

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

 medium.com/s2wlab/w1-jun-en-story-of-the-week-ransomware-on-the-darkweb-af491d33868b

Hyunmin Suh

June 3, 2021



Hyunmin Suh

Jun 2, 2021

6 min read

Corporate Data Matters

Co-Author: , , YH Jeong @ Talon



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)

Aa 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

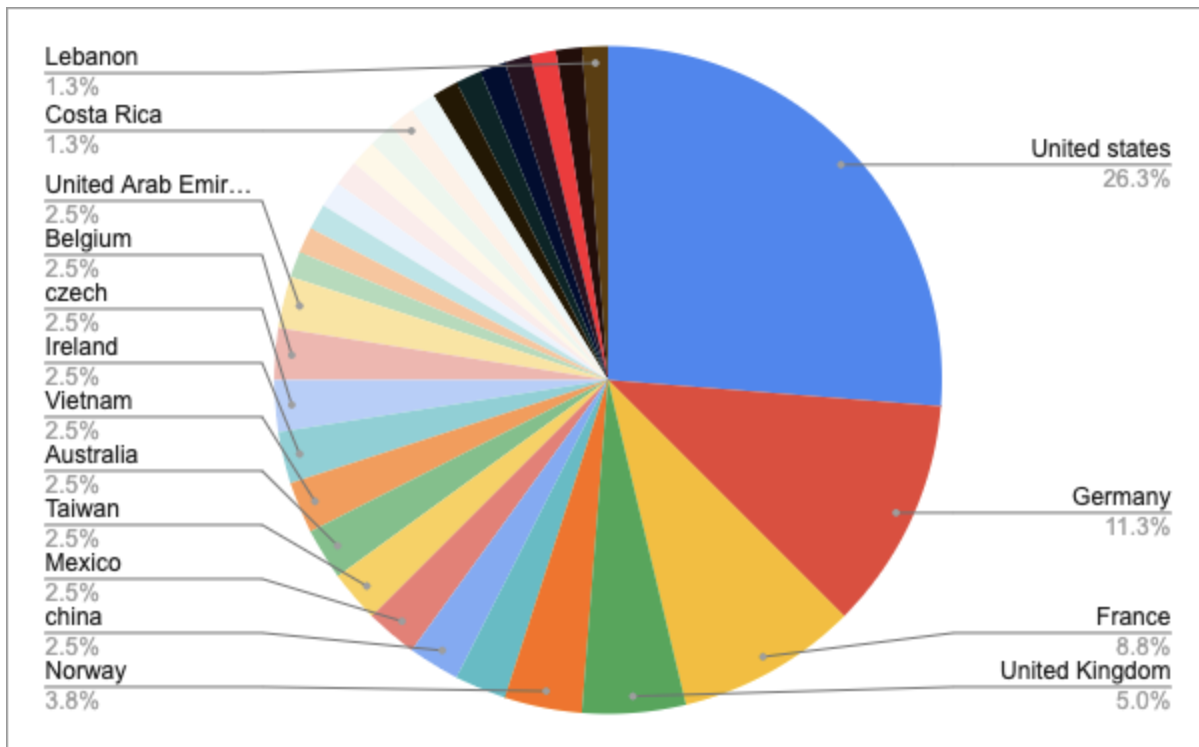
	May 26, 2021	Ireland	Financial	avaddon
	May 26, 2021	Taiwan	manufacturer	avaddon
	May 26, 2021	Belgium	Consultancy	avaddon
	May 26, 2021	France	media	avaddon
	May 26, 2021	Belgium	Law	avaddon
	May 26, 2021	Germany	Industrials	avaddon
	May 26, 2021	Costa Rica	Store	avaddon
	May 26, 2021	United states	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	Italy	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](#)

