Ransomware Evolution | How Cheated Affiliates Are Recycling Victim Data for Profit

By Jim Walter

Published: 2024-04-24 · Archived: 2026-04-05 16:28:40 UTC

Threat actors consistently alter and develop their schemes in order to further escalate their payoffs. In a new trend, ransomware affiliates are actively re-monetizing stolen data outside of their original RaaS agreements, especially as financial squabbles between threat actors emerge in the ransomware economy. The affiliates in such instances are starting to work with third-parties or external data leak services in order to re-extort victims who have already paid the ransom to the original attackers.

This blog post examines how affiliate attackers are embracing this new third-party extortion method, illustrated most recently by the ostensibly back-to-back cyberattacks on Change Healthcare and the emergence of services like RansomHub and Dispossessor.

ALPHV Exit Scam & Re-Extortion by RansomHub

In February 2024, a subsidiary of healthcare giant UnitedHealth Group (UHG) was forced to take down its IT systems and various services. The root of the disruption was a cyberattack by a BlackCat (*aka* ALPHV) affiliate on Change Healthcare, a healthcare technology platform used by the subsidiary.

Post-attack, ALPHV ransomware operators reportedly took down their data leak blog, servers, and operation negotiation sites, and failed to pay the affiliate their agreed share of the ransom.

Purportedly, Change Healthcare paid out the $22 million ransom demand, only to be targeted a second time just weeks after recovering from the initial attack. This time around, the ransomware attack was claimed by a threat actor working in conjunction with RansomHub, a new extortion group claiming to hold 4 terabytes of the victim's sensitive data including personally identifiable information (PII) of active U.S. military personnel, patient records, and payment information.

It is believed that after ALPHV reneged on their payment, the affiliate partnered with RansomHub and re-used the data stolen from the initial attack in order to secure a pay off. At the time of writing, Change Healthcare has been removed from RansomHub's DLS on April, 20, 2024, presumably due to payment and cooperation with the threat actors.

Change HealthCare - OPTUM Group - United HealthCare Group

Hello Change Health and United Health Groups,

As an introduction we will give everyone a fast update on what happened previously and on the current situation.

ALPHV stole the ransom payment (22 Million USD) that Change Healthcare and United Health payed in order to restore their systems and prevent the data leak.

HOWEVER we have the data and not ALPHV.

The data consists of over 4 TB of highly selective data. The data relates to all Change Health clients that have sensitive data being processed by the company.

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:
- Medicare
- Tricare
- CVS-CareMark
- Loomis

RansomHub and Change Healthcare Posting

RansomHub RaaS

RansomHub emerged in early February 2024 with a simple data leak site (DLS). Their focus mirrors other historically well-known operations such as REvil, ALPHV, and Play with regards to their core values and overall mission statements.

README_9daasd.txt

```
Hello!

Visit our Blog:
    Tor Browser Links:
        http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/
    Links for normal browser:
        http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/


>>> Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your
    data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for
     a long time. The sooner you pay the ransom, the sooner your company will be safe.



>>> If you have an external or cloud backup; what happens if you don't agree with us?

All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not
    agree with us, information pertaining to your companies and the data of your company's customers will be
    published on the internet, and the respective country's personal data usage authority will be informed.
    Moreover, confidential data related to your company will be shared with potential competitors through
    email and social media. You can be sure that you will incur damages far exceeding the amount we are
    requesting from you should you decide not to agree with us.
```

