vb 2023 LONDON

4 - 6 October, 2023 / London, United Kingdom

SHEEP'S CLOTHING OF DEEP & DARK WEB OPERATORS: THERE ARE NO SECRETS YOU CAN HIDE FOREVER

Youjin Lee, Kyunghee Kim, Jungyeon Lim & Dasom Kim

S2W, Republic of Korea

primarily@s2w.inc
kkh4y@s2w.inc
jungyunl@s2w.inc
ds_none028@s2w.inc

ABSTRACT

On 31 January 2022, Coelho (a.k.a. Omnipotent), the operator of RaidForums, was arrested in the United Kingdom. Subsequently, many existing RaidForums users migrated to the Breached forum. However, the operator of the Breached forum was also recently apprehended in New York.

According to a report released by *Flashlight* in 2023, deep and dark web (DDW) forums follow a certain creation cycle and circulate periodically. The Threat Detection Team at *S2W Threat Analysis Center* has conducted an analysis on approximately 30 active DDW forums, focusing on their operational cycles, active user counts, and post regeneration rates. Through this analysis, new benchmarks for major and minor forums have been discovered and will be shared.

A comparative and statistical analysis was conducted on the selected operators of three major forums in the deep dark web. Additionally, profiling results revealed that some operators used fake profiles on the surface web, but hints about their actual identities were hidden. During the process of their apprehension, commonalities and differences were identified between the confirmed identities and the hints they left behind. These findings will be presented.

This paper is based on articles and information available until 13 June 2023. The times mentioned in this paper are in KST (UTC+09:00).

THE LIFE CYCLE OF DDW FORUMS

According to a report released by *Flashpoint* in 2023 [1], it has been observed that forums have life cycles based on their creation periods. When a forum is initially created, it begins promotional activities such as advertising and events to attract users from other existing forums. As a result, the newly established forum experiences a surge in active users, and it either continues to operate and expand its scale or undergoes takedown/exit, leading to one of the two processes.

In cases where a forum is taken down or exits, users who were active on that forum may create and operate a new forum.

Figure 1: Cycle of takedowns and new markets. Source: [1].

We have been collecting DDW forum posts since 2014, and our data for post counts over the period from 2014 to 2023 is as shown in Figure 2. As can be seen in Figure 2, there was a stable trend until 2019, but a steady increase in post activity can be observed, with a sudden surge in posting volume starting in 2021. This indicates that DDW forums began to undergo active changes around 2020.

In particular, March 2020 marked the start of the COVID-19 pandemic. According to a 2023 report by *Kaspersky* [2], job postings within the dark web increased by approximately 6% after 2020. The report indicated that job categories such as reverse engineer, tester and designer became more specialized, leading to an expansion of the job market. Additionally, an article published by *Cointelegraph* [3] in May 2020 reported that dark web Bitcoin transactions saw a 65% increase in the first quarter of 2020.

In Figure 3 the number of DDW forum posts mentioning the keywords 'bitcoin' and 'job' can be seen in green and blue, respectively. Both show rapid growth starting from 2020, indicating a similar pattern to the increased activity on DDW forums attributed to the COVID-19 pandemic and the surge in Bitcoin transactions in 2020.

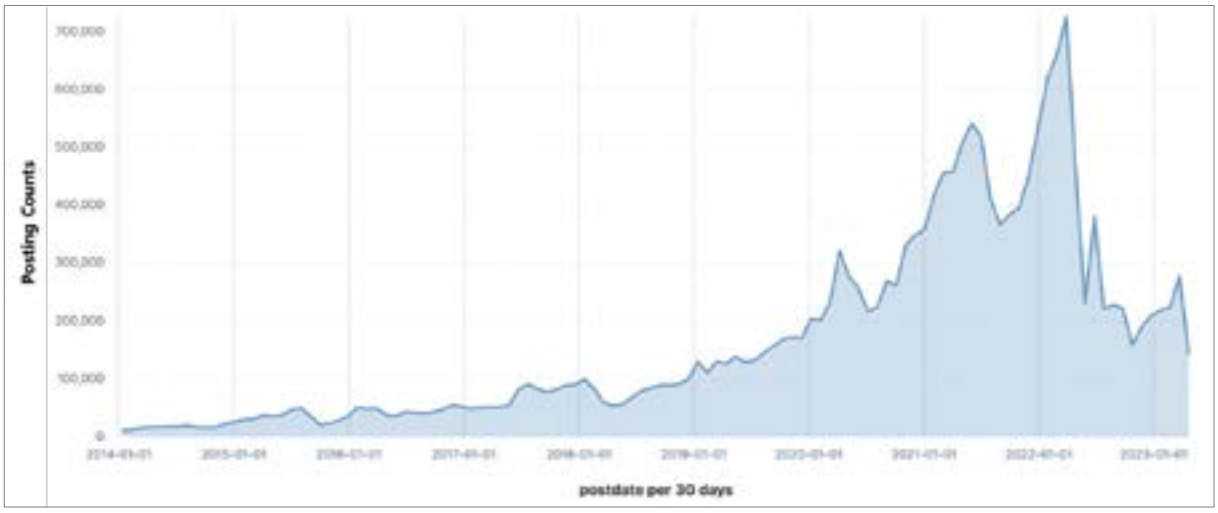


Figure 2: DDW forum post counts.

Figure 3: DDW forum post counts with 'bitcoin' or 'job' keyword.

Among the deep and dark web forums, the ones that experienced a significant increase in post activity from 2020 onwards were RaidForums, Breached and Leakbase. RaidForums operated in a stable manner until 2020, but an increase in posts was observed in the second half of 2019, with a sharp rise in post volume in 2020. As for the Breached forum, activity started increasing from the second half of 2022, after its opening. Leakbase, on the other hand, witnessed a sudden surge in post volume immediately after the closure of the Breached forum.

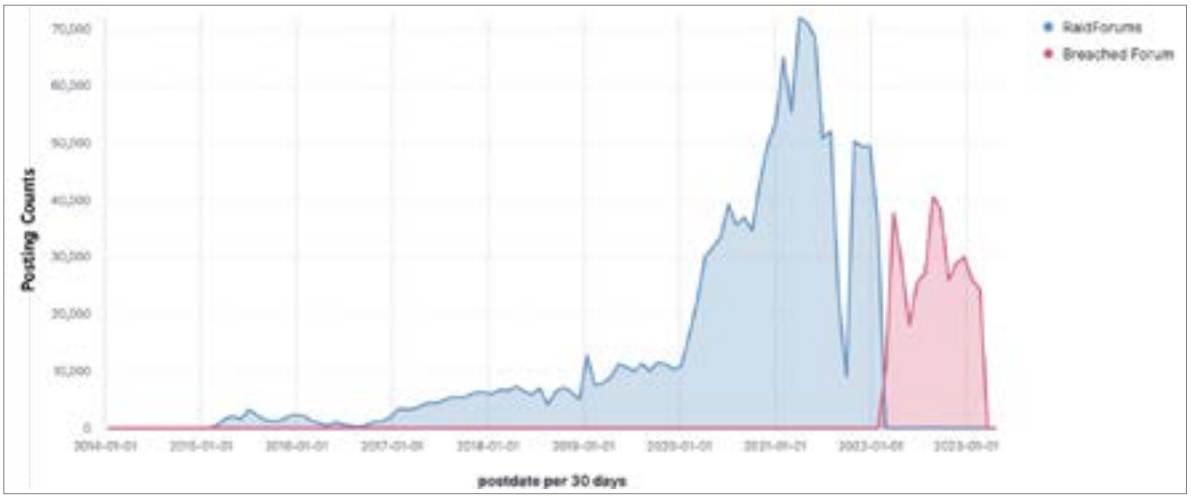


Figure 4a: Post counts on RaidForums and Breached.

