W1 Jun | EN | Story of the week: Ransomware on the Darkweb

By Hyunmin Suh

Published: 2021-06-03 · Archived: 2026-04-05 15:50:00 UTC

Corporate Data Matters

Get Hyunmin Suh’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Co-Author:

, , YH Jeong @ Talon

Press enter or click to view image in full size

Image from unsplash

> 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

- Compared to SoW 5 months ago (W1 Jan), the number of victimized firms increased by about 2.6 times, and the ransomware threat groups increased by 1.6 times, requiring attention to ransomware attacks.
- The United States was mostly positioned at top in terms of the rate of victim infection, but as the number of active ransomware threat groups increased, the percentage of victimized firms' country locations also varied.
- Users who worked as affiliate partners with Darkside (as a pentester) claiming to the admin of XSS forum as Darkside did not pay their portion properly, which accepted and permanently suspended the Darkside account.
- Babuk ransomware rebranded as Payload Bin and their first victim was CD PROJEKT.
- The CD PROJEKT's source code leak is an incident found to be related to HelloKitty ransomware as Babuk ransomware announced last week planning to integrate a platform by gathering ransomware partners who did not operate their own data leak site.

1. Weekly Status

A. Status of the victimized firms (5/24 ~ 5/30)

Press enter or click to view image in full size

Name	Date updated	HQ	Industry	Adversary
	May 29, 2021	Switzerland	manufacturer	nefilim
	May 26, 2021	Germany	media	nefilim
	May 26, 2021	Germany	e-commerce	nefilim
	May 31, 2021	United states	Education	marketo
	May 30, 2021	Indonesia	Agricultural	marketo
	May 28, 2021	United states	Health Care	marketo
	May 27, 2021	United states	manufacturer	marketo
	May 24, 2021	Swedish	Security	marketo
	May 24, 2021	United states	Retail	marketo
	May 27, 2021	France	manufacturer	LV Ransomware
	May 28, 2021	United states	manufacturer	LV Ransomware
	May 30, 2021	United states	Law	LV Ransomware
	May 27, 2021	United states	Education	LV Ransomware
	May 28, 2021	United states	manufacturer	revil
	May 28, 2021	United Kingdom	Financial	revil
	May 27, 2021	Germany	Store	revil
	May 24, 2021	china	Financial	revil
	May 30, 2021	Mexico	Hotel	revil
	May 24, 2021	United Kingdom	Education	conti
	May 24, 2021	India	manufacturer	conti
	May 24, 2021	Germany	Education	conti
	May 24, 2021	France	Hotel	conti
	May 25, 2021	Luxembourg	manufacturer	conti
	May 25, 2021	France	Consultancy	conti
	May 25, 2021	United states	education	conti
	May 25, 2021	France	Real estate	conti
	May 25, 2021	Taiwan	manufacturer	avaddon
	May 25, 2021	France	Consultancy	avaddon
	May 25, 2021	Germany	manufacturer	avaddon
	May 25, 2021	Brazil	Agricultural	avaddon
	May 25, 2021	United states	Health Care	avaddon
	May 25, 2021	Portugal	manufacturer	avaddon
	May 25, 2021	Australia	Telecommunication	avaddon
	May 25, 2021	Vietnam	manufacturer	avaddon
	May 25, 2021	Ireland	Telecommunication	avaddon
	May 25, 2021	czech	Industrials	avaddon
	May 25, 2021	czech	Industrials	avaddon
	May 25, 2021	Romania	Industrials	avaddon
	May 25, 2021	Australia	Construction	avaddon

