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

By Hyunmin Suh

Published: 2021-05-25 · Archived: 2026-04-05 14:57:25 UTC

An Unwanted Guest

Co-Author:

, @ Talon

Press enter or click to view image in full size

> 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,

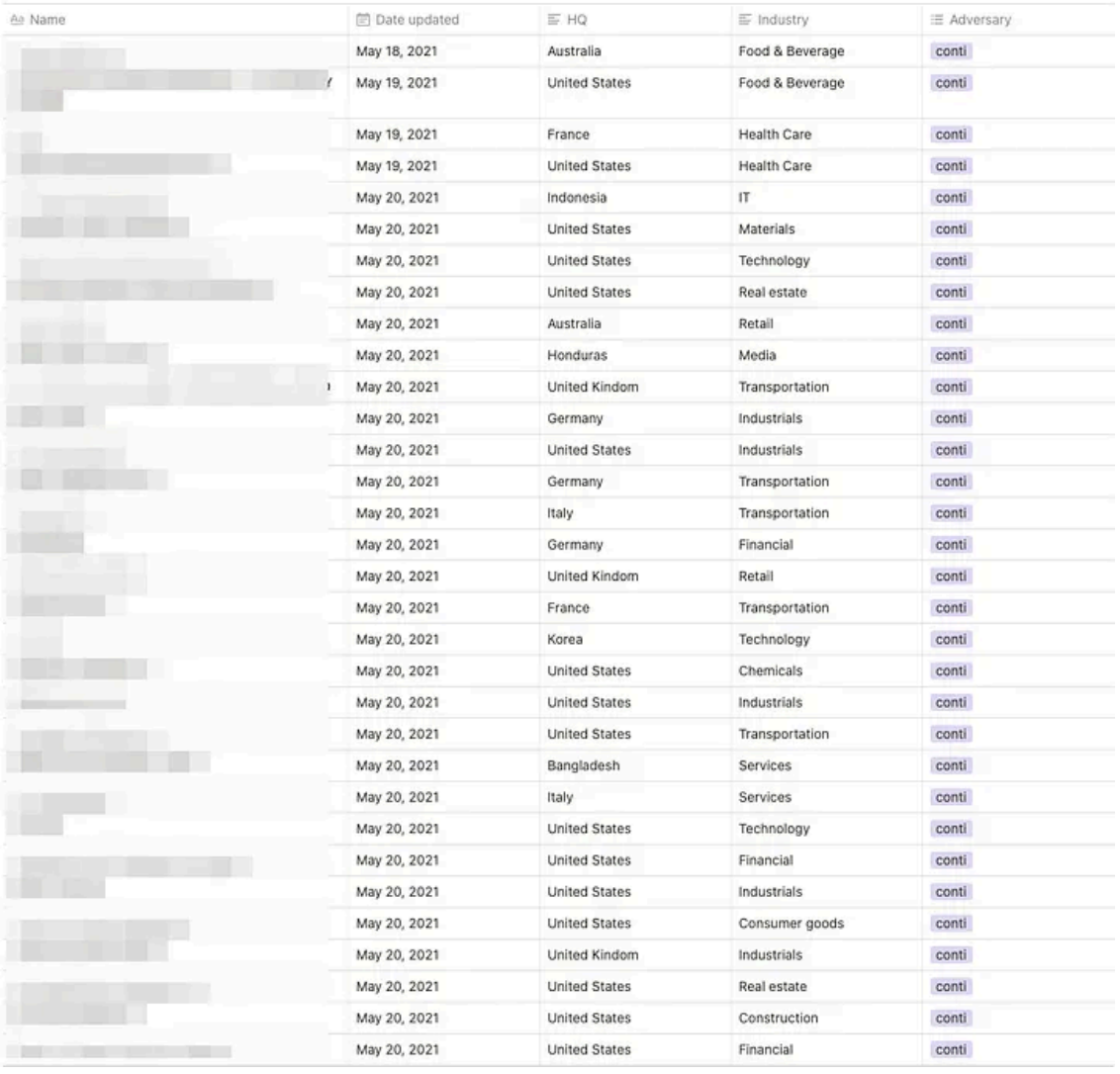
all halted ransomware operators' activity, and of course, there were many disappointing posts from the ransomware operators regarding such decisions made by administrator. Most of active accounts such as REvil, Lockbit, and Avaddon have announced that they will either stop their activities in the forum 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)