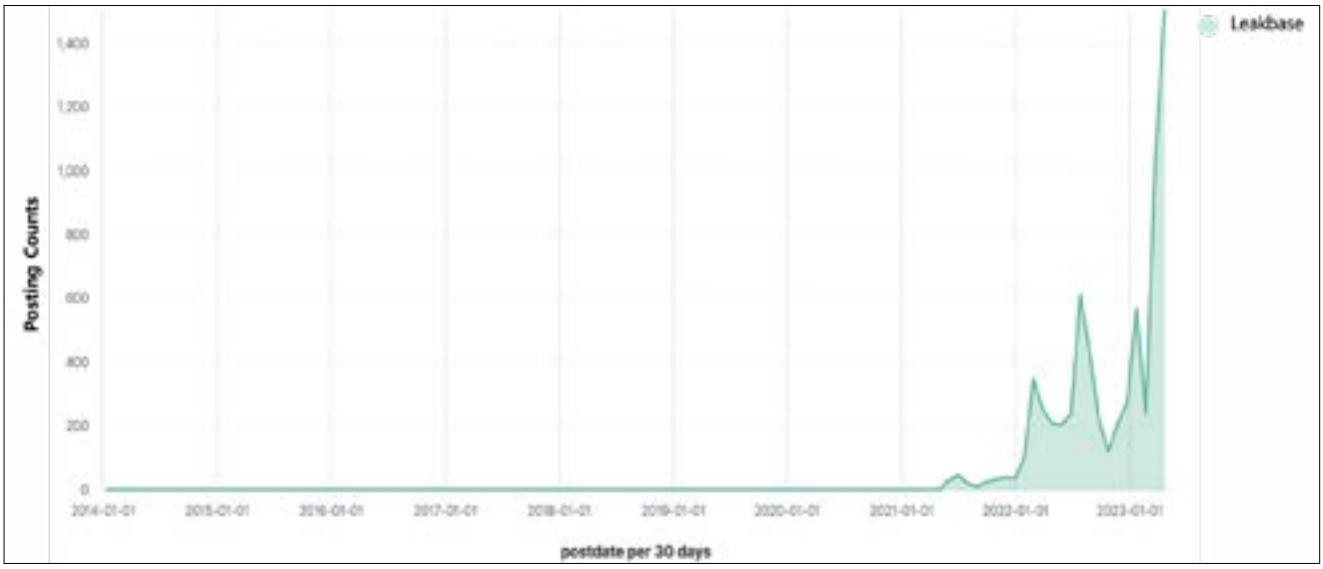


Figure 4b: Post counts on Leakbase.

PROFILING OF OPERATORS OF DDW FORUMS

We have conducted profiling on the operators of selected major forums: RaidForums (operated by Omnipotent), Breached (operated by Pompompurin), and Leakbase (operated by Chucky).

Omnipotent (RaidForums)

First, we conducted profiling on Omnipotent, the operator of RaidForums. Omnipotent joined RaidForums on 15 March 2015, and started their activities. RaidForums was operated until January 2022, and was consistently maintained by Omnipotent without any change in operators during its operation.

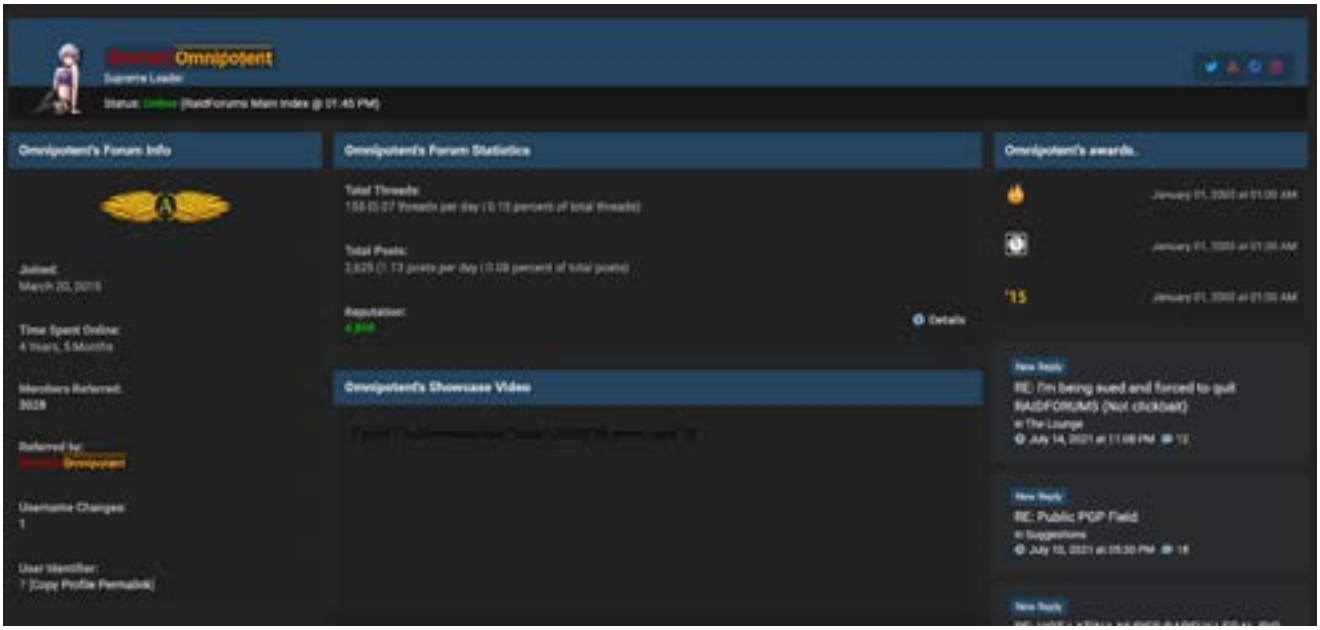


Figure 5: Omnipotent's profile on RaidForums.

Omnipotent began operating a personal *Twitter* account in October 2014. The *Twitter* handle was '1dot3dot3dot7', and the profile indicated that they were the operator, developer and host of RaidForums. The term '1337' is commonly used among hackers and is a shorthand for 'elite hacker' and 'leetspeak'. The IP is displayed as '134.11.13[.]37', but this appears to be a modification of the numbers 1337 in an IP format and does not hold significant meaning. At the time of writing this paper, the account has been suspended on *Twitter* and further information about it is no longer accessible.

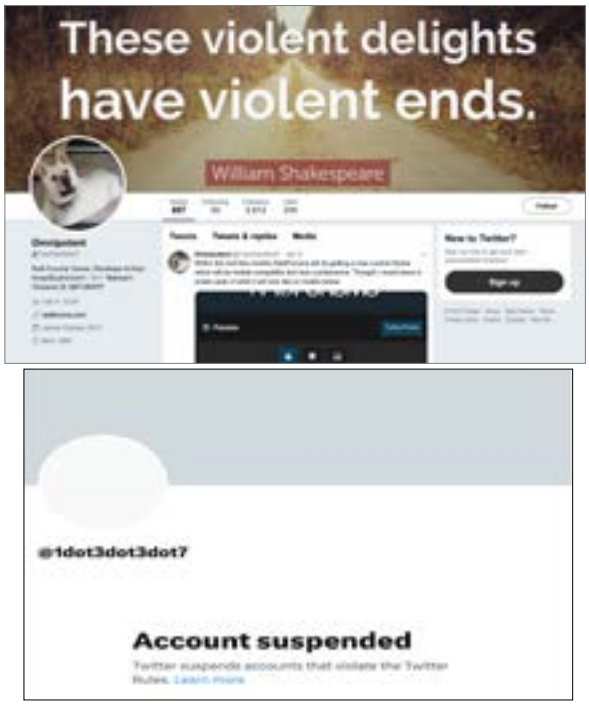


Figure 6: Omnipotent's Twitter account.

Omnipotent also maintained a personal *GitHub* account. He mentioned RaidForums and stated in his profile that he was a 'LEMP Stack Developer & SysAdmin'. In addition, the Miuna Shoutbox source code used on RaidForums and another domain of RaidForums, 'https://rf[.]to', was found on his *GitHub* account. However, the most noteworthy point about his *GitHub* account is that he specified his location as the United Kingdom.

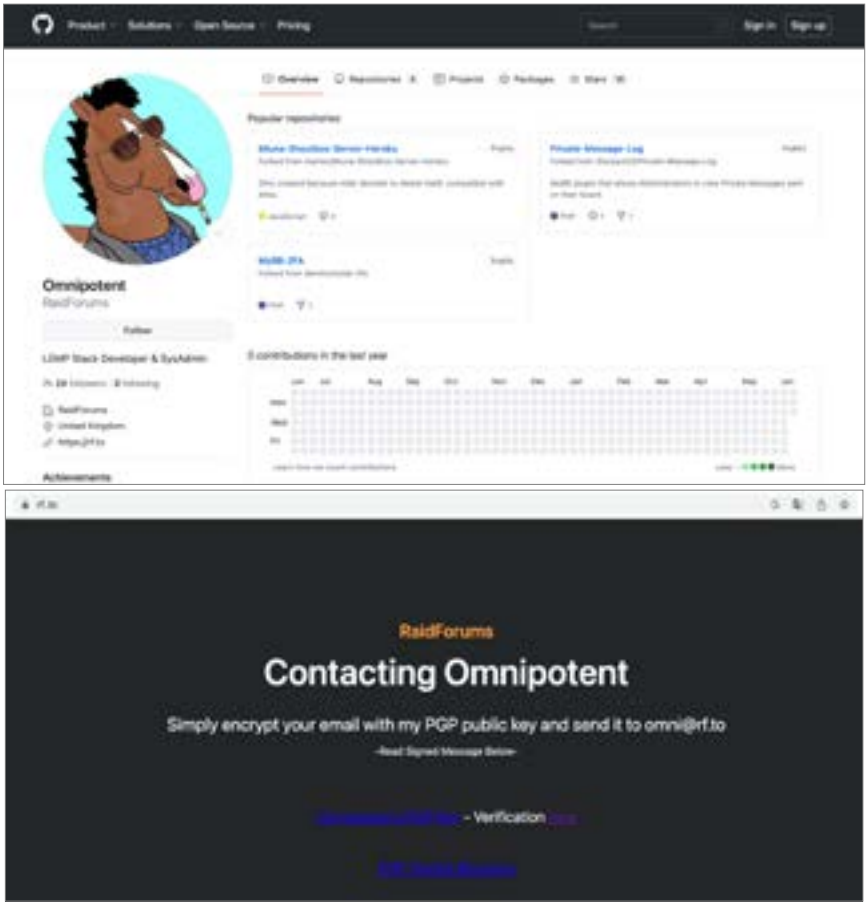


Figure 7: Omnipotent's GitHub account and rf.to website.