Press enter or click to view image in full size

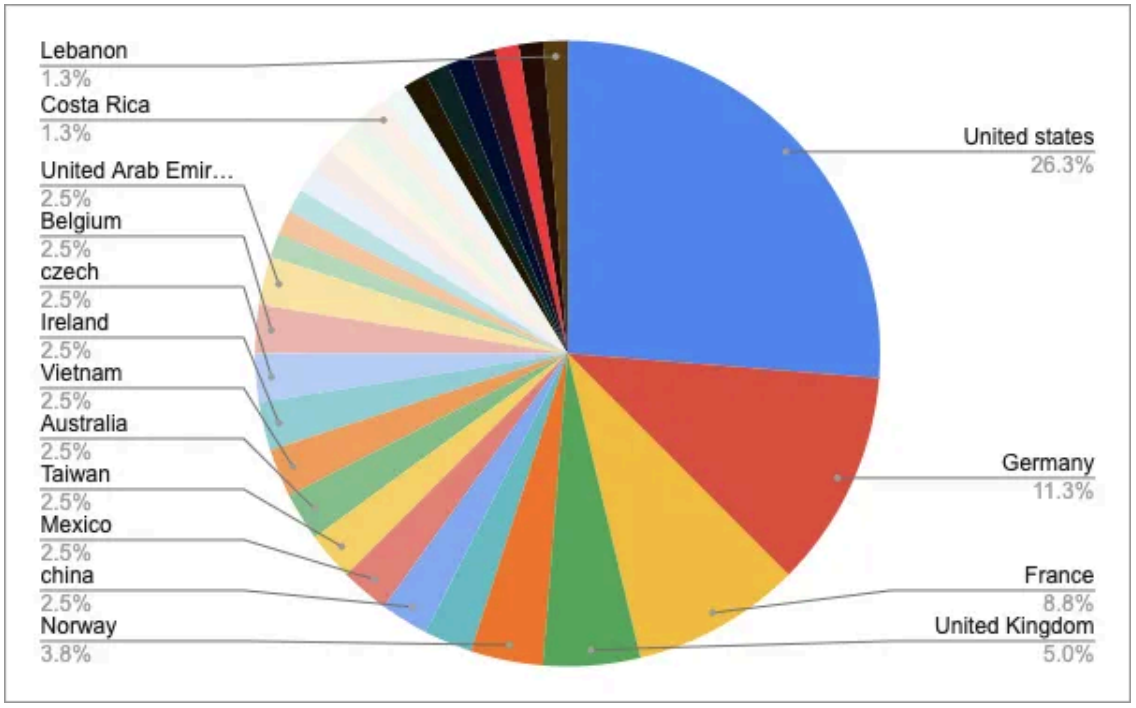
	May 26, 2021	Ireland	Financial	avaddon
	May 26, 2021	Taiwan	manufacturer	avaddon
	May 26, 2021	Belgium	Consultancy	avaddon
	May 26, 2021	France	media	avaddon
	May 26, 2021	Belgium	Law	avaddon
	May 26, 2021	Germany	Industrials	avaddon
	May 26, 2021	Costa Rica	Store	avaddon
	May 26, 2021	United states	manufacturer	avaddon
	May 28, 2021	Jamaica	Financial	avaddon
	May 28, 2021	Vietnam	Transportation	avaddon
	May 28, 2021	Germany	Consultancy	avaddon
	May 28, 2021	Germany	manufacturer	avaddon
	May 28, 2021	Mexico	Gamble	avaddon
	May 28, 2021	Kuwait	Service	avaddon
	May 28, 2021	United states	Financial	avaddon
	May 30, 2021	United states	Construction	avaddon
	May 30, 2021	Itay	Transportation	avaddon
	May 30, 2021	Canada	Industrials	avaddon
	May 30, 2021	China	Real estate	avaddon
	May 30, 2021	United states	Service	avaddon
	May 30, 2021	Switzerland	Service	avaddon
	May 30, 2021	United Kingdom	Law	avaddon
	May 25, 2021	France	Consultancy	Ragnar Locker
	May 26, 2021	Germany	Industrials	Ragnar Locker
	May 24, 2021	United states	Education	xing locker
	May 24, 2021	United states	Health Care	xing locker
	May 27, 2021	United Arab Emirates	Real estate	xing locker
	May 30, 2021	United Kingdom	manufacturer	Grief
	May 27, 2021	Italy	Government	Grief
	May 27, 2021	Spain	Store	Grief
	May 28, 2021	Dominica	Real estate	Grief
	May 27, 2021	United states	Government	Grief
	May 29, 2021	Norway	Store	Prometheus
	May 29, 2021	United states	Hotel	Prometheus
	May 27, 2021	Lebanon	Agricultural	Prometheus
	May 27, 2021	United Arab Emirates	Service	Prometheus
	May 27, 2021	Norway	Service	Prometheus
	May 27, 2021	Norway	Construction	Prometheus
	May 26, 2021	United states	Health care	Prometheus
	May 28, 2021	United states	Education	doppelpaymer
	May 30, 2021	United states	Automotive	doppelpaymer

- For a week, a total of 80 victimized firms were mentioned and a change in the state of the data leaked from the victims in the ransomware site was detected.
- 11 threat groups' activities were detected.
- Compared to previous statistics 5 months ago, the number of victims increased by about 2.6 times, and the ransomware threat groups increased by 1.6 times that needs to raise awareness about ransomware attacks.