Press enter or click to view image in full size



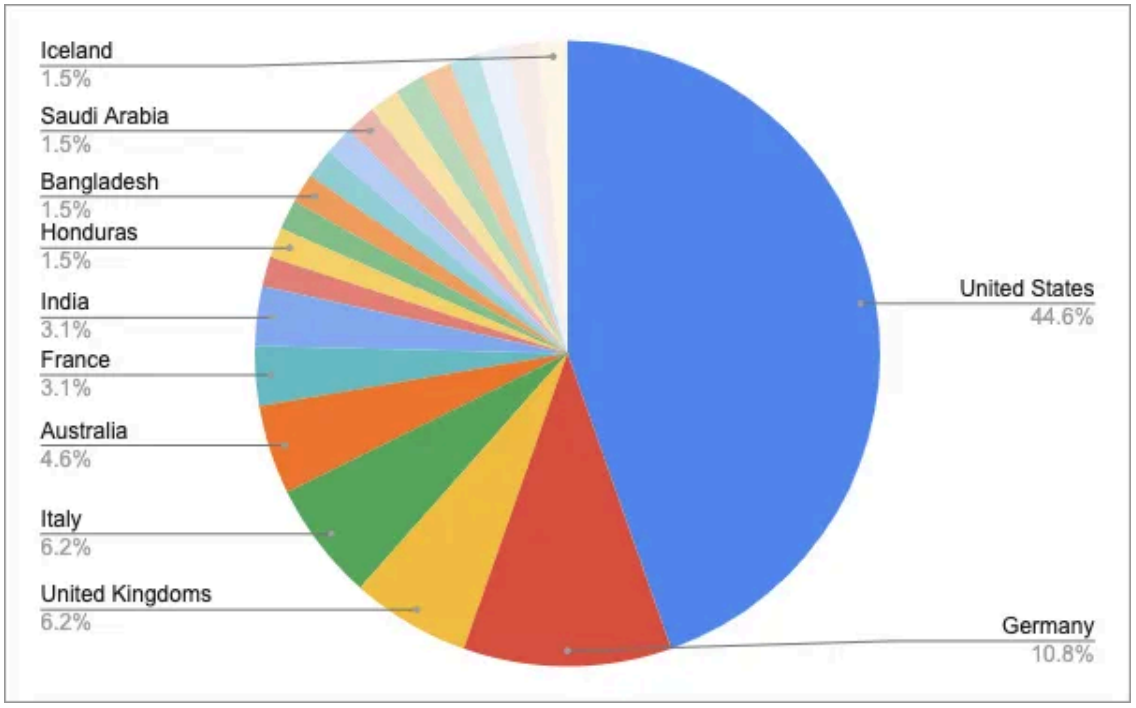
Name	Date updated	HQ	Industry	Adversary
	May 18, 2021	Australia	Food & Beverage	conti
	May 19, 2021	United States	Food & Beverage	conti
	May 19, 2021	France	Health Care	conti
	May 19, 2021	United States	Health Care	conti
	May 20, 2021	Indonesia	IT	conti
	May 20, 2021	United States	Materials	conti
	May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

Press enter or click to view image in full size

	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	clop
	May 19, 2021	India	Health Care	clop
	May 18, 2021	United States	Law	clop
	May 18, 2021	United States	Transportation	clop
	May 18, 2021	United States	Media	clop
	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 Repubic	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	Manufactoring	revil
	May 23, 2021	Australia	Industrials	LV Ransomware