It was possible to verify Omnipotent's *Keybase* account on *GitHub*. He was using the username 'predator' and had listed the websites he operates and a Bitcoin address.

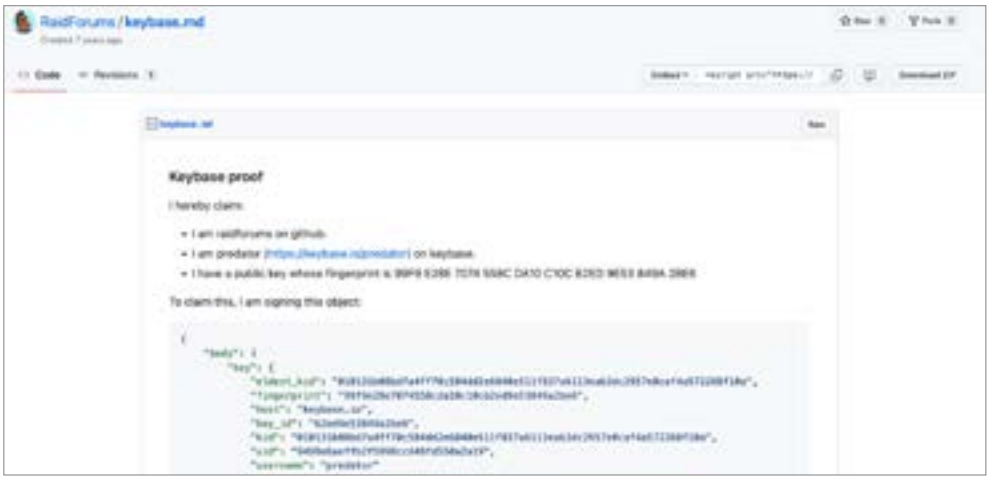


Figure 8: Keybase information recorded by Omnipotent on GitHub.

His *Keybase* account was consistently updated from 2019 to 2021. The domains rf.ws, negr.ooo and raid.lol were all identified as domains redirecting to RaidForums, while Rape.legal redirected to a nulled user profile page.

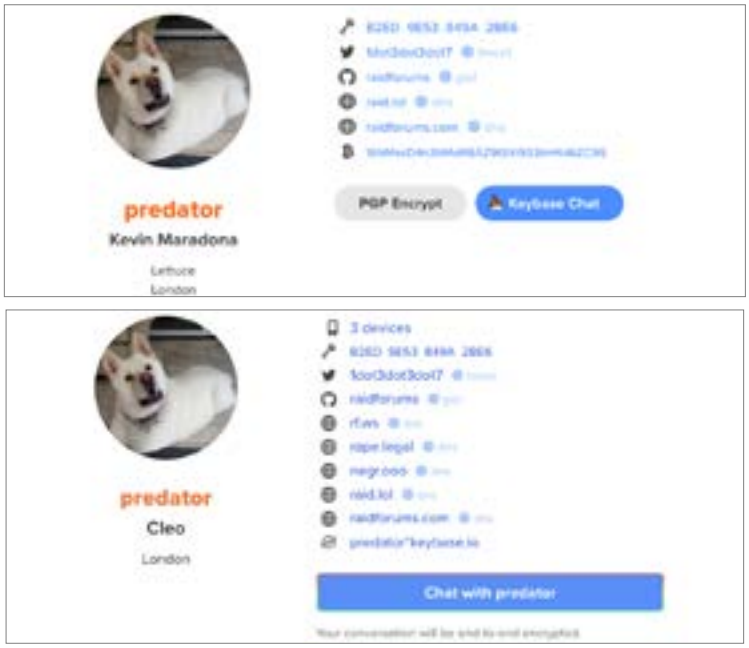


Figure 9: Omnipotent's Keybase account (top: March 2019; bottom: May 2020).

Table 1 shows a summary of the information gathered from Omnipotent's *Keybase* profile.

Num	Type	Content
01	Twitter	https://twitter[.]com/1dot3dot3dot7
02	GitHub	https://github.com/RaidForums
03	Site	https://raid[.]lol
04	Site	https://raidforums[.]com
05	Site	https://rf[.]ws
06	Site	https://rape[.]legal
07	Site	https://negr[.]ooo
08	BTC	16hMesD4n3hMoRBAZ9t9Xi933nH4d6ZC9S
09	Keybase	https://keybase[.]io/predator

Table 1: Profiling of Omnipotent.

According to the BTC transaction history, Omnipotent initiated his first transaction in April 2016 and had transactions recorded until August 2022.

Figure 10: Omnipotent's Bitcoin transactions.

Omnipotent listed his location as the United Kingdom on *GitHub* and as London on *Keybase*. It is worth noting that Coelho was indeed arrested in London, UK. This situation highlights the phrase 'Sometimes not adhering to OPSEC becomes the perfect OPSEC.'

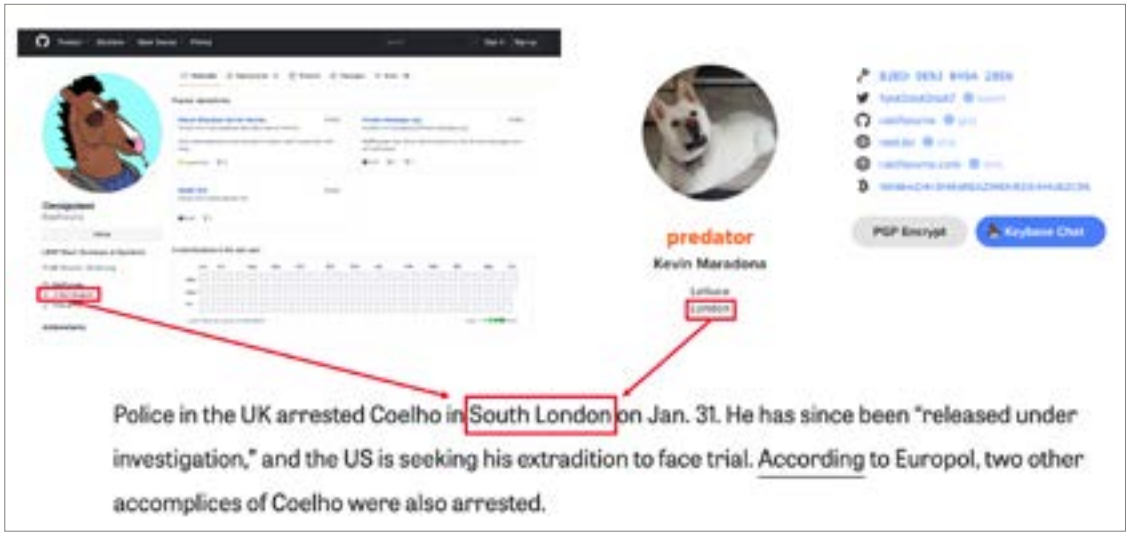


Figure 11: Residential area specified by Omnipotent.

Pompompurin (Breached)

Pompompurin started operating the Breached forum in May 2022. The Breached forum was run in a similar manner to RaidForums, and a credit system was also implemented similarly to RaidForums.

Figure 12: Pompompurin in the Breached forum.

Pompompurin operated personal blog sites 'https://pompur[.]in' and 'https://f[.]sb'. On the pompur[.]in site he listed a point of contact, and various social media accounts that he was operating could be found. On the f[.]sb site various proxy sites, including *Mastodon* and *Matrix* servers he operated, were listed. Additionally, his *GitHub* profile (https://github[.]com/pompompurins) was also discovered.