> Link to W1 Jan | EN | Story of the Week: Ransomware on the Darkweb

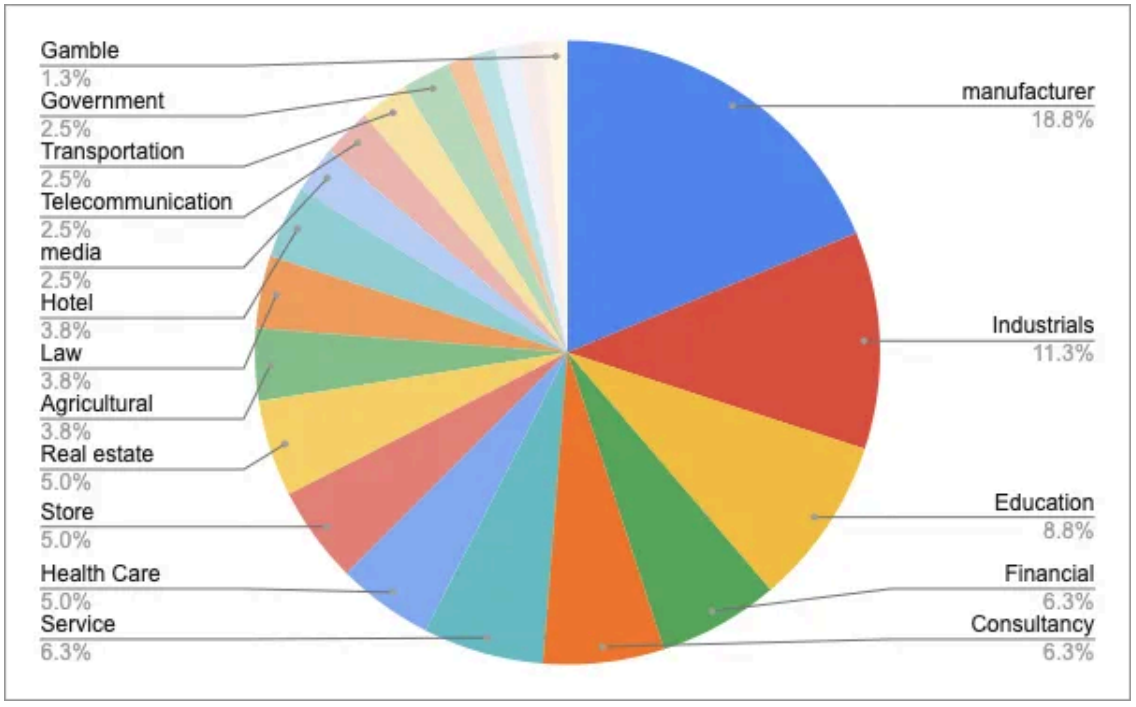
B. TOP 5 targeted countries

The United States was mostly positioned at top in terms of the rate of victim infection, but as the number of active ransomware threat groups increased, the percentage of victimized firms' country locations also varied.



1. United States — 26.3%
2. Germany — 11.3%
3. France — 8.8%
4. United Kingdom — 5.0%
5. Norway — 3.8%

C. TOP 5 targeted industrial sectors



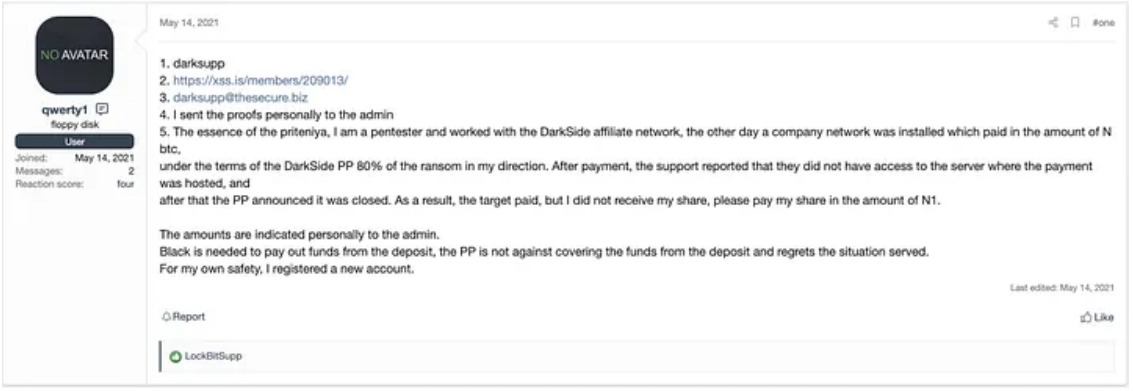
1. Manufacturer — 18.8%
2. industrial — 11.3%