Standard RansomHub ransom note

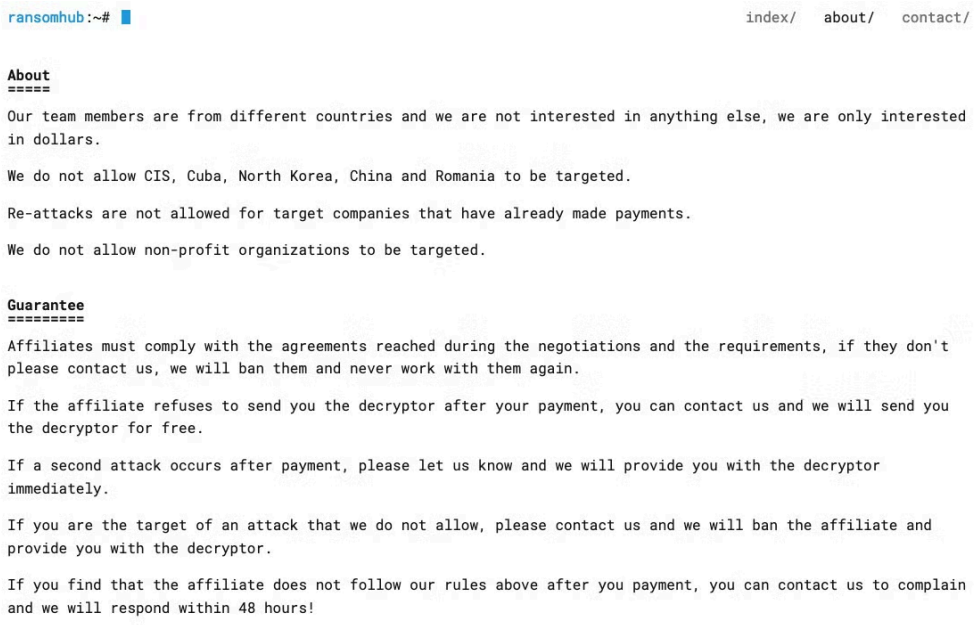
RansomHub operates as a ransomware-as-a-service (RaaS), partnering with affiliates that work with a variety of ransomware families, including ALPHV and LockBit. Notably, RansomHub works with other threat actors and groups to republish and rebroadcast the availability of victim data. There are multiple, revolving Telegram groups dedicated to amplifying the reach of RansomHub's leaks. An example of this is the "R3dd1sh_34_E4gl3_D4t4l34ks" channel (*aka* Reddish Eagle Dataleaks).

RandomHub archive amplified by R3dd1sh_34_E4gl3_D4t4l34ks

This development means that the data leak sites (DLSs) usually associated with a particular threat actor are no longer the only avenue of exposure for ransomware victims. Downstream amplification of these leaks is now common and generally open to all non-private Telegram or Discord groups.

Interestingly, according to RansomHub's own "rules", it does not allow:

- Affiliates to attack entities in the Commonwealth of Independent States (CIS), Cuba, China, Romania, or North Korea,
- Re-attacks for targeted companies that have already made payment, nor
- Attacks against non-profit organizations.



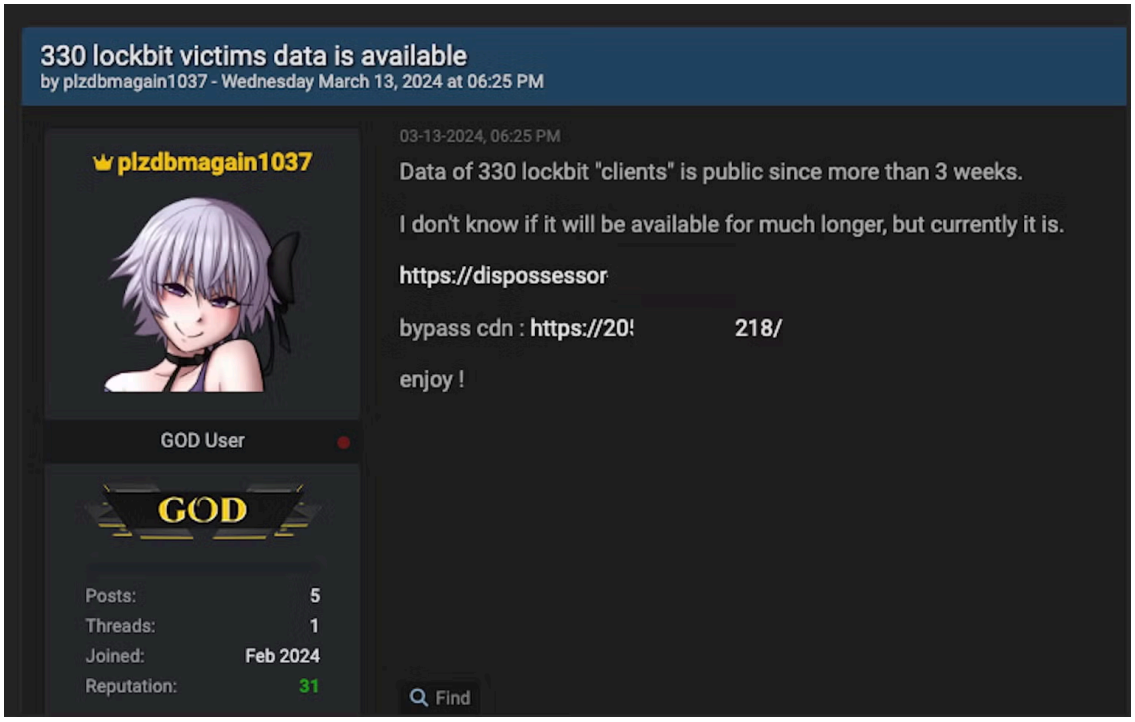
Original RansomHub About Page

However, given the current situation faced by Change Healthcare, the second bullet in the list above appears to be a gray area, especially if re-extorting ransomware victims constitutes an attack.