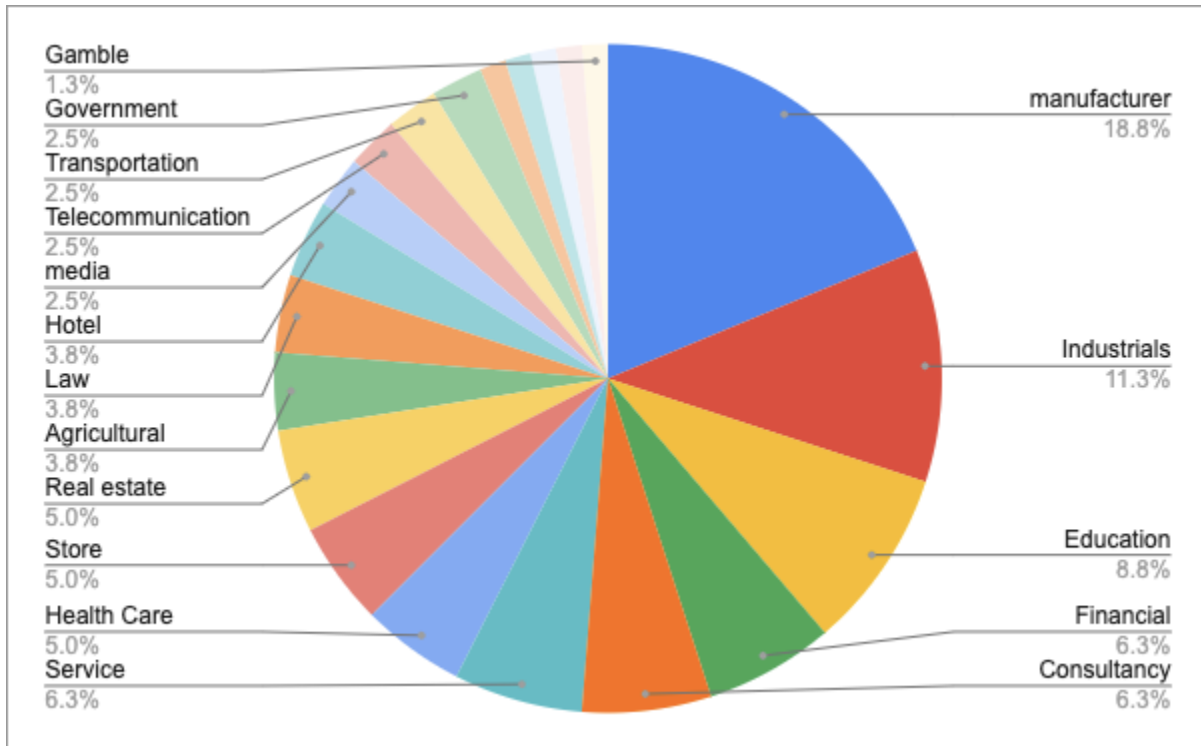
B. TOP 5 targeted countries

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

NO AVATAR

qwerty1

floppy disk

User

Joined: May 14, 2021

Messages: 2

Reaction score: four

May 14, 2021

#one

1. darksupp
2. <https://xss.is/members/209013/>
3. darksupp@thesecure.biz
4. I sent the proofs personally to the admin
5. The essence of the priteniya, I am a pentester and worked with the DarkSide affiliate network, the other day a company network was installed which paid in the amount of N btc, under the terms of the DarkSide PP 80% of the ransom in my direction. After payment, the support reported that they did not have access to the server where the payment was hosted, and after that the PP announced it was closed. As a result, the target paid, but I did not receive my share, please pay my share in the amount of N1.

The amounts are indicated personally to the admin.
 Black is needed to pay out funds from the deposit, the PP is not against covering the funds from the deposit and regrets the situation served.
 For my own safety, I registered a new account.

Last edited: May 14, 2021

Report Like

+ LockBitSupp

On May 14th, the user (qwerty1) 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.

May 15, 2021 # 2

The defendant had a substantial deposit.

Let me remind you that our rules are :

return to the victims occurs from the balance, dividing proportionally between the victims in a% ratio. Consideration of the return process takes place directly in black, within 7 days .

We begin the procedure for paying compensation from the PP deposit. I ask you to write here and inform if someone else has a claim against the defendant.

Report Like

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% ratio. Consideration of the return process takes place directly in black, within 7 days .

May 21, 2021 #eight

qwerty1 - Claim confirmed.

recuter - claim confirmed.

Yanukovych - claim not confirmed, refusal.

babeltom - claim not confirmed, refusal.

fastPrisoner - Claim not yet confirmed.

Report Like

Friday at 7:50 PM #sixteen

We carry out the calculation and payments from the deposit.

Confirmed damage:
 qwerty1 - * btc
 btc recuter - * btc
 X-DDoS - * btc

* converted everything to btc at the current rate
 * darksupp deposit is 22,081 btc
 *% of damage coverage by the deposit is 23.15%

Payouts (in proportion to losses):
 qwerty1 - * btc
 recuter - * btc
 the X-of DDoS - btc *

Amounts do not publish public requests.

Report Like

X-DDoS

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.