3. Education — 8.8%
4. Financial & Consultancy & Service — 6.3%
5. Health Care & Store & Real estate — 5.0%

2. Posts related to Ransomware threat actors @Dark Web

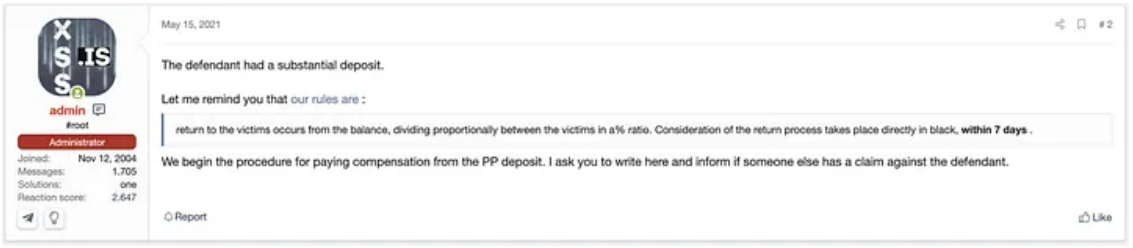
A. Darkside permanently banned from XSS forum

Press enter or click to view image in full size



On May 14th, the user (qwety1) of the XSS Forum claimed to the admin that the user did not receive any amount working as a pentester participating with the affiliate program of DarkSide Ransomware.

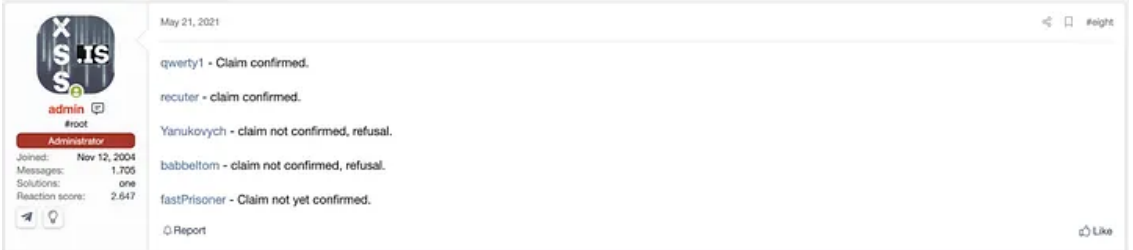
Press enter or click to view image in full size



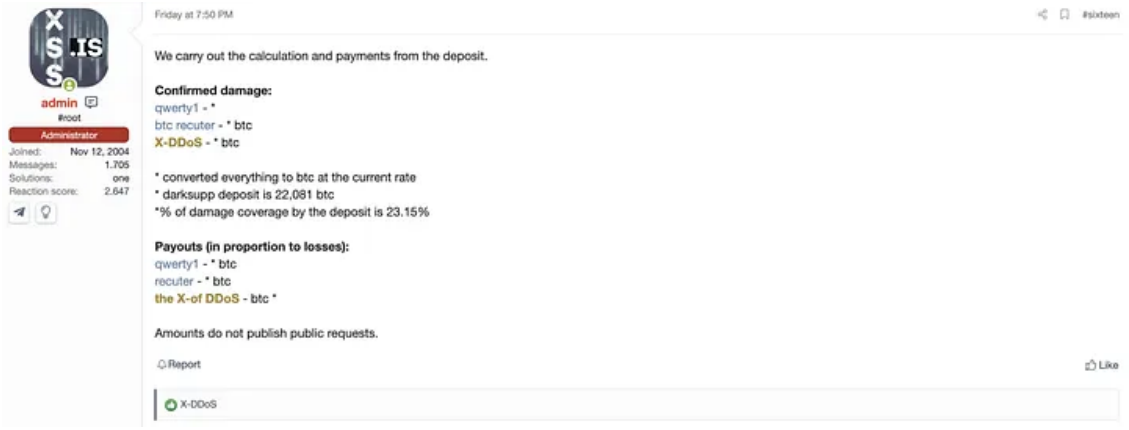
The administrator of the XSS Forum mentioned they begin the procedure for paying compensation with the rule of XSS Forum as below.

```
return to the victims occurs from the balance, dividing proportionally between the victims in a% rat
```

