, ASP.NET, ASP.NET 4.0.30319
back-end DBMS: Microsoft SQL Server 2012
[20:28:46] [INFO] fetching database names
```

Figure 10: Screenshot of the communication with @mont4na.

Through the sample, it was confirmed that @mont4na had tested the SQL injection vulnerability on a specific website by using the option included in the sqlmap tool, and actually steals and sells the database of the website where the SQL injection vulnerability exists. Recently, in addition to the SQL injection vulnerability, information related to VPN connection information, web shell, file read vulnerability, and local file download vulnerability were also sold.



08 April

forb1dden

VPN ACCESS(FORTINET) IF INTERESS IN ANY, TELL ME.

[redacted]

Figure 11: Screenshot of the message about selling VPN access.

15 May

forb1dden

WEBSHELL - [redacted]

Redacted by S2W

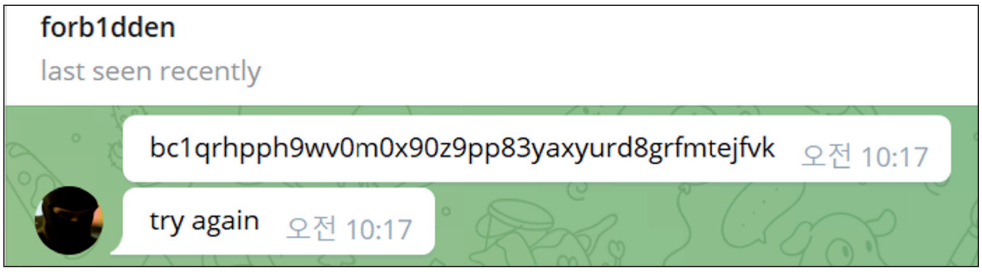
Figure 12: Screenshot of the message about selling web shell.

Bitcoin transaction analysis

@mont4na used Bitcointoyou and Mercado Bitcoin for exchanging Bitcoin

Through the conversation with @mont4na, we were able to obtain information about the Bitcoin wallet address being used by the actor. The flow of funds was analysed based on the transfer transaction in the corresponding Bitcoin wallet address.

- Bitcoin wallet address: bc1qrhpph9wv0m0x90z9pp83yaxyurd8grfmtejfvk (Balance: 0.44806273 BTC)
- First seen: 8 June 2021
- Total received: 1.53574364 BTC
- Total sent: 1.08768091 BTC
- Total transactions: 204



forb1dden

last seen recently

bc1qrhpph9wv0m0x90z9pp83yaxyurd8grfmtejfvk 오전 10:17

try again 오전 10:17

Figure 13: Screenshot of the communication with @mont4na.

Result of Bitcoin transaction analysis – (1) @mont4na used Bitcointoyou exchange

A total of 174 input transactions and 30 output transactions were confirmed in the corresponding Bitcoin wallet address, and the fund flow of the output transactions was analysed. The results are as follows:

1. Of the 1.08768091 BTC sent from bc1qrhpph9wv0m0x90z9pp83yaxyurd8grfmtejfvk, some of the funds went through the following three wallet addresses:
   - 3MDKhAuSo7zvVo21ZW6DNdghqFFQp2qWV5
   - 32odwQMeXPkKz6Nmb3rgayPBoGbDFeDc39
   - 34gWznW1hsaBP6bUFCH8ygRLEkAmigdZt4
2. As shown in Figure 14, it is estimated that most funds were collected at 32dmTJGu8Maq4AB8afhWK65B1s84hhqo5M and then the Bitcointoyou exchange was used.