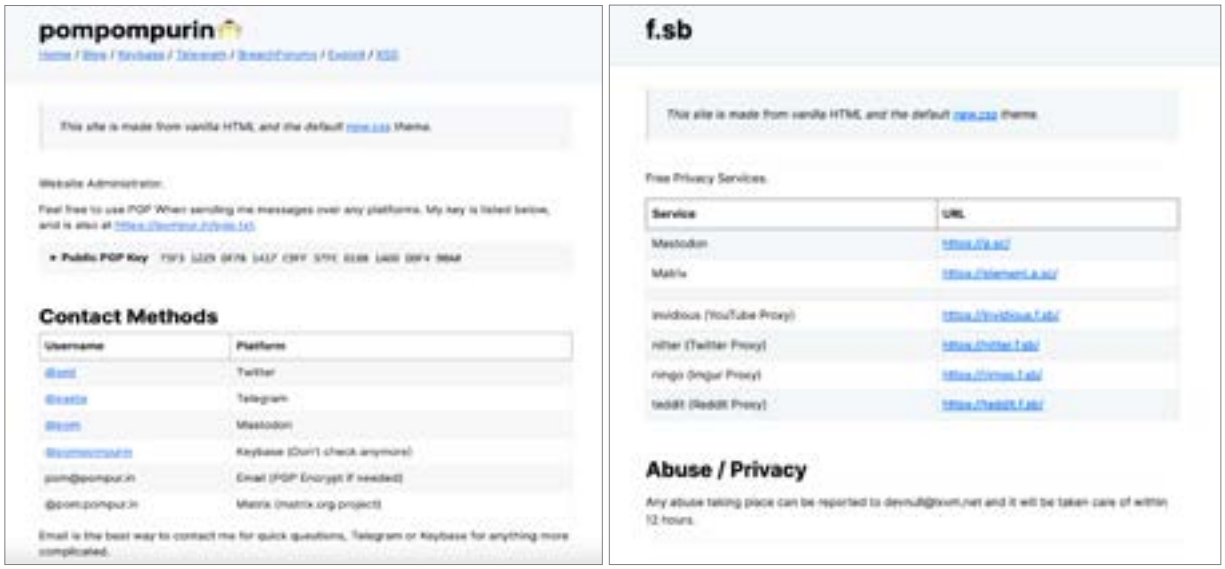


Figure 13: Left: Pompur[.]in site; right: f[.]sb site.

Pompompurin's *Twitter* account was created in April 2007. According to past records, posts were written primarily in Japanese up until July 2011, and most of the content appeared to be written by local Japanese individuals. However, in April 2022, there was a sudden shift where the account was reactivated and promotional posts for the Breached forum started appearing in English. Based on this information, it was determined that the account had been compromised by a user other than Pompompurin.

The profile mentioned an another account, @Whitepacketnet, but this is believed to be false. Additionally, the profile indicated that Pompompurin resided in Tokyo, Shibuya.

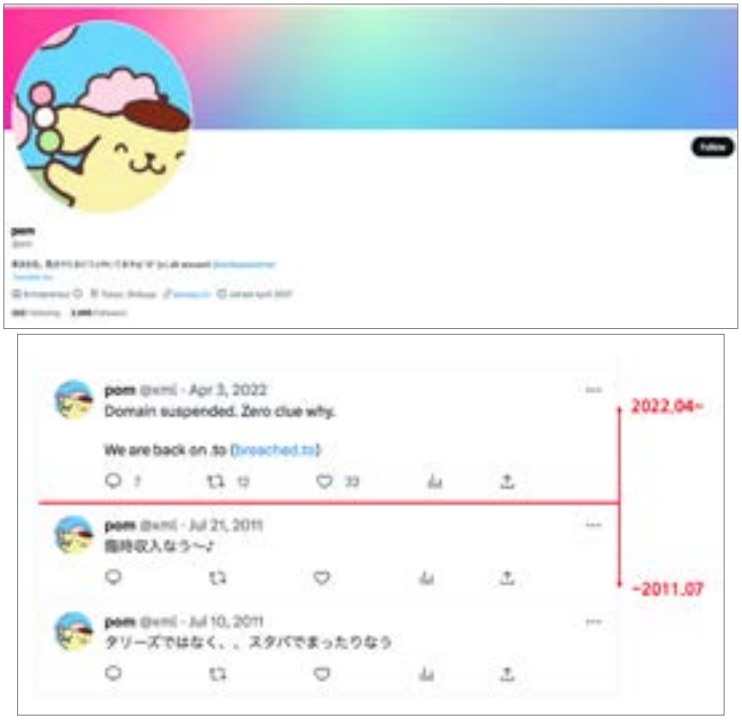


Figure 14: Top: Pompompurin's Twitter account; bottom: Twitter reactivation time point.

Like Omnipotent, Pompompurin also maintained *GitHub* and *Keybase* accounts, each of which listed the websites Pompompurin operated.

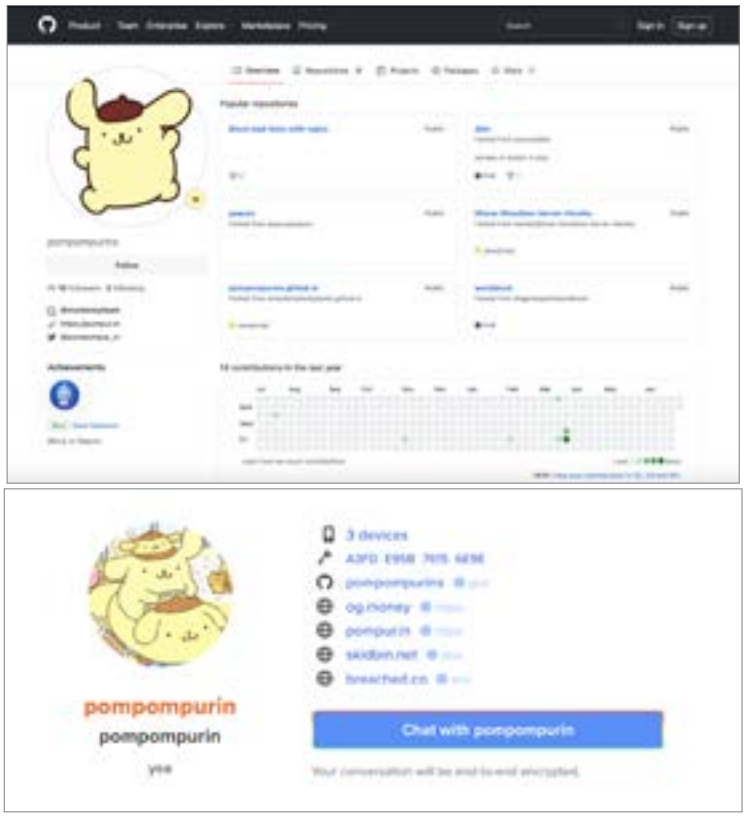


Figure 15: Top: GitHub; bottom: Keybase 2022.04.

Table 2 shows a summary of the information gathered from Pompompurin's blog and *GitHub* and *Keybase* accounts.

Num	Type	Content
01	Twitter	https://twitter[.]com/xml
02	Telegram	@paste
03	Mastodon	@pom
04	Keybase	https://keybase[.]io/pompompurin
05	Email	pom@pompur[.]in
06	Matrix	@pom:pompur[.]in
07	GitHub	https://github[.]com/pompompurins
08	Site	https://og[.]money
09	Site	https://pompur[.]in
10	Site	https://skidbin[.]net
11	Site	https://breached[.]co
12	Site	https://a[.]sc
13	Site	https://element.a[.]sc
14	Site	https://individious.f[.]sb
15	Site	https://rimgo.f[.]sb
16	Site	https://teddit.f[.]sb

Table 2: Profiling of Pompompurin.

It appears that one of the websites operated by Pompompurin, og[.]money, is an anonymous cloud file-hosting site. However, when accessing the main site, it reveals the official email address of *Night Lion Security*, a cybersecurity intelligence company. *Night Lion Security* has tracked Pompompurin in the past, and ironically, it seems that Pompompurin has taken advantage of the cyber intelligence analyst in this manner.

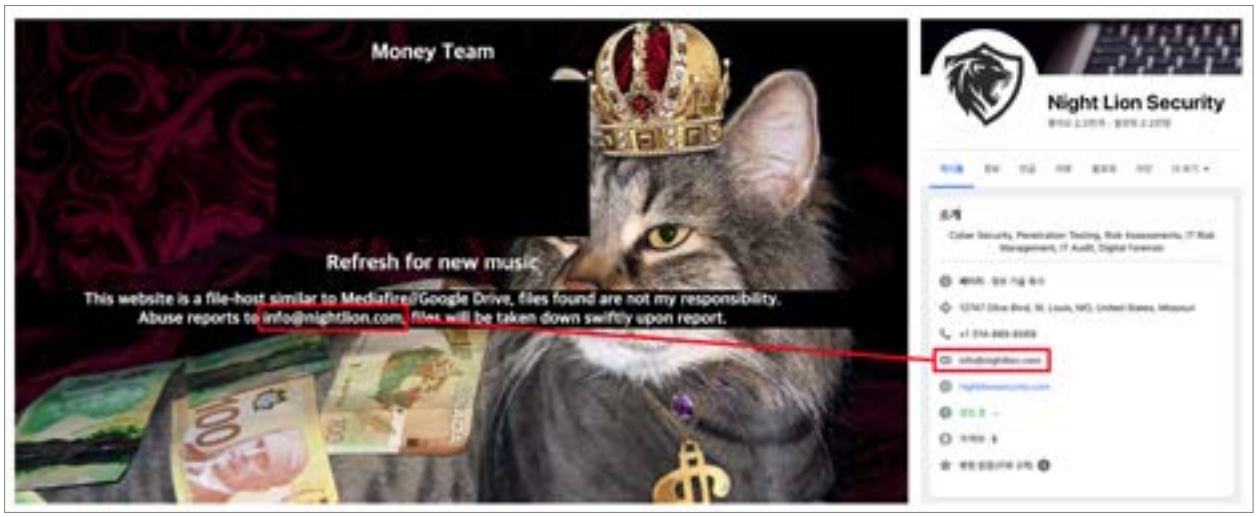


Figure 16: The email address associated with the og[.]money site matches that of Night Lion Security.