Press enter or click to view image in full size



Press enter or click to view image in full size



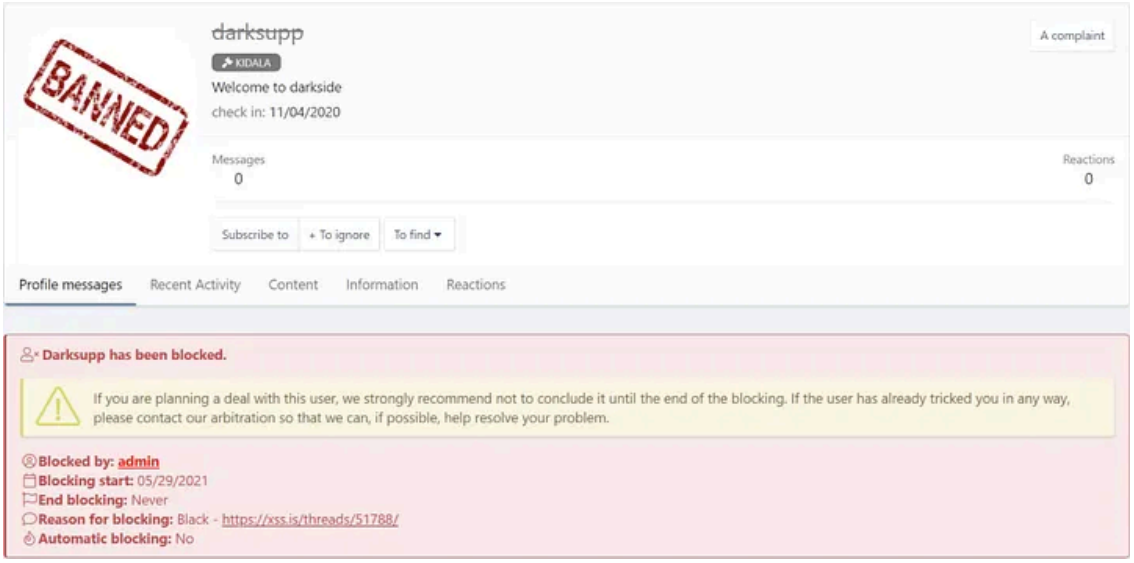
The administrator started reviewing proofs for 6 asserting users of participated in Darkside ransomware affiliate program. After that, 3 users were confirmed and compensated its loss by admin.

Press enter or click to view image in full size


```
XSS.IS adminThanks to all. The question is closed.
darksupp(Darkside ransomware's Operator) - the status is set. But I want to emphasize that the statu
Appeared faded> there was a "cut" of the deposit> the status is set. This is the observance of the p
Since I do not know anything, I am not ready to take responsibility for any loud statements and will
My job is just to follow the rules honestly, clearly and correctly.
```

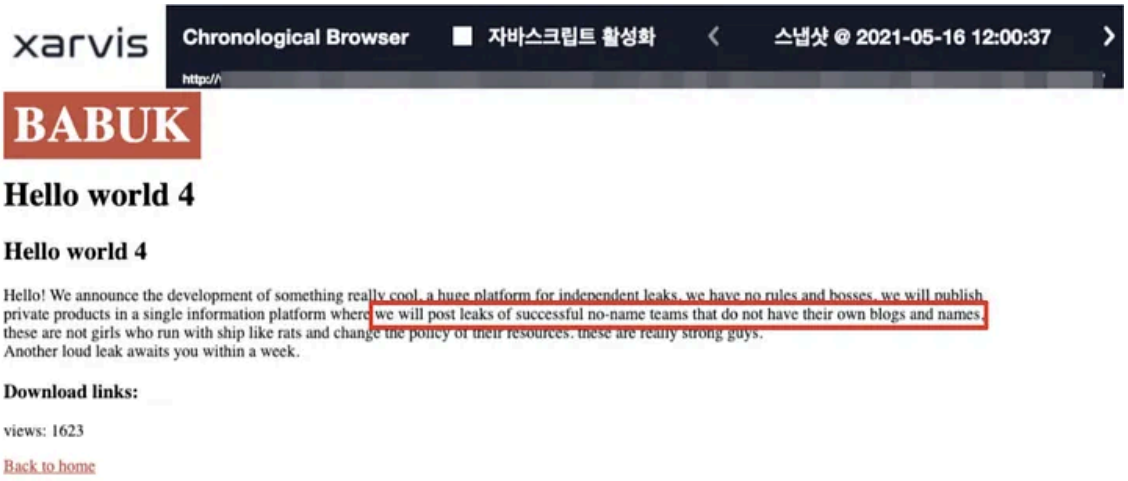
As a consequence, Darkside is banned by administrator violating the forum policy as a scammer.

