

W4 May | EN | Story of the week: Ransomware on the Darkweb

medium.com/s2wlab/w4-may-en-story-of-the-week-ransomware-on-the-darkweb-5f5b8d4c3b6f

Hyunmin Suh

May 25, 2021



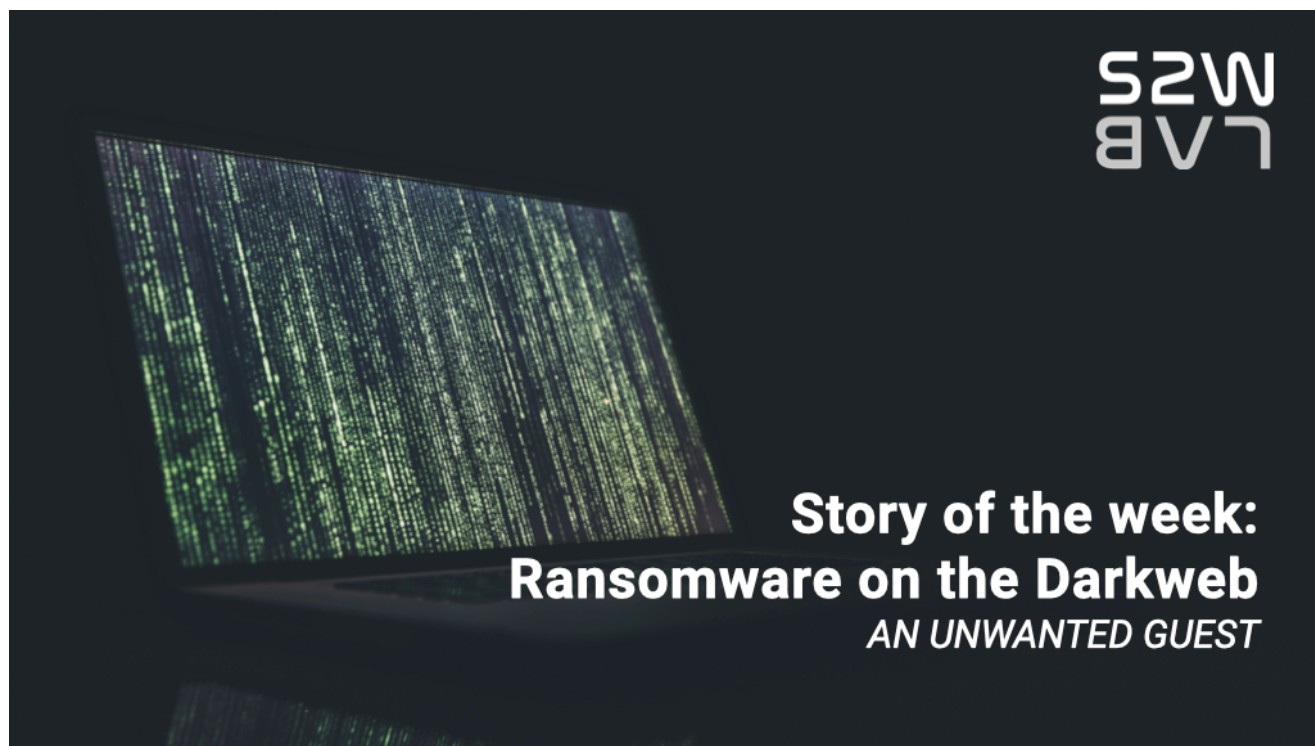
[Hyunmin Suh](#)

May 25, 2021

6 min read

An Unwanted Guest

Co-Author: , @ Talon



SoW (Story of the Week) publishes a report summarizing ransomware's activity on the Darkweb. The report includes summary of victimized firms, Top 5 targeted countries and industrial sectors, status of dark web forum posts by ransomware operators, etc.