In addition to the og[.]money website, Pompompurin also operated Skidbin[.]net, an anonymous text hosting site, and a[.]sc, a social media site similar to *Mastodon*.

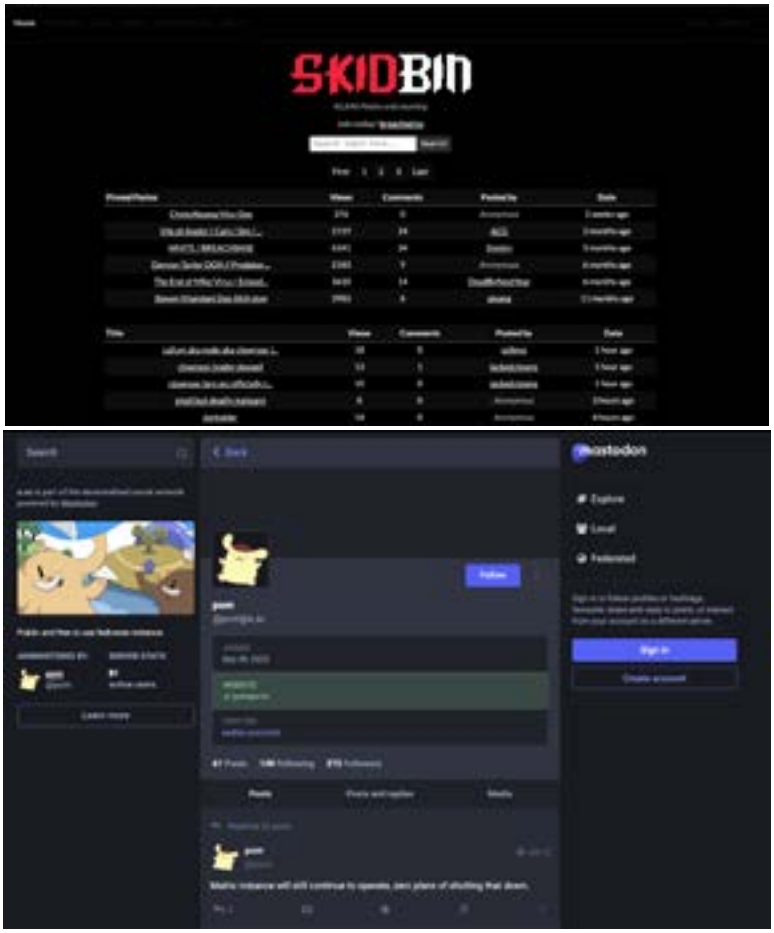


Figure 17: Top: Skidbin 2022.07; bottom: Mastodon 2023.02.

Chucky (Leakbase)

We have conducted profiling on Chucky, the operator of the Leakbase forum. Chucky joined the Breached forum in March 2022 and began activities by uploading SQL databases of specific corporate websites. The Leakbase forum, operated by Chucky, was opened in June 2021, before his activities on the Breached forum. Leakbase has established itself as a forum with over 8,000 active users currently.

Figure 18: Chucky's profile on the Leakbase forum.

Chucky also operates *Telegram* channels where various data, including leaked databases and stolen logs, are uploaded. Two prominent channels are Leaklogs Official and Leakbase Official.

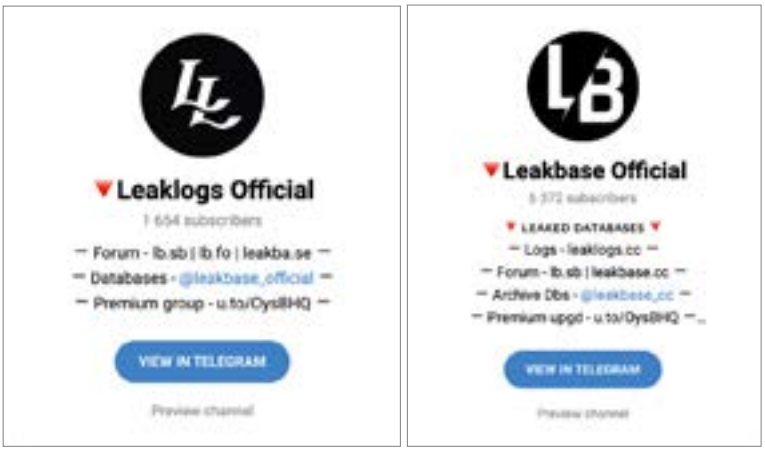


Figure 19: Telegram channels operated by Chucky, the operator of Leakbase.

Chucky has listed his *Telegram* account, '@bhfchucky', on the Leakbase[.]cc forum. Through this account, his activity history on the BHF forum was discovered. He has provided his *Qiwi*, *BTC*, *Skype*, *ICQ*, *Jabber* and *Telegram* accounts on the BHF forum.

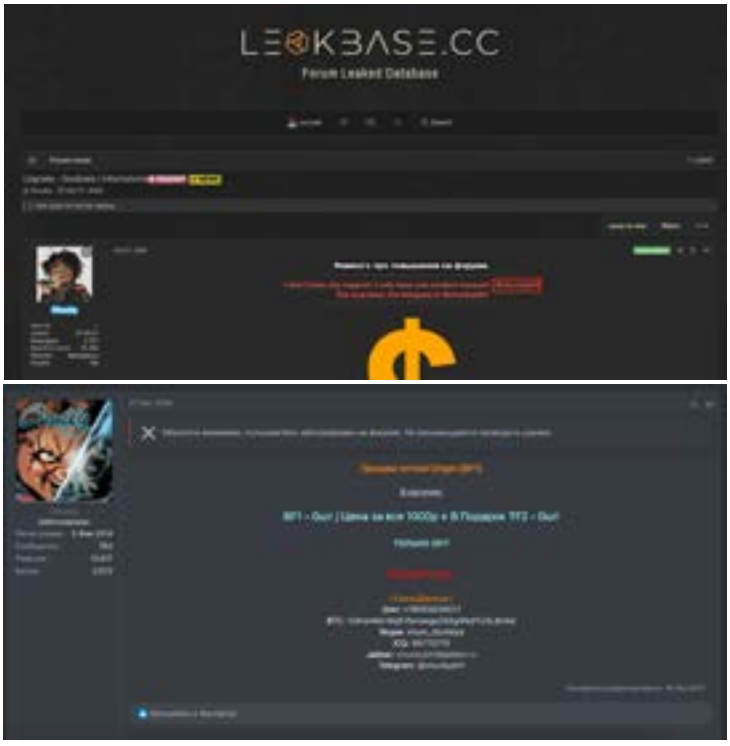


Figure 20: Top: Leakbase forum; bottom: BHF forum.

Table 3 shows a summary of the information gathered from Chucky's presence on Leakbase[.]cc and the BHF forum.

Num	Type	Content
01	Telegram	@chuckybhf
02	Qiwi	+790X503X017
03	BTC	124rsHMv16qKVbnowgqTdXg4NdYU3L8nXw
04	Skype	shum_dozhdya
05	ICQ	99770770
06	Jabber	chuckybhf@jabber.ru
07	Site	https://leakbase[.]cc

Table 3: Profiling of Chucky.

It has been confirmed that Chucky's *Skype* account is listed as 'Chucky | Mailpass.pw', and the location is given as Russian Federation.

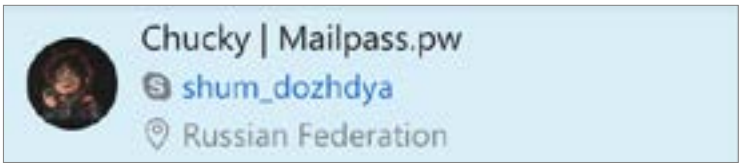


Figure 21: Chucky's Skype profile.

It has been verified that Chucky's BTC address shows transaction history starting in October 2016 and continuing until July 2019.