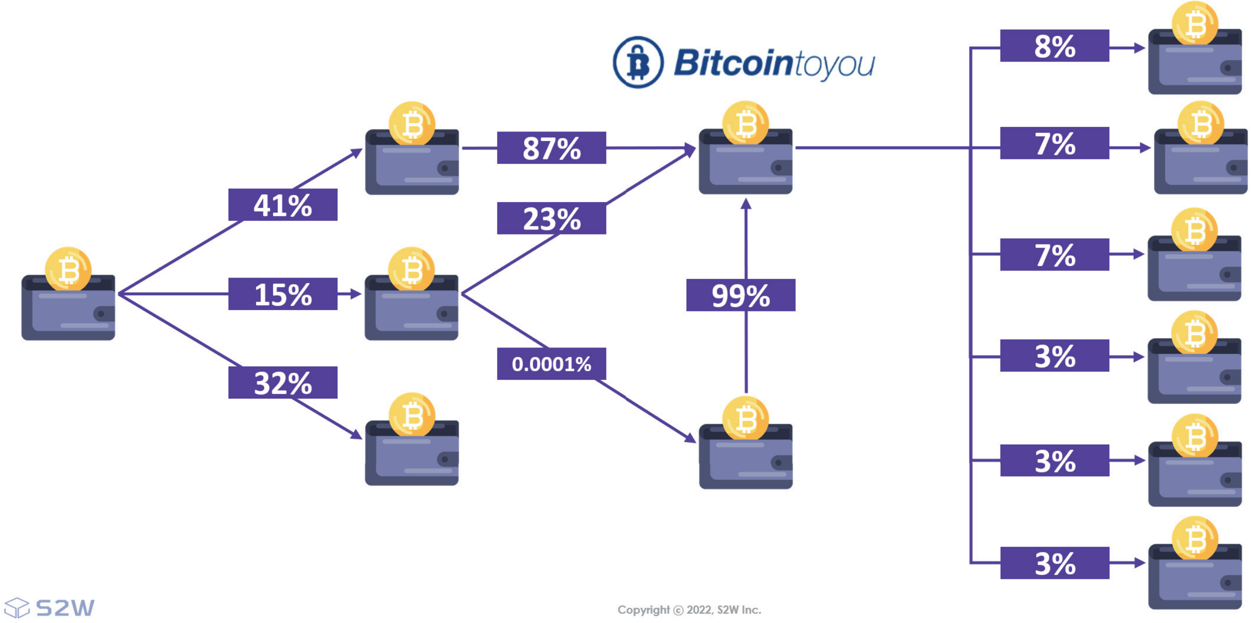


Figure 14: Screenshot of the communication with @mont4na.

Result of Bitcoin transaction analysis – (2) @mont4na used Mercado Bitcoin exchange

The flow of transfer funds was analysed for the transfer transaction ID below. The analysis results are as follows:

1. It is assumed that most of the funds were transferred to the wallet address of the Mercado Bitcoin exchange.
2. The Mercado Bitcoin exchange is confirmed as a cryptocurrency exchange headquartered in Brazil.
   - Outgoing TX ID: eed9640b608f6899af97d3ac0bd475bc78f61bba988b7d21144f7fa20530e96e
   - Date: 3 May 2022
   - Volume: 0.02303557 BTC

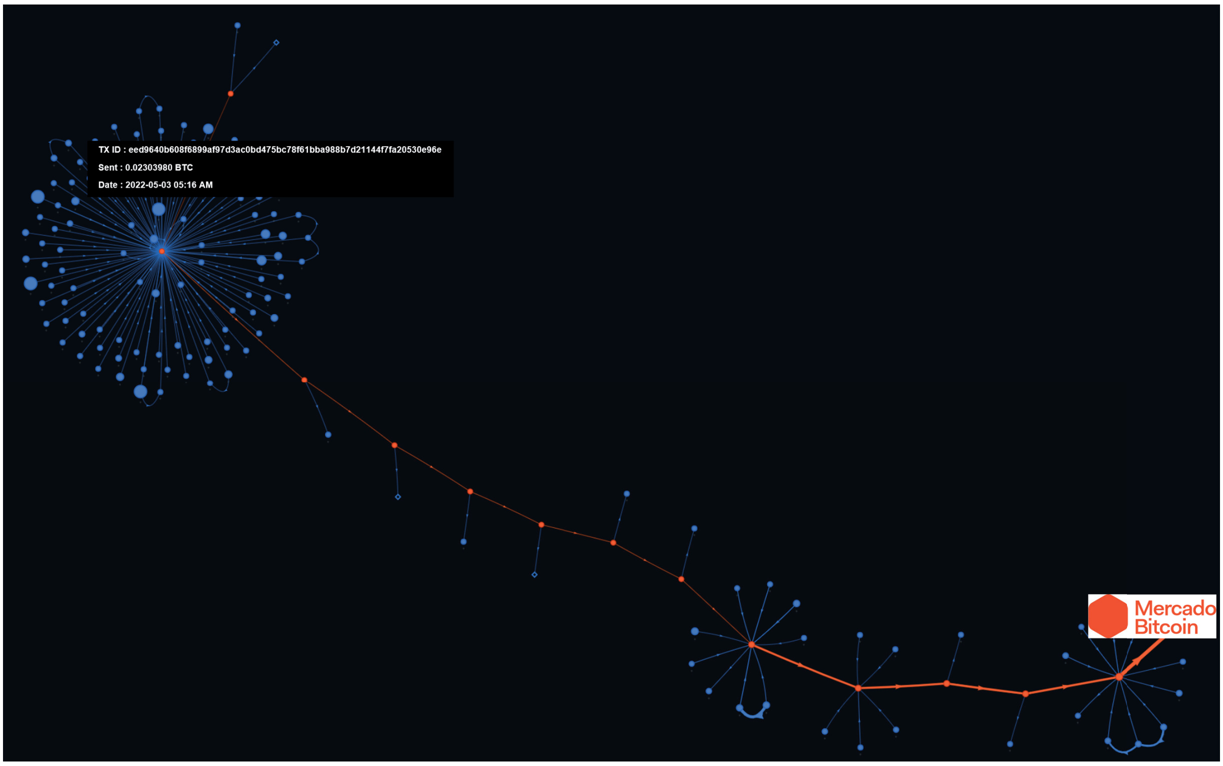

TX ID : eed9640b608f6899af97d3ac0bd475bc78f61bba988b7d21144f7fa20530e96e
Sent : 0.02303980 BTC
Date : 2022-05-03 05:16 AM

Figure 15: Screenshot of the communication with @mont4na.