Executive Summary

On May 13th, the notorious Russian hacking forum XSS banned all ransomware promoting posts and operators' accounts. It was Darkside ransomware's colonial pipeline infection that triggered this incident.

As the U.S. government and FBI narrowed down the investigation, the Darkside ransomware operation server was taken down, and even the Russian hacking forums announced that they are banning and deleting all the posts related to ransomware activity. Three biggest hacking forums, starting with XSS Forum, Exploit, and Raidforums, all halted ransomware operators' activity, and of course, there were many disappointing posts from the ransomware operators regarding such decisions made by administrator. Most of active accounts such as REvil, Lockbit, and Avaddon have announced that they will either stop their activities in the forum or move out to their own independent platform.

Then, where will they go? Let's see what will happen after the consequence of banning ransomware activity in all forums.

1. Weekly Status

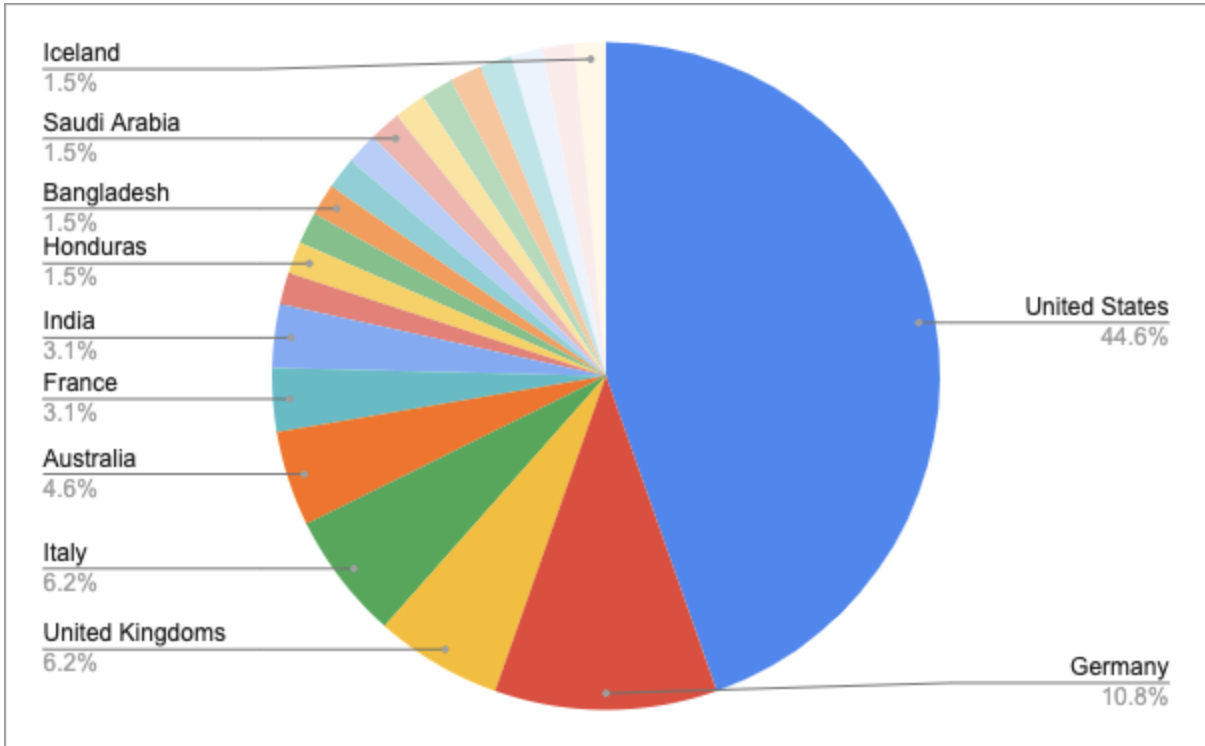
A. Status of the victimized firms (5/17 ~ 5/24)