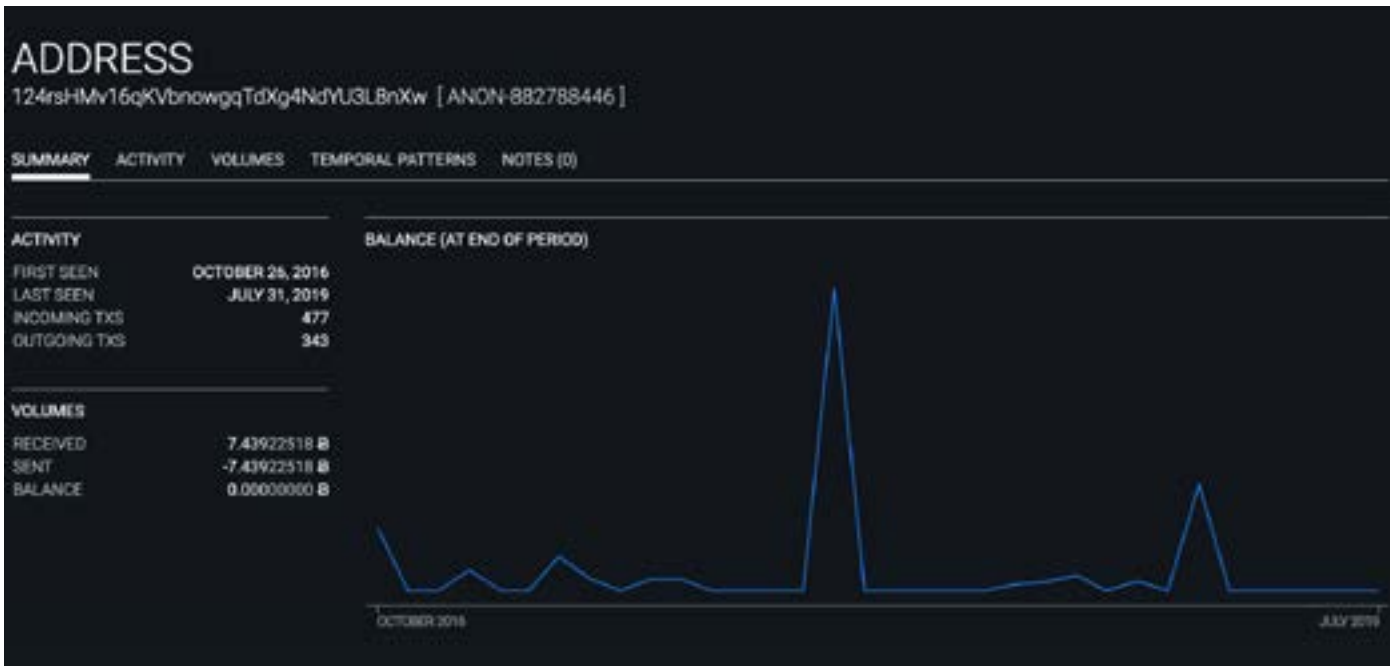


Figure 22: Chucky's Bitcoin transactions.

COMPARATIVE ANALYSIS OF THE OPERATORS OF DDW FORUMS

Finally, we conducted comparative and statistical analyses of the three major forum operators, focusing on both their activities as forum operators and their activities as regular forum users. We examined various aspects, including their activity frequency, language usage characteristics, and active time zones.

First, we examined the statistics of threads and reviews for each user over time.

Omnipotent, who has been operating RaidForums since 2015, consistently created threads and reviews. Notably, Omnipotent exhibited a higher ratio of review creation compared to thread creation.

[Operator] Omnipotent – RaidForums activity graph **Activity type**

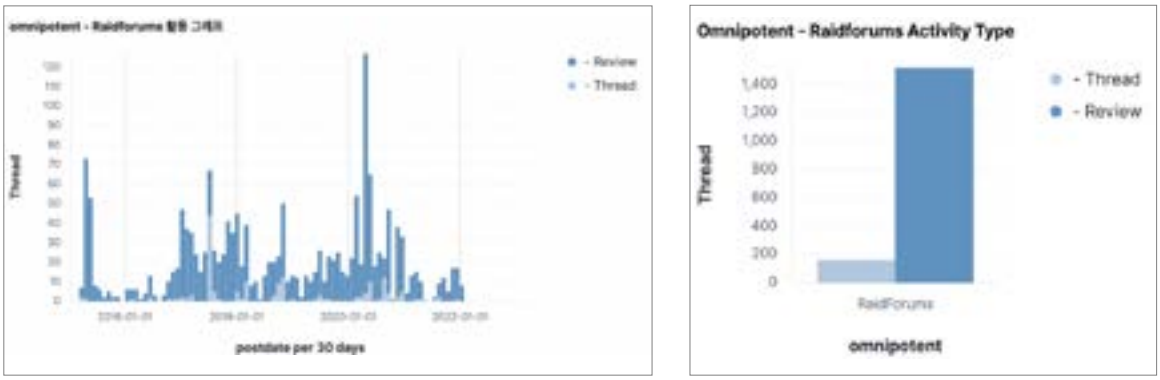
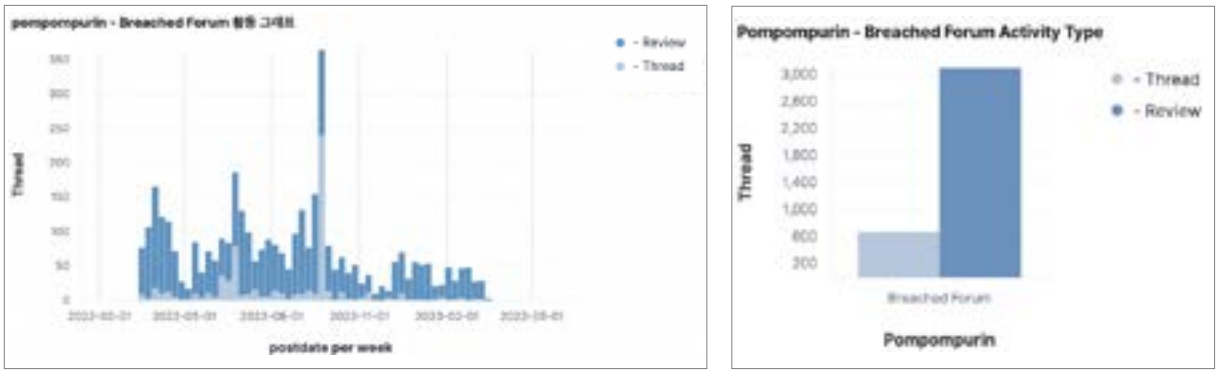


Figure 23: Omnipotent's forum activity pattern.

Pompompurin had a significantly higher ratio of review creation compared to thread creation during his activity on RaidForums. Similarly, when it comes to his own forum (Breached), it is confirmed that Pompompurin wrote reviews more than threads, but the pattern is relatively balanced between the two numbers.

[Operator] pompompurin – Breached forum activity graph **Activity type**



[User] pompompurin – RaidForums activity graph **Activity type**

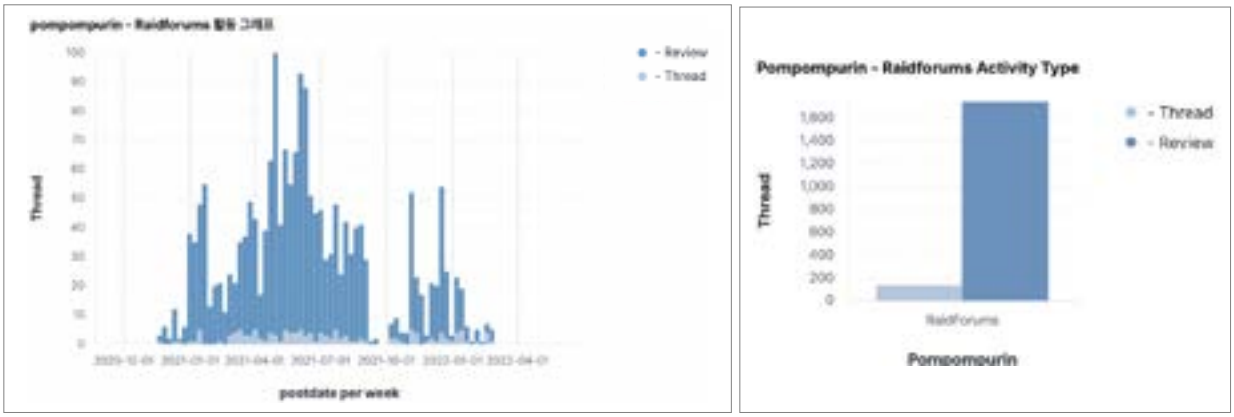
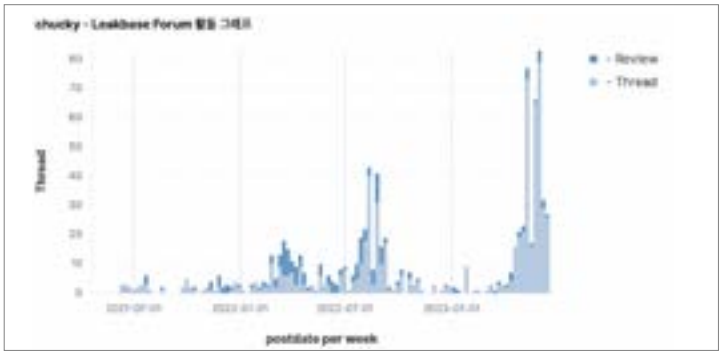


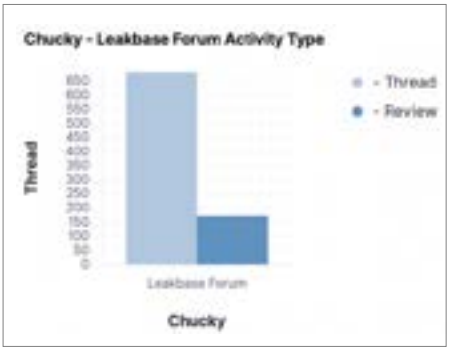
Figure 24: Pompompurin's forum activity pattern.