SCRIPT KIDDY ON THE DEEP & DARK WEB: LOOKS SERIOUS? BUT EMPTY SUIT!

@zerocool888 and @mont4na are not nation state attack groups, they are not attack groups that have been active in the deep & dark web forums for a long time, and are not threat actors with advanced hacking skills. @zerocool888 sold information that other users have already shared for free on *Telegram* on the RaidForums forum, and @mont4na uses sqlmap to target a website with a valid SQL injection vulnerability. They are script kiddies.

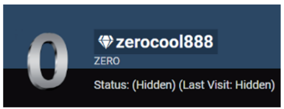
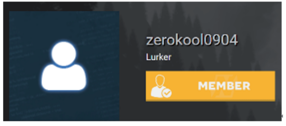
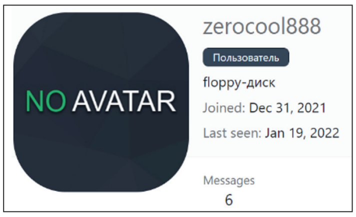
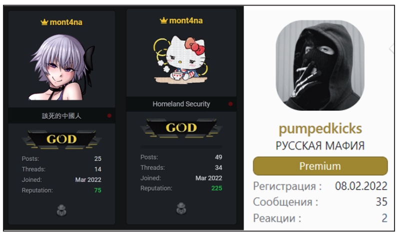
@zerocool888 zerocool888 is Korean, living in Hong Kong	**@mont4na (a.k.a. pumpedkicks)**
 zerocool888 ZERO Status: (Hidden) (Last Visit: Hidden)  zerokool0904 Lurker MEMBER  NO AVATAR zerocool888 Пользователь floppy-диск Joined: Dec 31, 2021 Last seen: Jan 19, 2022 Messages 6	 mont4na 該死的中國人 GOD Posts: 25 Threads: 14 Joined: Mar 2022 Reputation: 75 mont4na Homeland Security GOD Posts: 49 Threads: 34 Joined: Mar 2022 Reputation: 225 pumpedkicks РУССКАЯ МАФИЯ Premium Регистрация : 08.02.2022 Сообщения : 35 Реакции : 2
Telephone number: - +852 5 *** **14 - +852 4 *** **25 Gmail: zerocoke520@gmail.com Telegram ID: - @zerocool888 - @zerocoolplus Joining dates of deep & dark web forums: - (2021-11-11) zerocool888 joined RaidForums - (2021-11-13) zerocool888 joined XSS - (2021-12-31) zerokool0904 joined Nulled Bitcoin wallet address: - 3N2sZrtUFU2PguCZDYEMFKRG5DMoE4dyzA	Telegram ID: @jfq666 Joining dates of deep & dark web forums: - (2020-11-10) mont4na joined RaidForums - (2020-12-31) mont4na joined XSS - (2022-02-08) pumpedkicks joined XSS - (2022-03-18) mont4na joined Breached Bitcoin wallet address: - bc1qrhpph9wv0m0x90z9pp83yaxyurd8grfmtejfvk Used hacking tools: - sqlmap

Table 2: The profiles of @zerocool888 and @mont4na.

The targets they attacked include well known companies in each country, and websites that people use daily. In the case of @zerocool888, the data leaked several times has already been sold on *Telegram* or other forums (XSS, DeepMix, RaidForums). In the case of @mont4na, the sqlmap tool was mainly used to sell website information with valid SQL injection vulnerabilities. Data leakage may look serious when we look at the title, but when we check the data, it is often an empty suit.

However, in some cases, valid personal information or corporate credential information was sold. We should focus on the fact that they steal information from key companies and websites in certain countries using only open source-based hacking attack tools.

This work was supported by an Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No.2022-0-00740, The Development of Darkweb Hidden Service Identification and Real IP Trace Technology).