| Aa Name | 📅 Date updated | 🌐 HQ | 🏭 Industry | 👤 Adversary |
|------------|----------------|---------------|-----------------|-------------|
| [Redacted] | May 18, 2021 | Australia | Food & Beverage | conti |
| [Redacted] | May 19, 2021 | United States | Food & Beverage | conti |
| [Redacted] | May 19, 2021 | France | Health Care | conti |
| [Redacted] | May 19, 2021 | United States | Health Care | conti |
| [Redacted] | May 20, 2021 | Indonesia | IT | conti |
| [Redacted] | May 20, 2021 | United States | Materials | conti |
| [Redacted] | May 20, 2021 | United States | Technology | conti |
| [Redacted] | May 20, 2021 | United States | Real estate | conti |
| [Redacted] | May 20, 2021 | Australia | Retail | conti |
| [Redacted] | May 20, 2021 | Honduras | Media | conti |
| [Redacted] | May 20, 2021 | United Kindom | Transportation | conti |
| [Redacted] | May 20, 2021 | Germany | Industrials | conti |
| [Redacted] | May 20, 2021 | United States | Industrials | conti |
| [Redacted] | May 20, 2021 | Germany | Transportation | conti |
| [Redacted] | May 20, 2021 | Italy | Transportation | conti |
| [Redacted] | May 20, 2021 | Germany | Financial | conti |
| [Redacted] | May 20, 2021 | United Kindom | Retail | conti |
| [Redacted] | May 20, 2021 | France | Transportation | conti |
| [Redacted] | May 20, 2021 | Korea | Technology | conti |
| [Redacted] | May 20, 2021 | United States | Chemicals | conti |
| [Redacted] | May 20, 2021 | United States | Industrials | conti |
| [Redacted] | May 20, 2021 | United States | Transportation | conti |
| [Redacted] | May 20, 2021 | Bangladesh | Services | conti |
| [Redacted] | May 20, 2021 | Italy | Services | conti |
| [Redacted] | May 20, 2021 | United States | Technology | conti |
| [Redacted] | May 20, 2021 | United States | Financial | conti |
| [Redacted] | May 20, 2021 | United States | Industrials | conti |
| [Redacted] | May 20, 2021 | United States | Consumer goods | conti |
| [Redacted] | May 20, 2021 | United Kindom | Industrials | conti |
| [Redacted] | May 20, 2021 | United States | Real estate | conti |
| [Redacted] | May 20, 2021 | United States | Construction | conti |
| [Redacted] | May 20, 2021 | United States | Financial | conti |

| | | | | |
|--|--------------|----------------|----------------|---------------|
| | May 20, 2021 | Italy | Industrials | conti |
| | May 20, 2021 | Italy | Industrials | conti |
| | May 20, 2021 | Netherlands | Financial | conti |
| | May 21, 2021 | India | Electronics | conti |
| | May 19, 2021 | Ireland | Transportation | clon |
| | May 19, 2021 | India | Health Care | clon |
| | May 18, 2021 | United States | Law | clon |
| | May 18, 2021 | United States | Transportation | clon |
| | May 18, 2021 | United States | Media | clon |
| | May 20, 2021 | United States | Technology | avaddon |
| | May 20, 2021 | Germany | IT | avaddon |
| | May 20, 2021 | Saudi Arabia | Manufacturing | avaddon |
| | May 20, 2021 | Cyprus | Financial | avaddon |
| | May 20, 2021 | United States | Financial | avaddon |
| | May 20, 2021 | Czech Republic | Law | avaddon |
| | May 20, 2021 | Germany | consumer goods | avaddon |
| | May 20, 2021 | Colombia | Financial | avaddon |
| | May 20, 2021 | United States | Manufacturing | avaddon |
| | May 19, 2021 | US | Real Estate | revil |
| | May 20, 2021 | Portugal | Technology | avaddon |
| | May 19, 2021 | United States | Health Care | xing locker |
| | May 18, 2021 | United States | Manufacturing | revil |
| | May 17, 2021 | Germany | Media | nefilim |
| | May 17, 2021 | Germany | e-commerce | nefilim |
| | May 17, 2021 | United States | Others | marketo |
| | May 17, 2021 | Canada | e-commerce | marketo |
| | May 20, 2021 | United States | Manufacturing | LV Ransomware |
| | May 21, 2021 | Japan | Industrials | LV Ransomware |
| | May 19, 2021 | United States | Services | N3tw0rm |
| | May 19, 2021 | United States | Financial | N3tw0rm |
| | May 20, 2021 | France | Materials | ransomexx |
| | May 19, 2021 | United States | Law | revil |
| | May 19, 2021 | Israel | Health Care | N3tw0rm |
| | May 22, 2021 | United States | Manufacturing | revil |
| | May 23, 2021 | Australia | Industrials | LV Ransomware |