Saturday at 11:28 am # 23

Thanks to all. The question is closed.

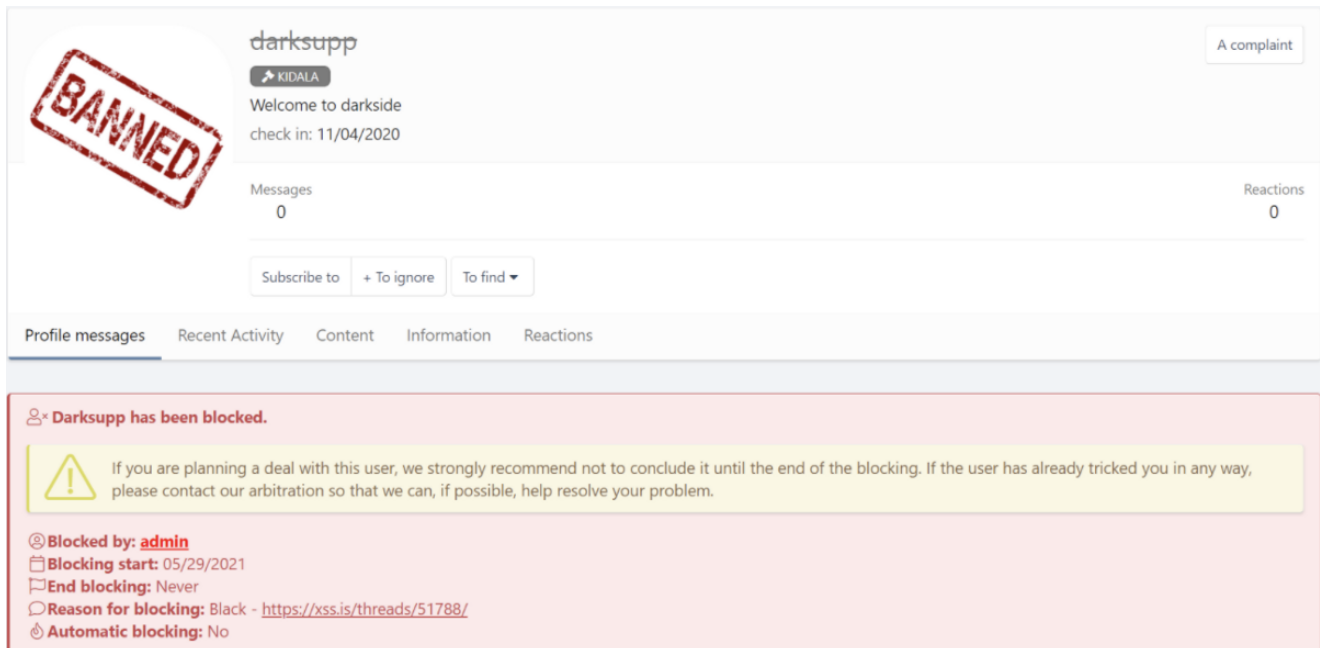
darksupp - the status is set. But I want to emphasize that the status is set purely on a formal basis. Appeared faded> there was a "cut" of the deposit> the status is set. This is the observance of the procedure, nothing more. Since I do not know anything, I am not ready to take responsibility for any loud statements and will not hang labels. My job is just to follow the rules honestly, clearly and correctly.