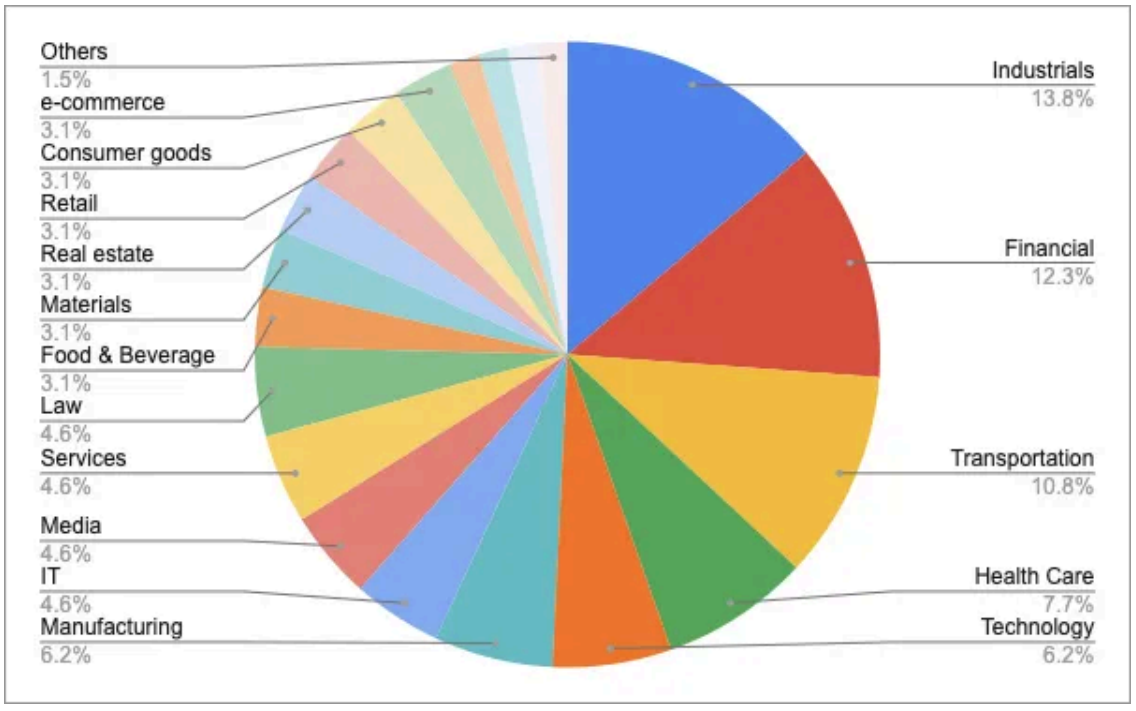
- For a week, a total of 67 victimized firms were mentioned and a change in the state of the data leaked from the victims in the ransomware site was detected
- 10 threat groups' activities were detected

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



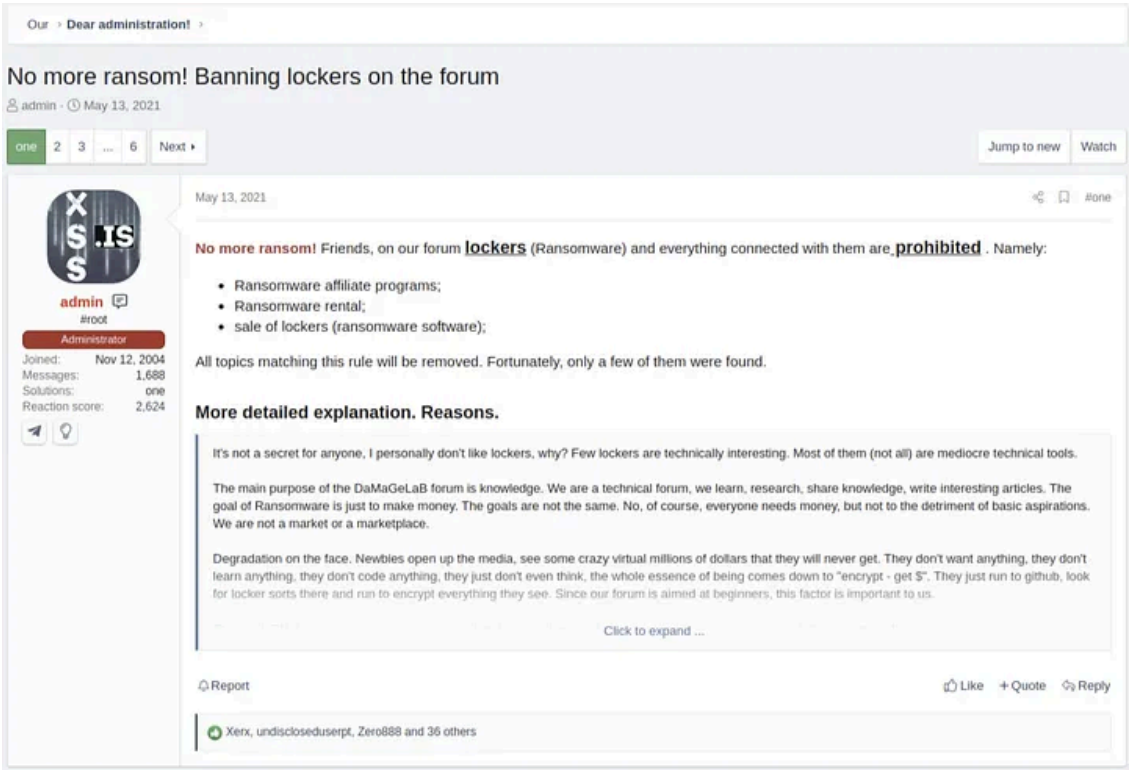
1. Industrials — 13.8%
2. Services — 12.3%