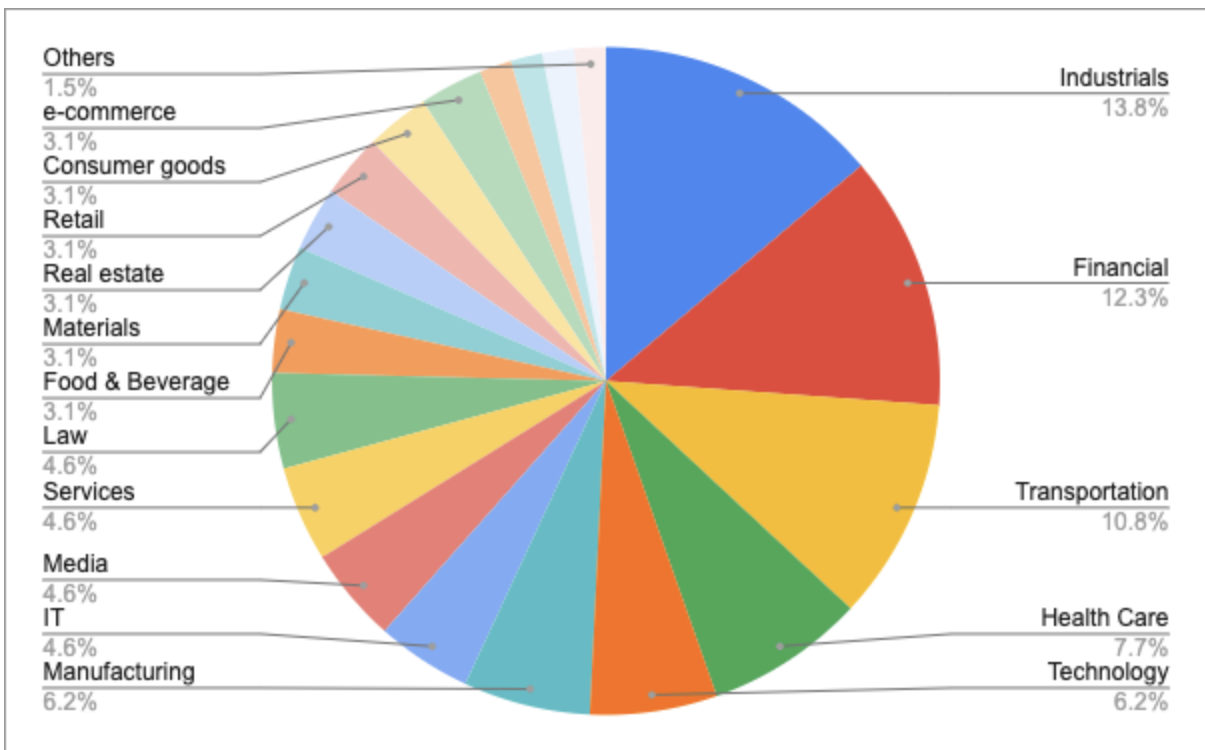
- For a week, a total of 67 victimized firms were mentioned and a change in the state of the data leaked from the victims in the ransomware site was detected
- 10 threat groups' activities were detected