Our research indicates that multiple affiliates are now partnering with RansomHub in an effort to regain profitability following the apparent collapse of ALPHV.

Dispossessor Data Leak Blog

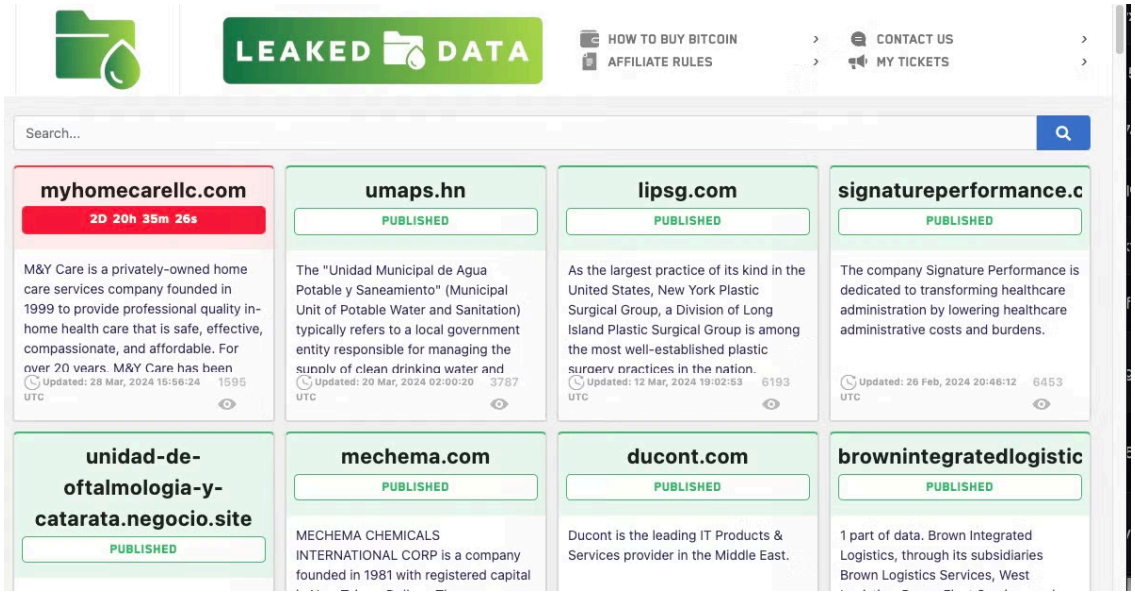
Dispossessor emerged in February of 2024, advertising the availability of previously-leaked data for download and potential sale. These announcements were placed across multiple forums and markets, including BreachForums and XSS.



Dispossessor announcement on Breachforums (LockBit data)

The X account @ransomfeednews recently posted regarding this new group, presenting their findings that indicated how Dispossessor *"is not ransomware, but a group of scoundrels trying to monetize (on nothing) using the claims of other groups."* The group is also active in Telegram, posting similar announcements across well-trafficked Telegram channels.