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

Press enter or click to view image in full size



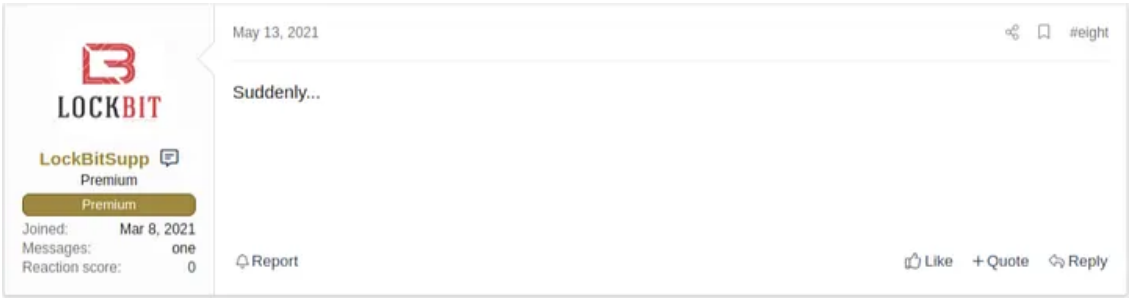
On May 13th, the administrator of the XSS Forum announced that ransomware-related content is no longer allowed. In particular, it will be limited to the following contents.

```
- 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".

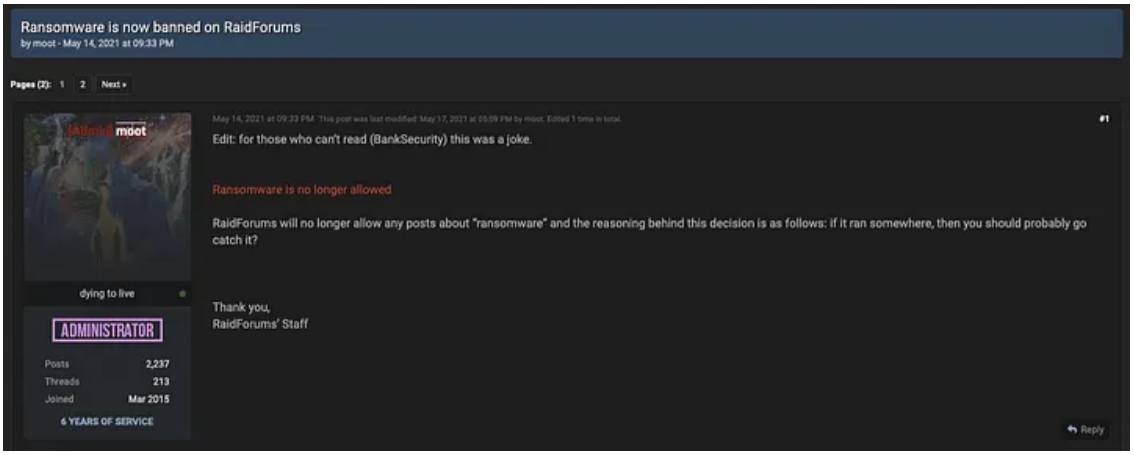
Press enter or click to view image in full size



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

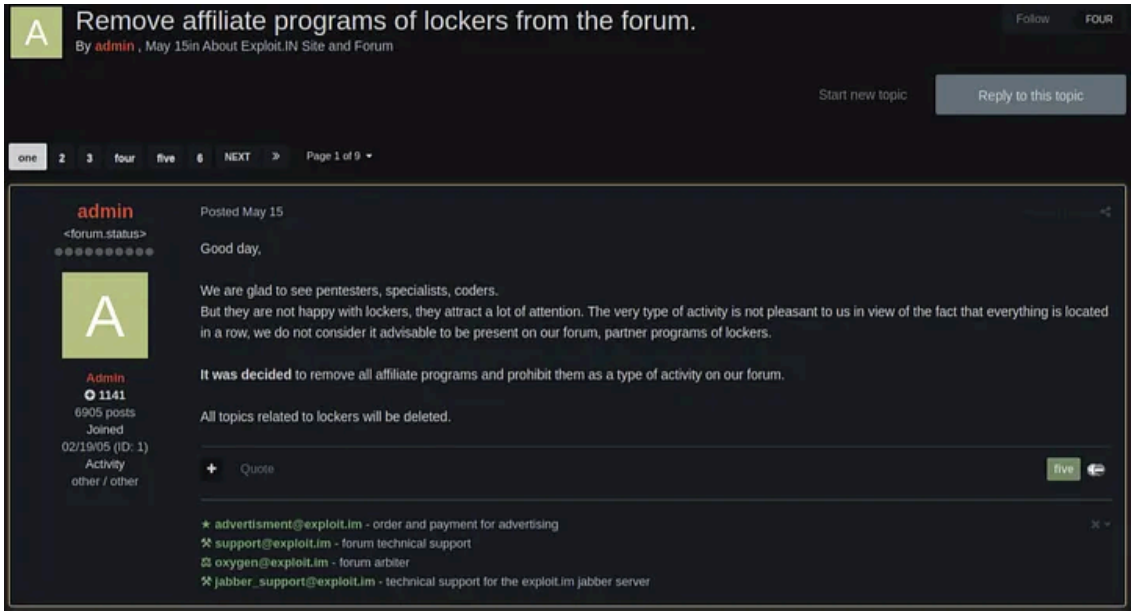