B. TOP 5 targeted countries



1. United States — 44.6%
2. Germany — 10.8%
3. United Kingdoms — 6.2%
4. Italy — 6.2%
5. Australia — 4.6%

C. TOP 5 targeted industrial sectors



1. Industrials — 13.8%

2. Services — 12.3%
3. Transportation — 10.8%
4. Health Care — 7.7%
5. Technology — 6.2%

2. Status of active Ransomware forum posts @Dark Web

A. XSS Forum

Our > Dear administration! >

No more ransom! Banning lockers on the forum

admin · May 13, 2021

one 2 3 ... 6 Next ▶

Jump to new Watch

May 13, 2021

No more ransom! Friends, on our forum **lockers** (Ransomware) and everything connected with them are **prohibited**. Namely:

- Ransomware affiliate programs;
- Ransomware rental;
- sale of lockers (ransomware software);

All topics matching this rule will be removed. Fortunately, only a few of them were found.

More detailed explanation. Reasons.

It's not a secret for anyone, I personally don't like lockers, why? Few lockers are technically interesting. Most of them (not all) are mediocre technical tools.

The main purpose of the DaMaGeLaB forum is knowledge. We are a technical forum, we learn, research, share knowledge, write interesting articles. The goal of Ransomware is just to make money. The goals are not the same. No, of course, everyone needs money, but not to the detriment of basic aspirations. We are not a market or a marketplace.

Degradation on the face. Newbies open up the media, see some crazy virtual millions of dollars that they will never get. They don't want anything, they don't learn anything, they don't code anything, they just don't even think, the whole essence of being comes down to "encrypt - get \$". They just run to github, look for locker sorts there and run to encrypt everything they see. Since our forum is aimed at beginners, this factor is important to us.

Click to expand ...

Report Like + Quote Reply


Xerx, undiscloseduserpt, Zero888 and 36 others

On May 13th, the administrator of the XSS Forum announced that ransomware-related content is no longer allowed. In particular, it will be limited to the following contents.

- Ransomware affiliate programs;- Ransomware rental;- sale of lockers (ransomware software);

In other words, ransomware affiliate program cannot be promoted for partner recruitment, and any forms of selling Ransomware-as-a-Service (RaaS) or ransomware software itself is prohibited.

Obviously, the administrator's announcement shocked the ransomware operators who were currently running. For example, the LockBit ransomware operator seems to have felt a kind of betrayal with the comment "Suddenly".



LOCKBIT

LockBitSupp Premium

Joined: Mar 8, 2021
Messages: one
Reaction score: 0

May 13, 2021

#eight

Suddenly...


Report
Like
+ Quote
Reply

Shortly after this announcement from XSS forum, the administrator of Exploit and Raidforums announced the same rules about banning ransomware-related posts.

B. Exploit & Raidforums

Ransomware is now banned on RaidForums
by moot - May 14, 2021 at 09:33 PM

Pages (2): 1 2 Next »



ADMINISTRATOR

Posts: 2,237
Threads: 213
Joined: Mar 2015
6 YEARS OF SERVICE

May 14, 2021 at 09:33 PM. This post was last modified: May 17, 2021 at 05:09 PM by moot. Edited 1 time in total.

Edit: for those who can't read (BankSecurity) this was a joke.

Ransomware is no longer allowed

RaidForums will no longer allow any posts about "ransomware" and the reasoning behind this decision is as follows: if it ran somewhere, then you should probably go catch it?

Thank you,
RaidForums' Staff

Reply

2021.05.14 Raidforums posts that will not allow ransomware related content

A

Remove affiliate programs of lockers from the forum.