Press enter or click to view image in full size



B. Babuk ransomware rebranded as Payload[.]bin

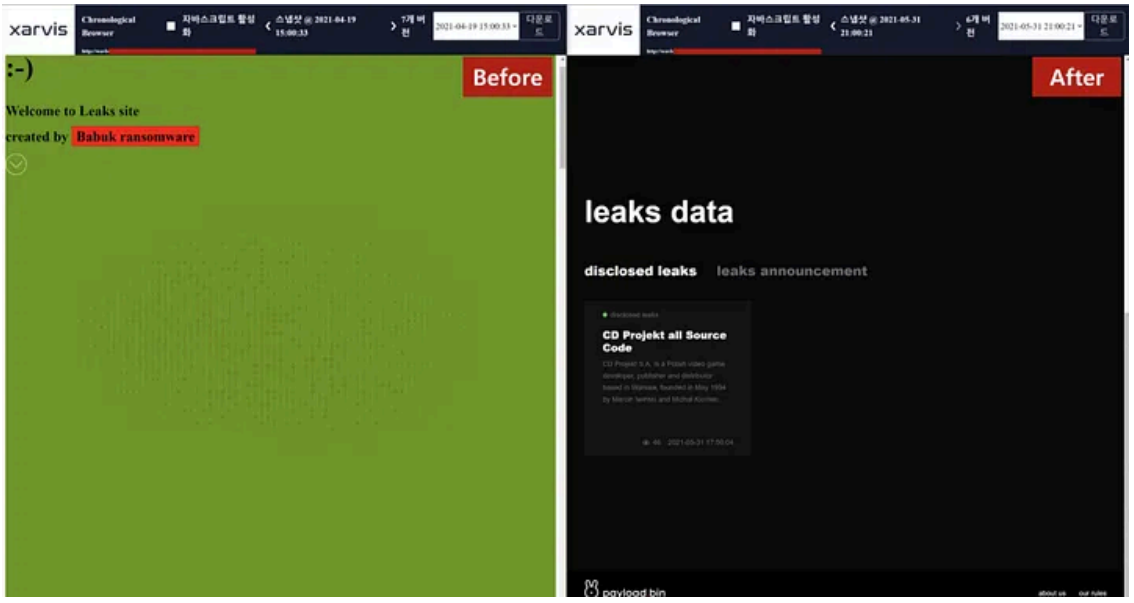
Press enter or click to view image in full size



> Link to W4 May | EN | Story of the Week: Ransomware on the Darkweb

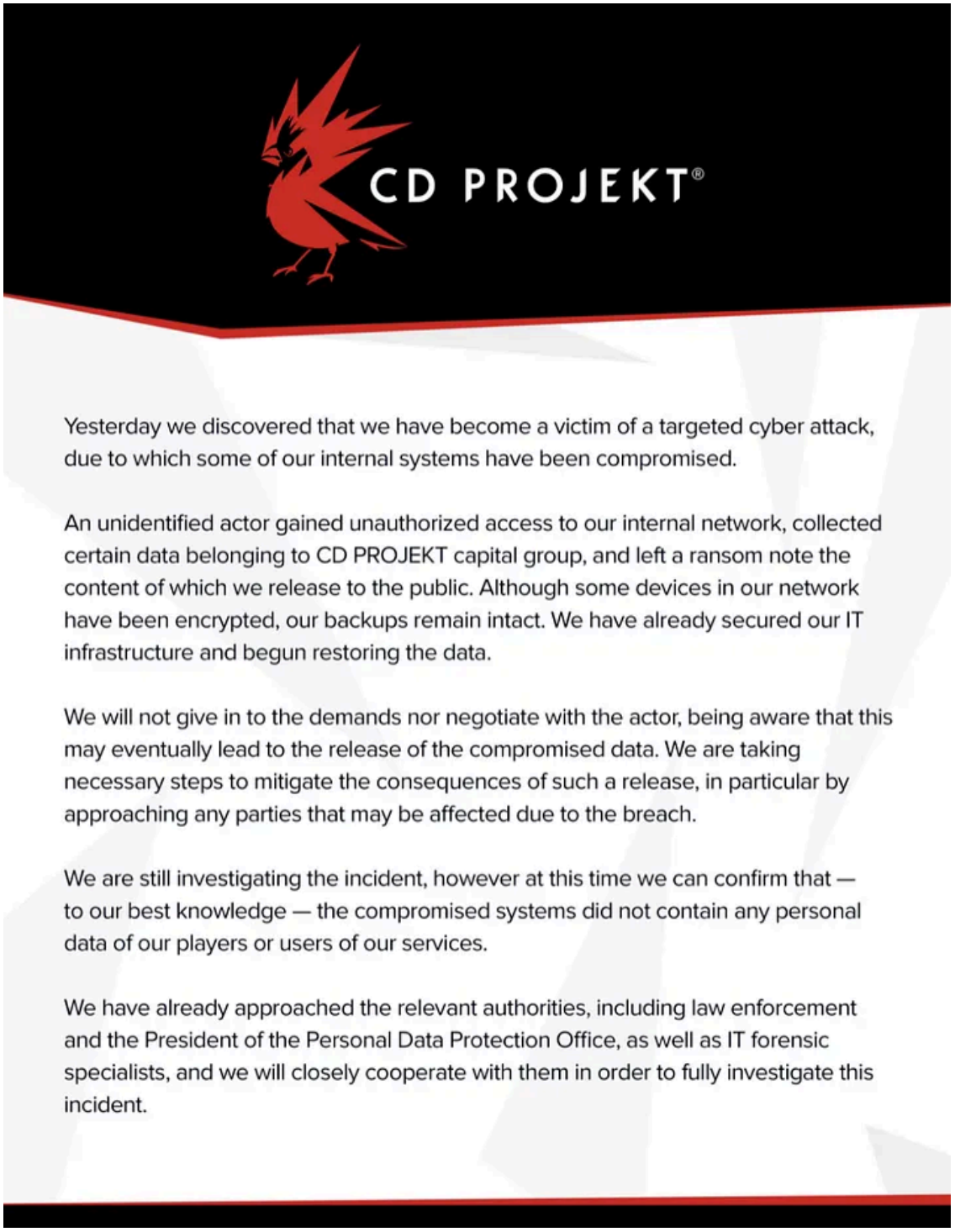
Last week, we covered a post where the Babuk ransomware launch an integrated platform gathering partners who don’t have a data leak site, and operate them instead. On May 31, the Babuk ransomware rebranded as Payload Bin and re-organised the homepage.