A complaint Report Like

Unknown, Quake3, Madzin and 1 more person

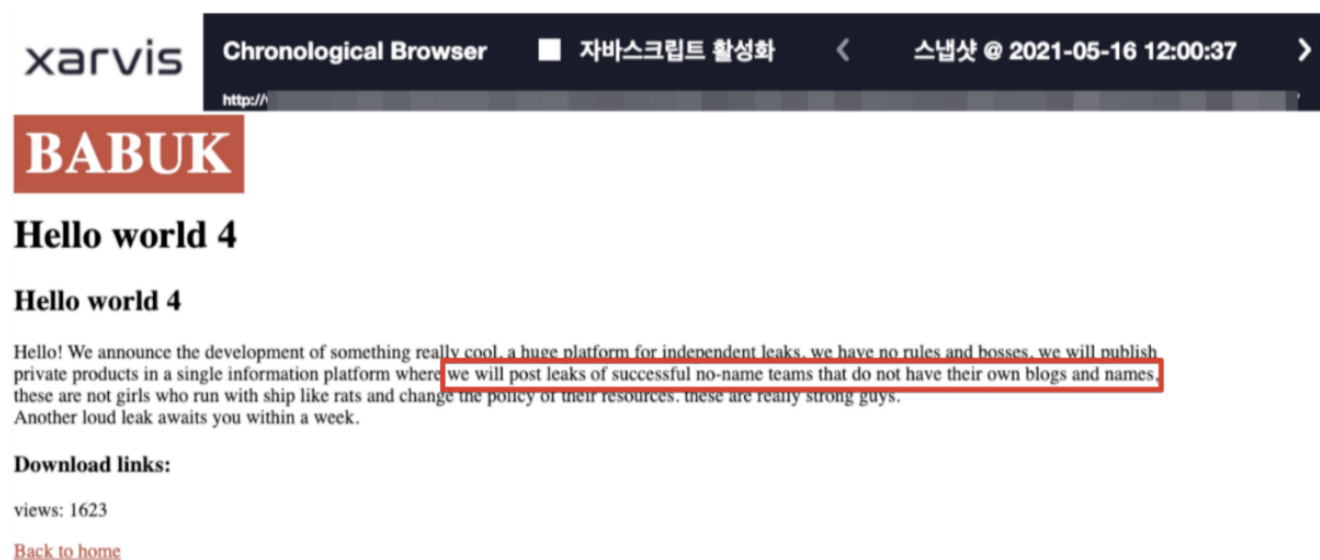
XSS.IS admin Thanks to all. The question is closed. darksupp (Darkside ransomware's Operator) - the status is set. But I want to emphasize that the status is set purely on a formal basis. Appeared faded> there was a "cut" of the deposit> the status is set. This is the observance of the procedure, nothing more. Since I do not know anything, I am not ready to take responsibility for any loud statements and will not hang labels. 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.



The screenshot shows a forum profile for a user named 'darksupp'. A large red 'BANNED' stamp is overlaid on the profile picture. The profile includes a 'KIDALA' badge, a 'Welcome to darkside' message with a 'check in: 11/04/2020' timestamp, and statistics for 'Messages' (0) and 'Reactions' (0). Below the profile are buttons for 'Subscribe to', '+ To ignore', and 'To find'. A navigation bar at the bottom of the profile section includes 'Profile messages', 'Recent Activity', 'Content', 'Information', and 'Reactions'. A prominent red notification banner states: 'Darksupp has been blocked.' Below this, a yellow warning box contains a triangle icon and text: 'If you are planning a deal with this user, we strongly recommend not to conclude it until the end of the blocking. If the user has already tricked you in any way, please contact our arbitration so that we can, if possible, help resolve your problem.' Further down, details of the block are listed: 'Blocked by: admin', 'Blocking start: 05/29/2021', 'End blocking: Never', 'Reason for blocking: Black - https://xss.is/threads/51788/', and 'Automatic blocking: No'.

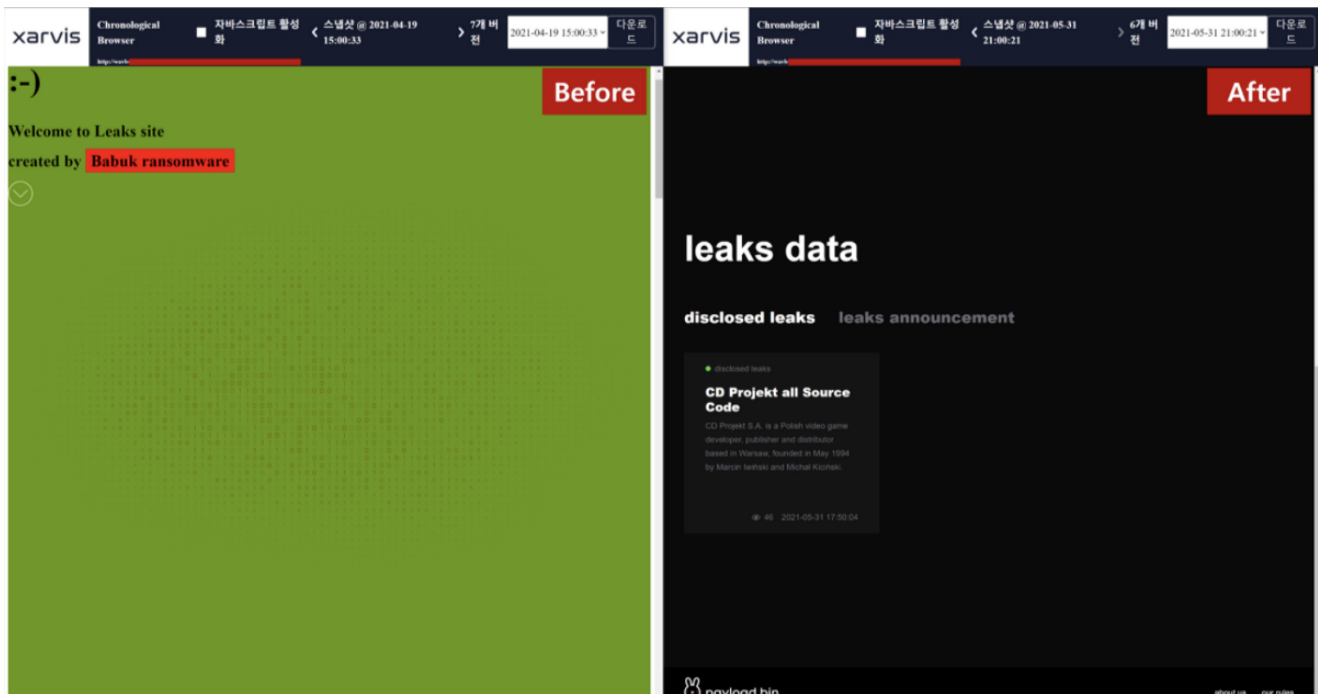
B. Babuk ransomware rebranded as Payload[.]bin