By admin, May 15in About Exploit.IN Site and Forum

Follow FOUR

Start new topic
Reply to this topic

one 2 3 four five 6 NEXT » Page 1 of 9 ▾

admin

<forum.status>

A

Admin
1141
6905 posts
Joined
02/19/05 (ID: 1)
Activity
other / other

Posted May 15

Good day,

We are glad to see pentesters, specialists, coders.
But they are not happy with lockers, they attract a lot of attention. The very type of activity is not pleasant to us in view of the fact that everything is located in a row, we do not consider it advisable to be present on our forum, partner programs of lockers.

It was decided to remove all affiliate programs and prohibit them as a type of activity on our forum.

All topics related to lockers will be deleted.

+ Quote

★ advertisement@exploit.im - order and payment for advertising

✧ support@exploit.im - forum technical support

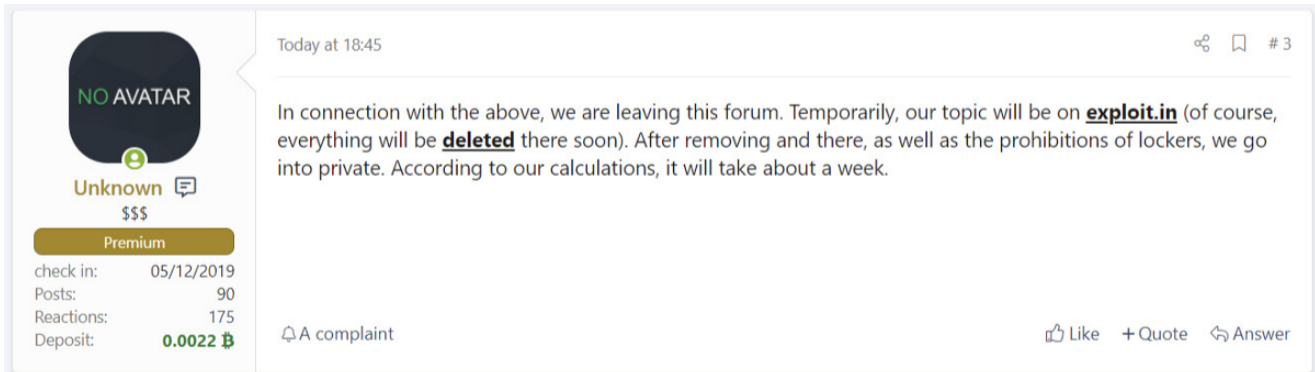
🌿 oxygen@exploit.im - forum arbiter

✧ jabber_support@exploit.im - technical support for the exploit.im jabber server

7/10

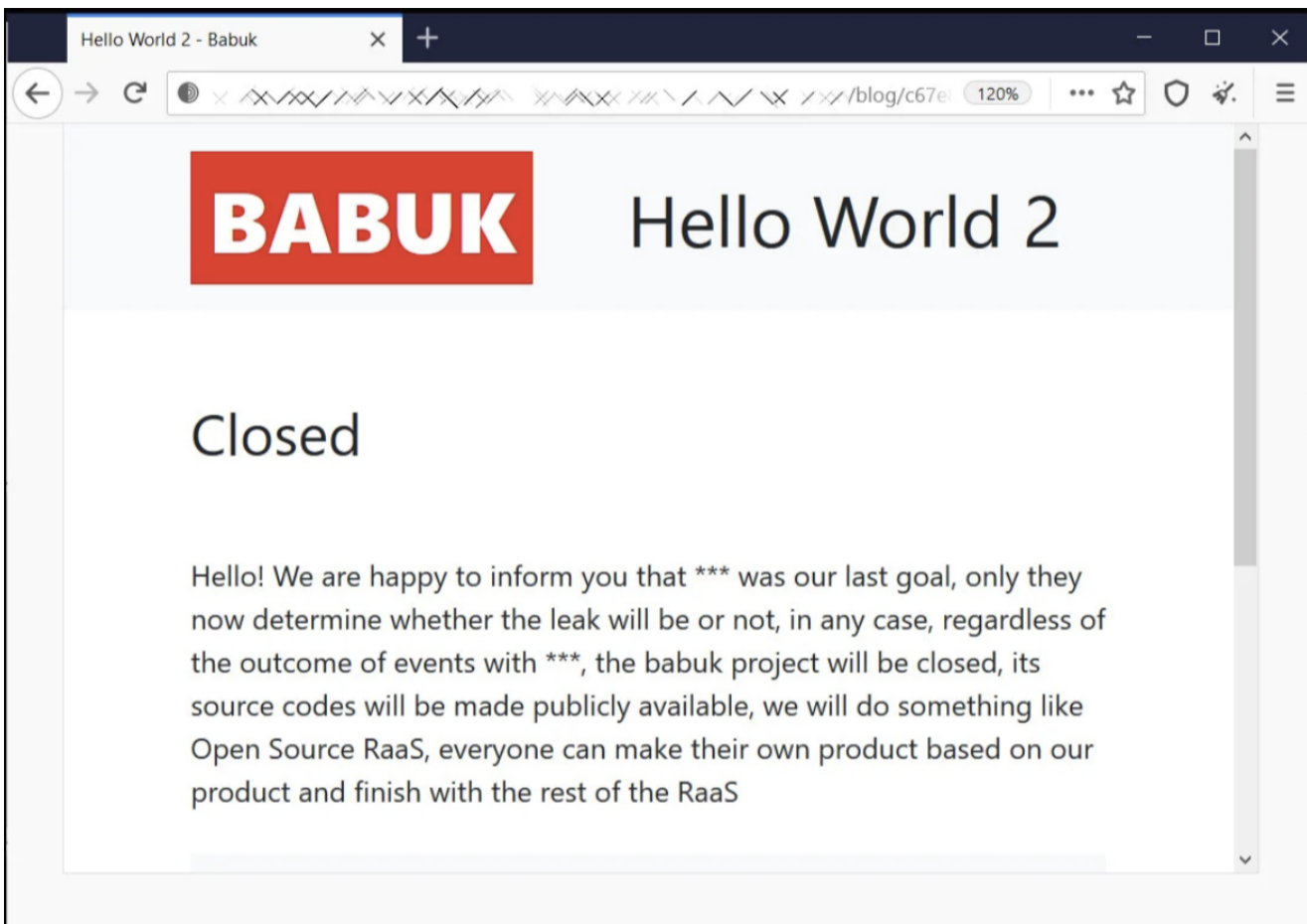
3. Ransomware operators' next move

A. Revil (Sodinokibi)



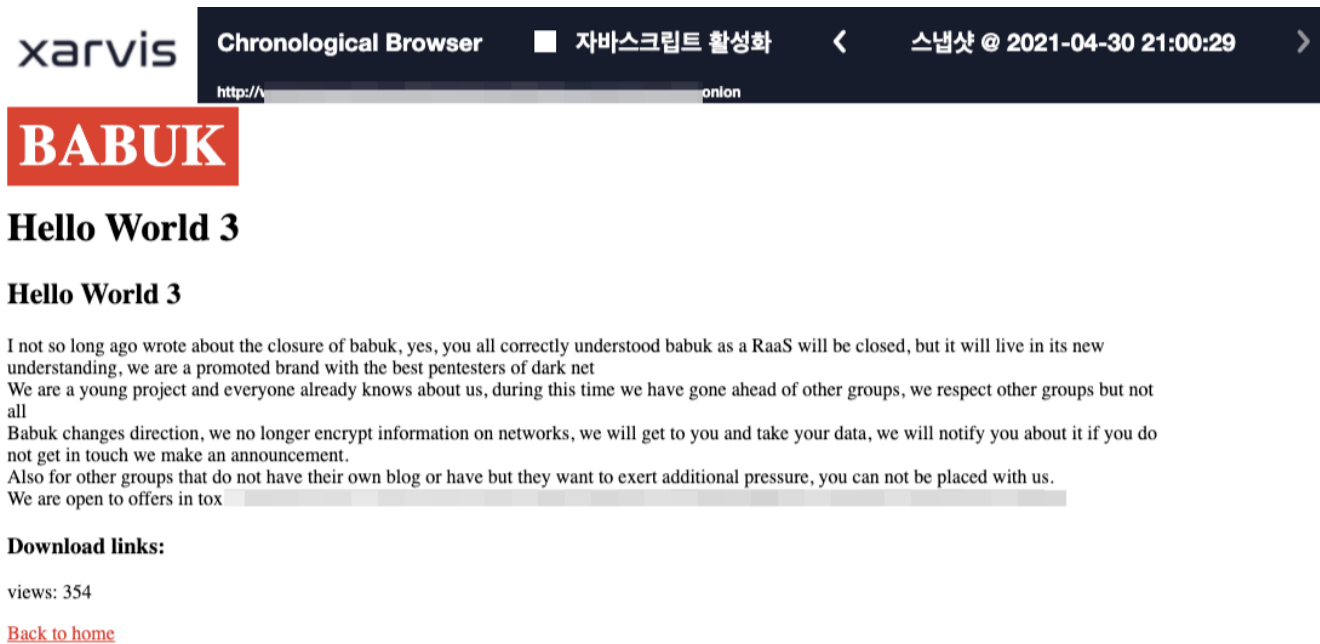
Due to the change in the policy of the administrator of XSS forum, REvil also declared retirement in Exploit and will switch to a private platform

B. Babuk



Source: Bleeping Computer ()

2021.04.29 Bleeping computer reported that Babuk ransomware would close the BABUK project and release the source code to the outside by leaving a note titled 'Hello World 2'