Chucky had a significantly higher ratio of thread creation compared to review creation during his activity on the Breached forum, and a similar pattern was observed on the Leakbase forum. However, as operator of the Leakbase forum, the proportion between the number of reviews and the number of threads shows a relatively balanced pattern.

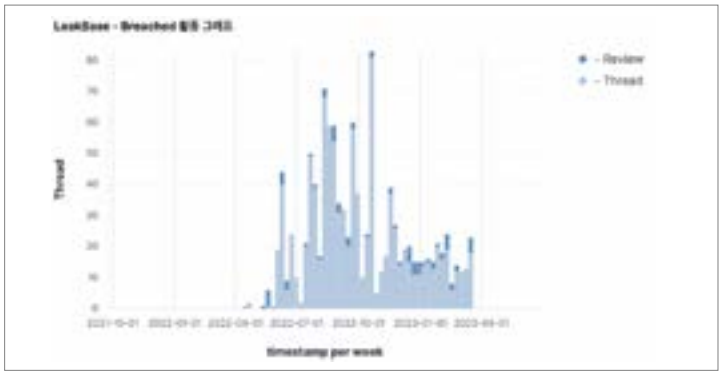
[Operator] Chucky – Leakbase forum activity graph



Activity type



[User] Leakbase – Breached forum activity graph



Activity type

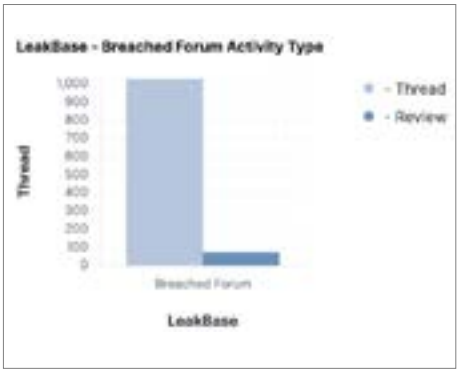


Figure 25: Leakbase (Chucky's) forum activity pattern.

We can see that the three users had unique activity characteristics, such as overwhelmingly writing reviews or writing a lot of threads in forums where they were active as users. On the other hand, as forum operators, we confirmed that they tried to keep a balance in the post writing pattern between reviews and threads.

Next, we examined the language usage characteristics of each user. Omnipotent had the highest usage of English, accounting for 95.74%, on RaidForums. This aligns with the fact that Omnipotent was arrested in the UK, suggesting a strong correlation.

Pompompurin used English in both the Breached forum he operated and in RaidForums as a user, with a usage rate of over 90%. This further correlates with the fact that Pompompurin was arrested in the United States.

Chucky used English at a rate of around 50% in both the Leakbase forum he operated and the Breached forum where he was active. Chucky also used various other languages, including Russian. Chucky's nationality and place of residence have not yet been disclosed. However, it is noteworthy that Chucky specified 'Russian Federation' on his *Skype* account, suggesting a potential connection to Russia or neighbouring countries.

Through the analysis of the graphs shown in Figures 26 to 28, it was concluded that the main language used in the forums operated by the forum operators is likely influenced by their country of residence or nationality.

Furthermore, when analysing the posting activity time zones of the three users (in UTC+0), several observations were made:

- Omnipotent: Based on the activity levels in London, UK time (UTC+1), Omnipotent's activity was relatively low during daytime hours but increased at around 23:00. This indicates that Omnipotent was primarily active during the early morning hours.
- Pompompurin: In the Breached forum (based on New York, USA time, UTC-4), the highest forum activity level was observed at 14:00, while the activity was relatively low between 17:00 and 24:00. On the other hand, in RaidForums, the activity was at its lowest between 14:00 and 16:00 and highest between 21:00 and 10:00. This suggests that Pompompurin separated activity times between the forum he operated and other forums.
- Chucky: Based on UTC+0, in the Leakbase forum, Chucky's activity level was low between 12:00 and 13:00 and between 15:00 and 16:00, while it was high between 04:00 and 5:00, 11:00 and 12:00, 14:00 and 15:00, and 20:00 and 21:00. However, in the Breached forum, the activity pattern was different, indicating a reversal of activity patterns.

[Operator] Omnipotent – RaidForums language usage

Figure 26: Omnipotent's language usage.

[Operator] Pompompurin – Breached forum language usage

[User] Pompompurin – RaidForums language usage

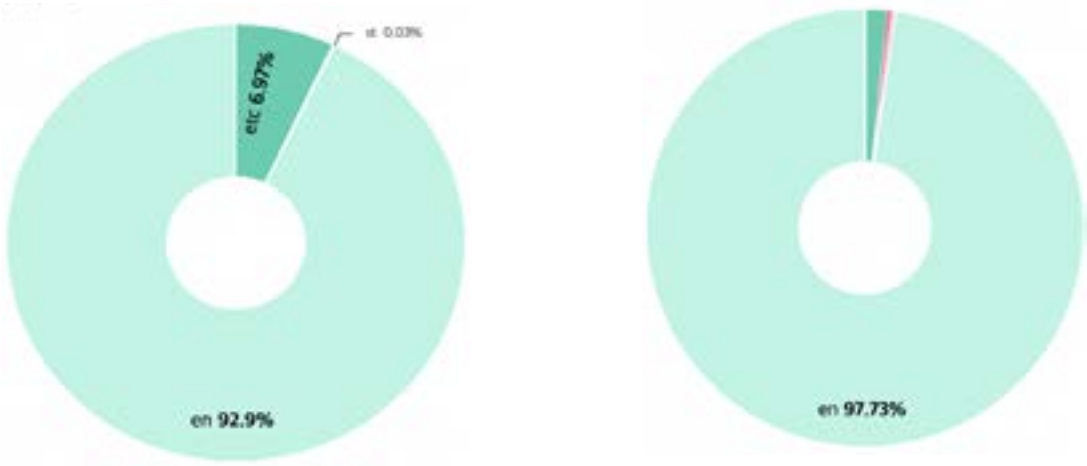


Figure 27: Pompompurin's language usage.

[Operator] Chucky – Leakbase forum language usage

[User] Leakbase – Breached forum language usage

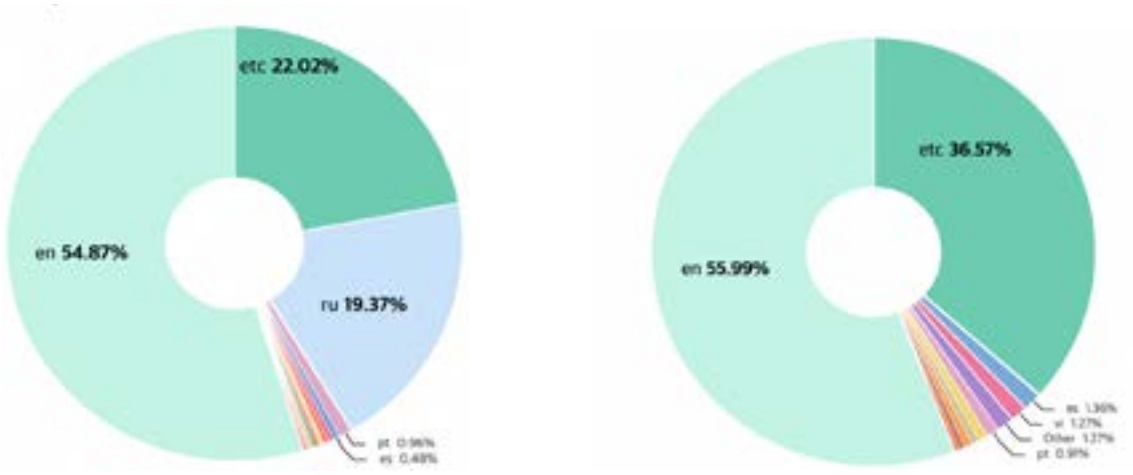


Figure 28: Chucky's language usage.