B. Exploit & Raidforums

Press enter or click to view image in full size



2021.05.14 Raidforums posts that will not allow ransomware related content

Press enter or click to view image in full size

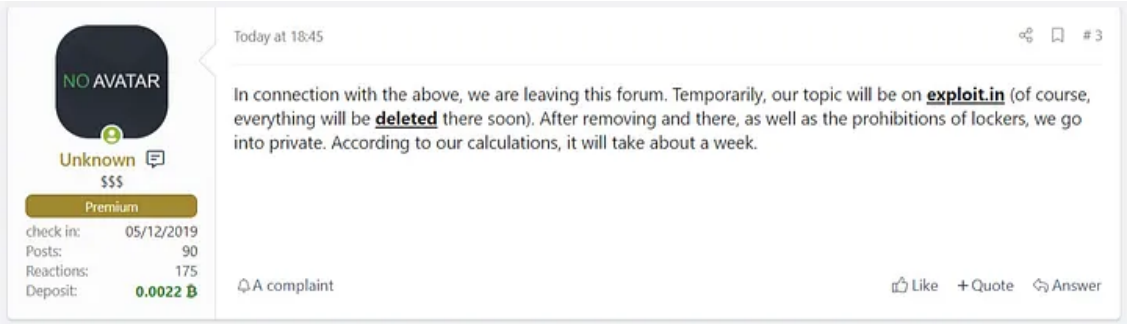


2021.05.15 Exploit forum posts that will not allow ransomware related content

3. Ransomware operators' next move

A. Revil (Sodinokibi)

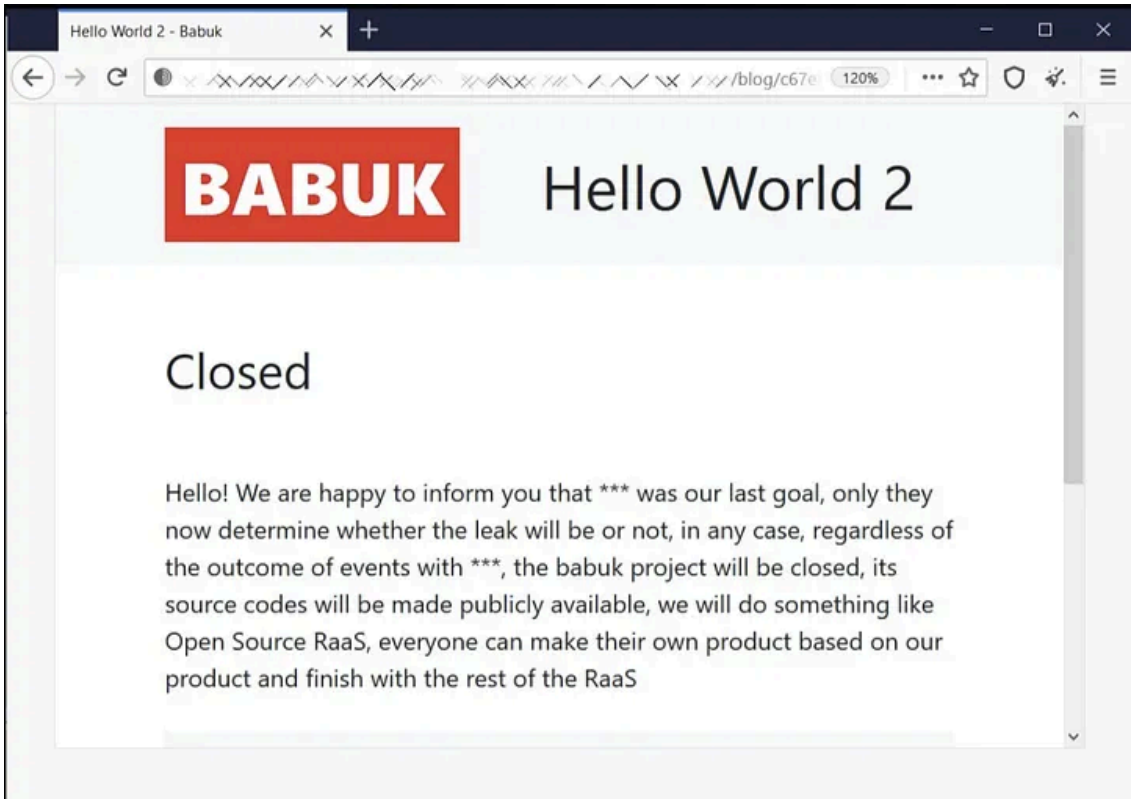
Press enter or click to view image in full size



- 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

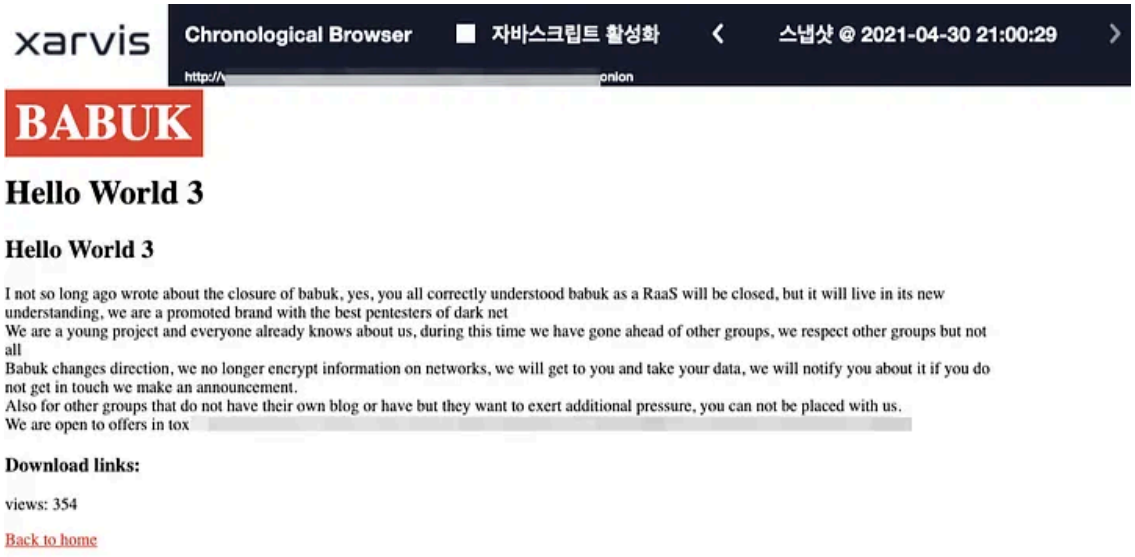