Press enter or click to view image in full size



All leaks data previously disclosed by the Babuk ransomware disappeared with renewal but CD Projekt's source code data. The CD PROJEKT's source code leak is an incident found to be related to HelloKitty ransomware on Feb 9.

Press enter or click to view image in full size



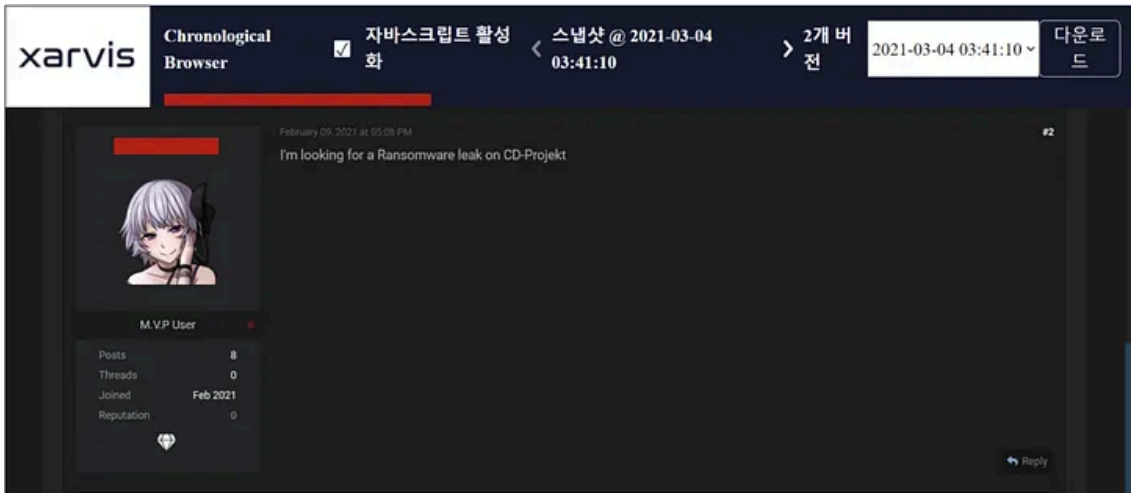
Ransomware damage announced by CD Projekt