I not so long ago wrote about the closure of babuk, yes, you all correctly understood babuk as a RaaS will be closed, but it will live in its new understanding, we are a promoted brand with the best pentesters of dark net We are a young project and everyone already knows about us, during this time we have gone ahead of other groups, we respect other groups but not all Babuk changes direction, we no longer encrypt information on networks, we will get to you and take your data, we will notify you about it if you do not get in touch we make an announcement. Also for other groups that do not have their own blog or have but they want to exert additional pressure, you can not be placed with us. We are open to offers in tox: ****Sanitized by S2W LAB

- However just a day after, Babuk reappeared with a post titled 'Hello World 3' saying that it will no longer focus on data encryption but rather exfiltrating data.
- It also states that other ransomware groups either do not have a data leak site or have but they want to exert additional pressure, shall not work with Babuk.

BABUK

Hello world 4

Hello world 4

Hello! We announce the development of something really cool, a huge platform for independent leaks, we have no rules and bosses, we will publish private products in a single information platform where we will post leaks of successful no-name teams that do not have their own blogs and names, these are not girls who run with ship like rats and change the policy of their resources. these are really strong guys. Another loud leak awaits you within a week.

Download links:

views: 1623

[Back to home](#)

Hello! We announce the development of something really cool, a huge platform for independent leaks, we have no rules and bosses, we will publish private products in a single information platform where we will post leaks of successful no-name teams that do not have their own blogs and names, these are not girls who run with ship like rats and change the policy of their resources. these are really strong guys. Another loud leak awaits you within a week.

- After that, in 'Hello World 4', Babuk is planning a huge platform for data leakage, and it is stated that ransomware groups that do not operate their own data leakage sites will join together.
- A huge leak will happen very soon (they mentioned a week or soon)

Conclusion

Most of renowned hacking forums banned ransomware-related content, but the number of victimized firms was not significantly reduced.

Operators who have been kicked out of forums are likely to switch to their own platform and additional ransomware groups that do not operate leak sites will likely join the crews.

Such sanctions against ransomware operators are just temporary, and this does not mean any termination or downfall of ransomware gangs, so we strongly recommend never let loose the guard.