These observations provide insights into the distinct activity time patterns and habits of the forum operators across different time zones and forums.

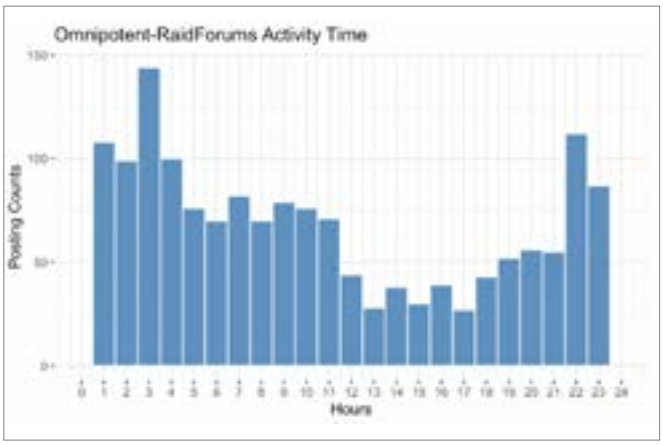
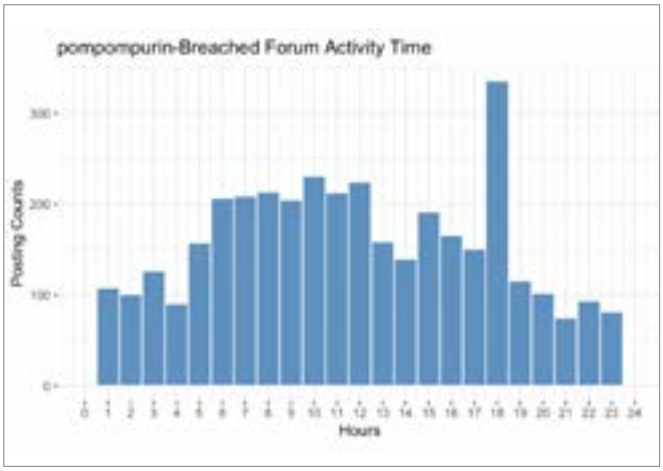
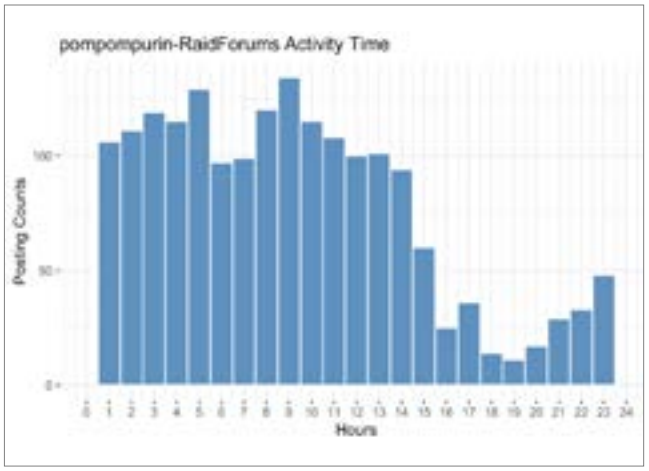
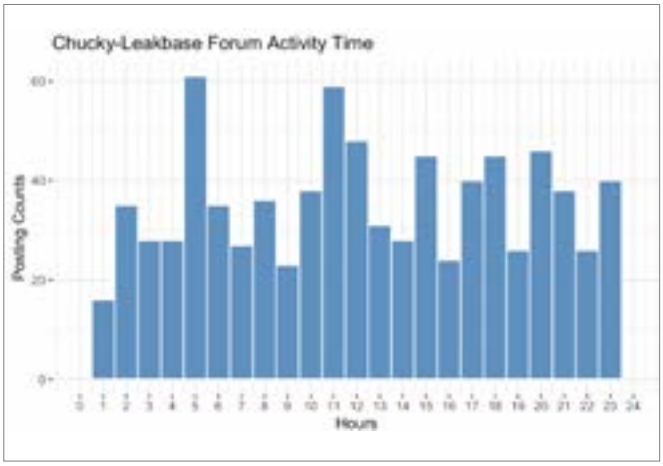
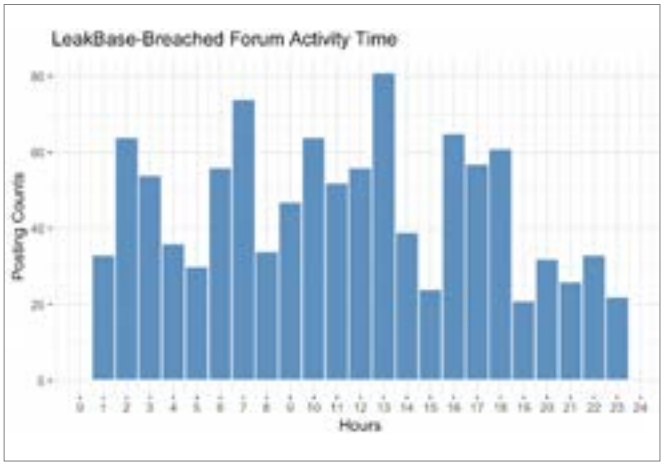
Operator	Active in other forum
	None
	
	

Figure 29: Activity time of the three operators.

Additionally, when considering the combined activity time zones of the forums they operated and the forums they were active in, it is evident that there are differences in the operating hours among the forum operators. By referring to Figure 30, the major activity time zones of each user can be identified, and it is likely that these times are related to the activity hours of their respective nationalities or places of residence.

Total active time

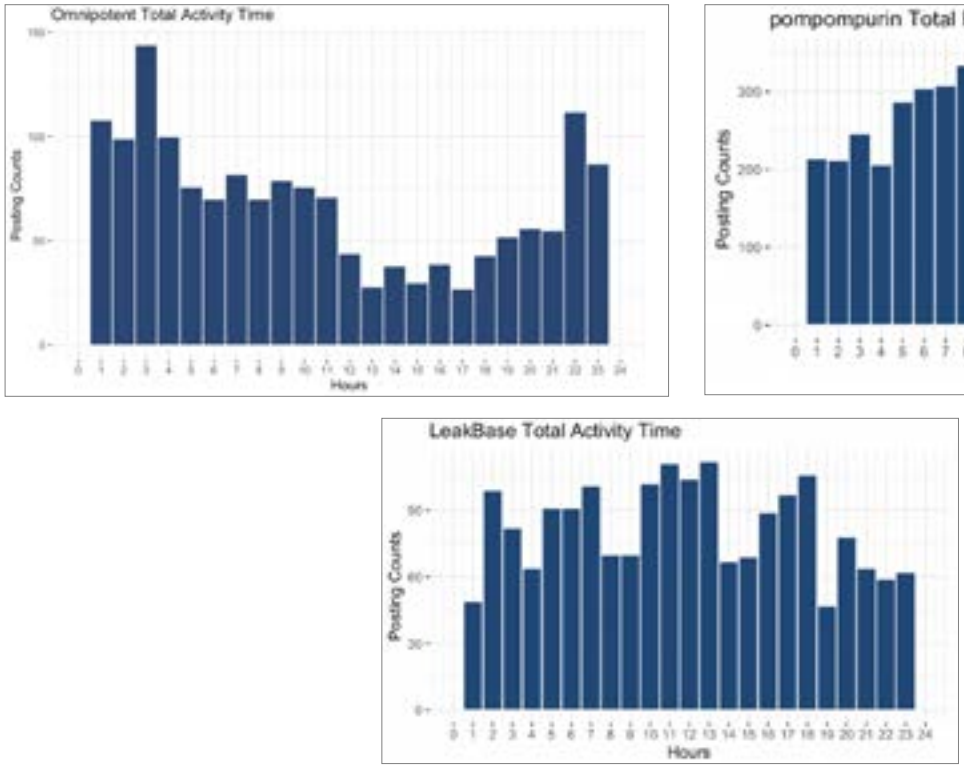


Figure 30: Total activity time of the three operators.

REFERENCES

[1] Flashpoint. State of Cyber Threat Intelligence: 2023. https://flashpoint.io/resources/report/state-of-cyber-threat-intel-2023/.

[2] Kaspersky. Developers, attackers and designers topped the list of the most demanded IT professionals on the Darknet. 30 January 2023. https://www.kaspersky.com/about/press-releases/2023_developers-attackers-and-designers-topped-the-list-of-the-most-demanded-it-professionals-on-the-darknet.

[3] Erazo, F. Bitcoin Activity on the Dark Web Grew by 65% in Q1 2020, Says Study. Cointelegraph. 19 May 2020. https://cointelegraph.com/news/bitcoin-activity-on-the-dark-web-grew-by-65-in-q1-2020-says-study.