The screenshot shows a website interface. At the top, there is a navigation bar with 'xarvis' on the left, 'Chronological Browser' in the center, and '자바스크립트 활성화' (JavaScript Enabled) on the right. A date and time stamp '스냅샷 @ 2021-05-16 12:00:37' is also visible. Below the navigation bar, the word 'BABUK' is displayed in large, bold, white letters on a dark red background. Underneath, the text 'Hello world 4' is repeated twice. A paragraph of text follows: '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.' The quote 'we will post leaks of successful no-name teams that do not have their own blogs and names' is highlighted with a red border. Below the text, there is a section for 'Download links:' followed by 'views: 1623' and a 'Back to home' link.

| [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.



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.



CD PROJEKT®

Yesterday we discovered that we have become a victim of a targeted cyber attack, due to which some of our internal systems have been compromised.

An unidentified actor gained unauthorized access to our internal network, collected certain data belonging to CD PROJEKT capital group, and left a ransom note the content of which we release to the public. Although some devices in our network have been encrypted, our backups remain intact. We have already secured our IT infrastructure and begun restoring the data.

We will not give in to the demands nor negotiate with the actor, being aware that this may eventually lead to the release of the compromised data. We are taking necessary steps to mitigate the consequences of such a release, in particular by approaching any parties that may be affected due to the breach.

We are still investigating the incident, however at this time we can confirm that — to our best knowledge — the compromised systems did not contain any personal data of our players or users of our services.

We have already approached the relevant authorities, including law enforcement and the President of the Personal Data Protection Office, as well as IT forensic specialists, and we will closely cooperate with them in order to fully investigate this incident.