Press enter or click to view image in full size



Source: Bleeping Computer (https://www.bleepingcomputer.com/news/security/babuk-ransomware-readies-shut-down-post-plans-to-open-source-malware/)

- 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’

  Press enter or click to view image in full size

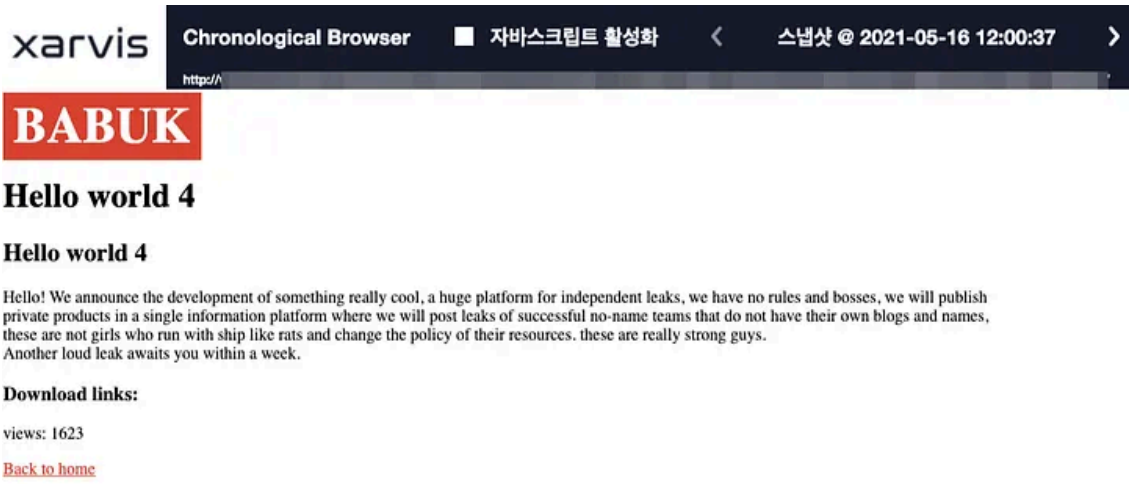



```
I not so long ago wrote about the closure of babuk, yes, you all correctly understood babuk as a Raa
We are a young project and everyone already knows about us, during this time we have gone ahead of o
Babuk changes direction, we no longer encrypt information on networks, we will get to you and take y
```

```
Also for other groups that do not have their own blog or have but they want to exert additional pres
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.

  Press enter or click to view image in full size




```
Hello! We announce the development of something really cool, a huge platform for independent leaks,
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.

- Homepage: https://www.s2wlab.com
- Facebook https://www.facebook.com/S2WLAB/
- Twitter https://twitter.com/s2wlab