Press enter or click to view image in full size

Ransom note released by CD Projekt via Twitter

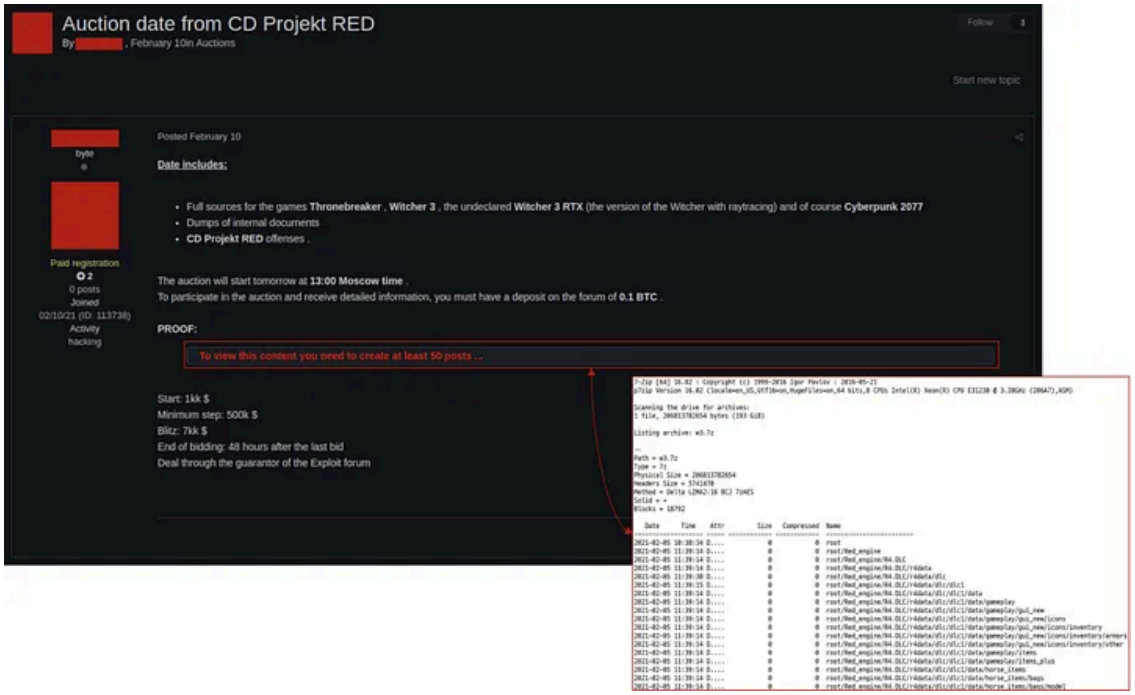
> *https://twitter.com/CDPROJEKTRED/status/1359048125403590660/photo/1*

Press enter or click to view image in full size



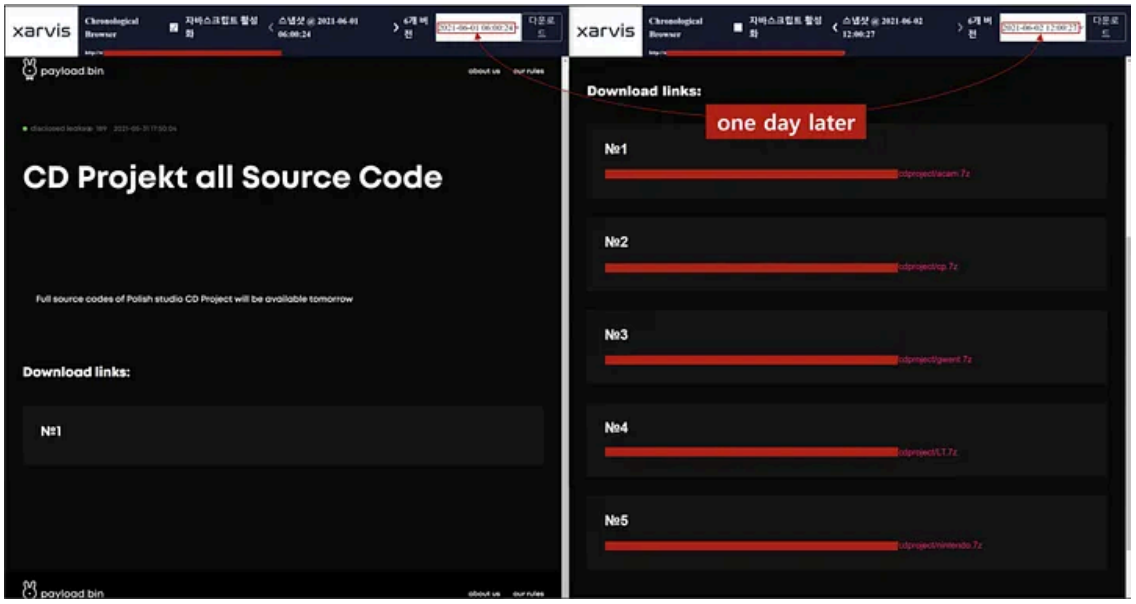
After the announcement, there was a user looking for the leaked data regarding CD Projekt's incident.

Press enter or click to view image in full size



However, there wasn't any free sharing page on DDW, rather a seller appeared trying to sell the source code of CD Projekt on DDW as a form of auction.

Press enter or click to view image in full size



As Babuk announced, the data appears to be CD Projekt's data which was stolen by HelloKitty ransomware regarding previous incident, and they seem to be partnered with Babuk ransomware now rebranded as Payload Bin.

Conclusion

- The number of victims mentioned on data leak site operated by ransomware is rapidly increasing compared to 5 months ago, so it needs to be vigilant
- Babuk ransomware rebranded as Payload Bin, appears to strengthen its strategy of threatening victims by focusing on exfiltrating the data by partnering with the previously active ransomware groups who did not have their own data leak page.

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

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