Ransomware damage announced by CD Projekt

```
read_me_unlock - Notepad
File Edit Format View Help
@
!!!!!!!!!!!!!!!!!!!! Hello CD PROJEKT !!!!!!!!!!!!!!!!!!!!!

Your have been EPICALLY pwned!!

We have dumped FULL copies of the source codes from your Perforce server for Cyberpunk 2077, Witcher 3, Gwent and the unreleased version of Witcher 3!!!

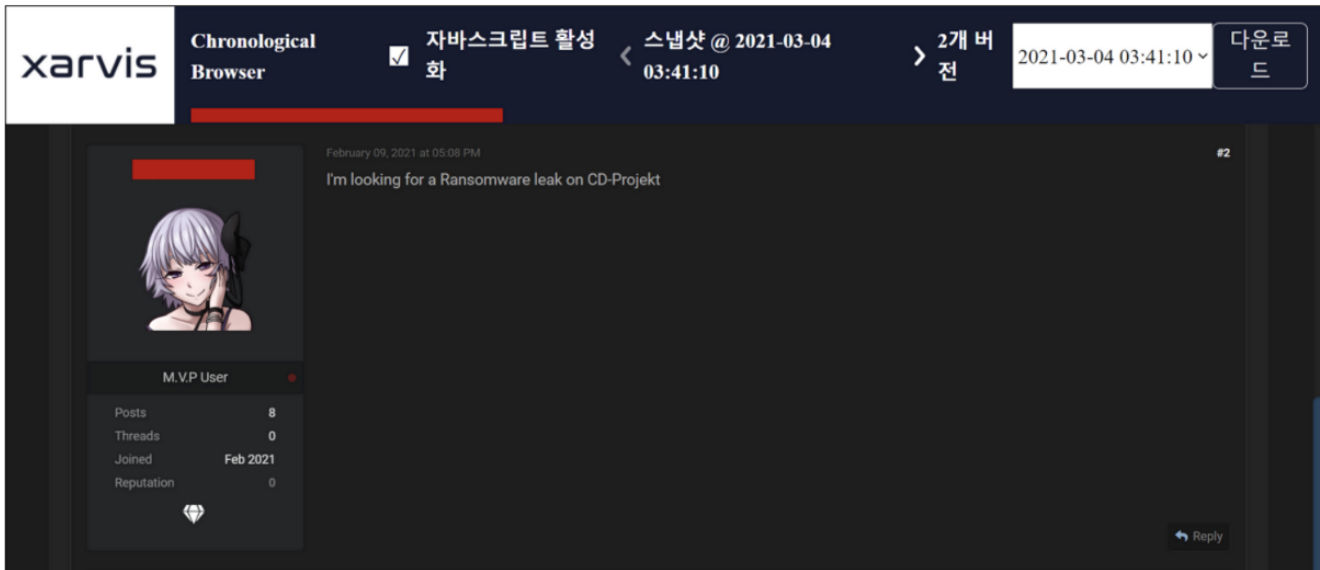
We have also dumped all of your documents relating to accounting, administration, legal, HR, investor relations and more!

Also, we have encrypted all of your servers, but we understand that you can most likely recover from backups.

If we will not come to an agreement, then your source codes will be sold or leaked online and your documents will be sent to our contacts in gaming journalism. Your public image will go down the shitter even more and people will see how you shitty your company functions. Investors will lose trust in your company and the stock will dive even lower!

You have 48 hours to contact us.]
```

Ransom note released by CD Projekt via Twitter



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

Auction date from CD Projekt RED
By [redacted], February 10 in Auctions

Posted February 10

Date includes:

- Full sources for the games **Thronebreaker**, **Witcher 3**, the undeclared **Witcher 3 RTX** (the version of the Witcher with raytracing) and of course **Cyberpunk 2077**
- Dumps of internal documents
- CD Projekt RED offenses .

The auction will start tomorrow at **13:00 Moscow time** .
To participate in the auction and receive detailed information, you must have a deposit on the forum of **0.1 BTC** .

PROOF:

To view this content you need to create at least 50 posts ...

```

7-Zip [64] : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
677ip Version 16.02 (locale=en_US,UTF16-on,HugeFiles-on,64 bits,8 CPUs Intel(R) Xeon(R) CPU E31220 @ 3.20GHz (26847),A90)

Scanning the drive for archives:
1 file, 286613782654 bytes (193 GiB)

Listing archive: w3.7z
---
Path = w3.7z
Type = 7z
Physical Size = 286613782654
Headers Size = 3742478
Method = Delta LZMA2:16 BC3 7AES
Solid = +
Blocks = 18792

Date      Time      Attr      Size  Compressed  Name
-----
2021-02-05 10:30:34 D...  0         0      root
2021-02-05 11:39:14 D...  0         0      root/Red_engine
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc
2021-02-05 11:39:15 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/data
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/data/gameplay
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/data/gameplay/gpu_new
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/data/gameplay/gpu_new/icons
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/data/gameplay/gpu_new/icons/inventory
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/data/gameplay/gpu_new/icons/inventory/armors
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/dlc/data/gameplay/items
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/dlc/data/gameplay/items_plus
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/dlc/data/horse_items
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/dlc/data/horse_items/bags
2021-02-05 11:39:14 D...  0         0      root/Red_engine/R4.SLC/r4data/dlc/dlc/dlc/data/horse_items/bags/model
  
```

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.

CD Projekt all Source Code

Full source codes of Polish studio CD Projekt will be available tomorrow

Download links:

№1 [redacted]

Download links:

№1 [redacted]

№2 [redacted] `cdproject/acam.7z`

№3 [redacted] `cdproject/cp.7z`

№4 [redacted] `cdproject/gwent.7z`

№5 [redacted] `cdproject/L.T.7z`

№6 [redacted] `cdproject/nintendo.7z`

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.