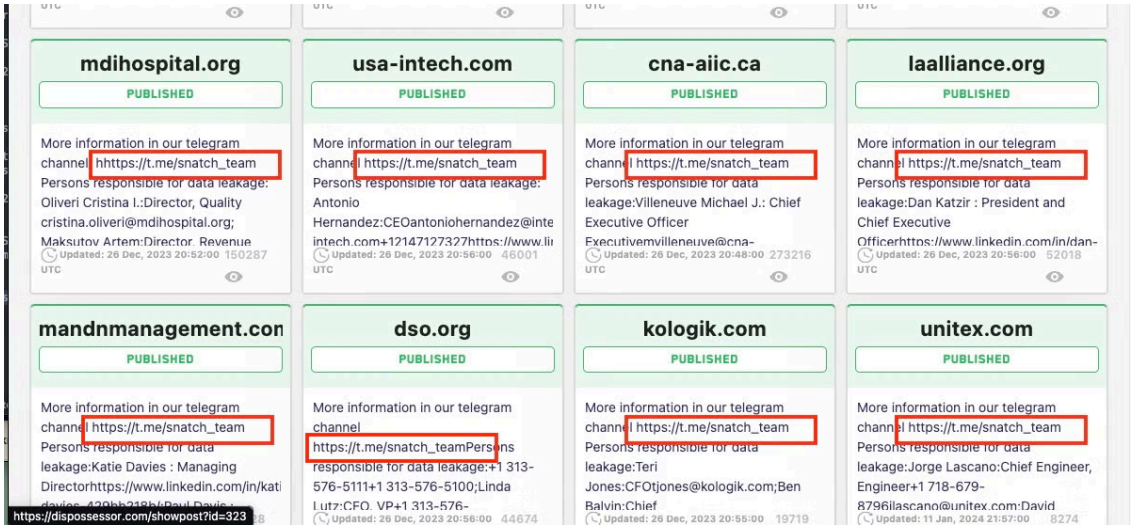
Dispossessor initially announced the renewed availability of the data from some 330 LockBit victims. This was claimed to be reposted data from previously available LockBit victims, now hosted on Dispossessor's network and thus not subject to LockBit's availability restrictions.



Dispossessor Blog

Dispossessor appears to be reposting data previously associated with other operations with examples ranging from Cl0p, Hunters International, and 8base. We are aware of at least a dozen victims listed on Dispossessor that have also been previously listed by other groups.

In addition, there are apparent links to other aggregate-style operators like Snatch.



Dispossessor Blog with Snatch links highlighted

In many cases, the Dispossessor page links to the Dispossessor-Cloud repository. One victim was originally on CL0P's data leak site in early 2023. Dispossessor's data is identical to that hosted in the original CL0P magnet links for this and other victims.

Rabbit Hole Data Leak Site (DLS)

A third emerging service with potential to contribute to the expansion of monetization of previously leaked victim data is Rabbit Hole DLS, first observed on March 13, 2024. In an English translation of the site's About Page, Rabbit Hole is described as a leaks "blog for small and medium-sized teams that do not have their own website". The site is currently promoted in forums and dark markets.

Translated Rabbit Hole Blog announcement

Original Postings (RU):

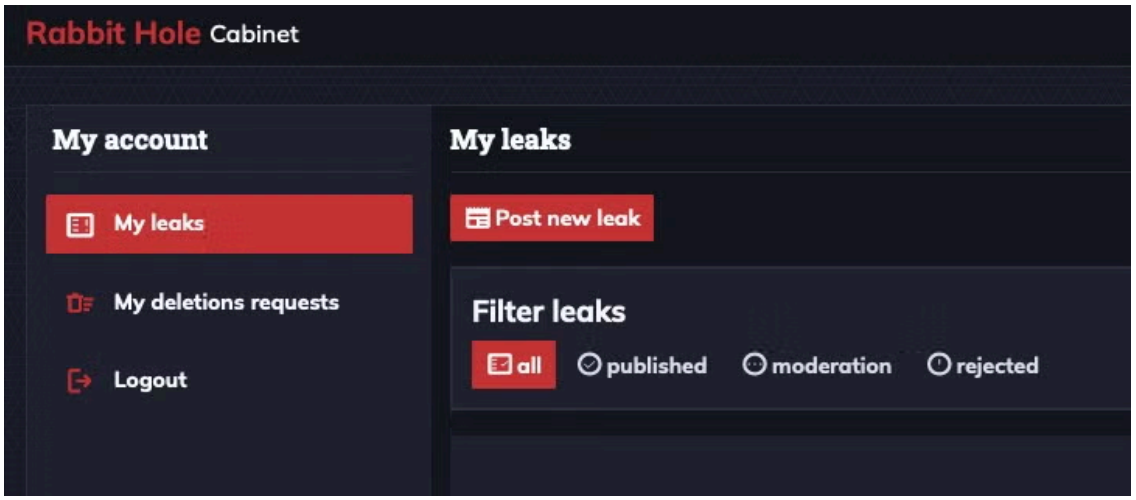
блог для малых и средних команд у которых нет своего сайта

кроличья нора не является рансом группой, это общий блог для малых и средних команд. данный блог создан в целях оказания давления на корпорации, за счет большого количества публикаций разных команд — кроличья нора предлагает вам пристанище, где вы можете опубликовать любую утечку [гос учреждения и больницы являются исключением]

Original Postings (EN):
blog for small and medium-sized teams that do not have their own website

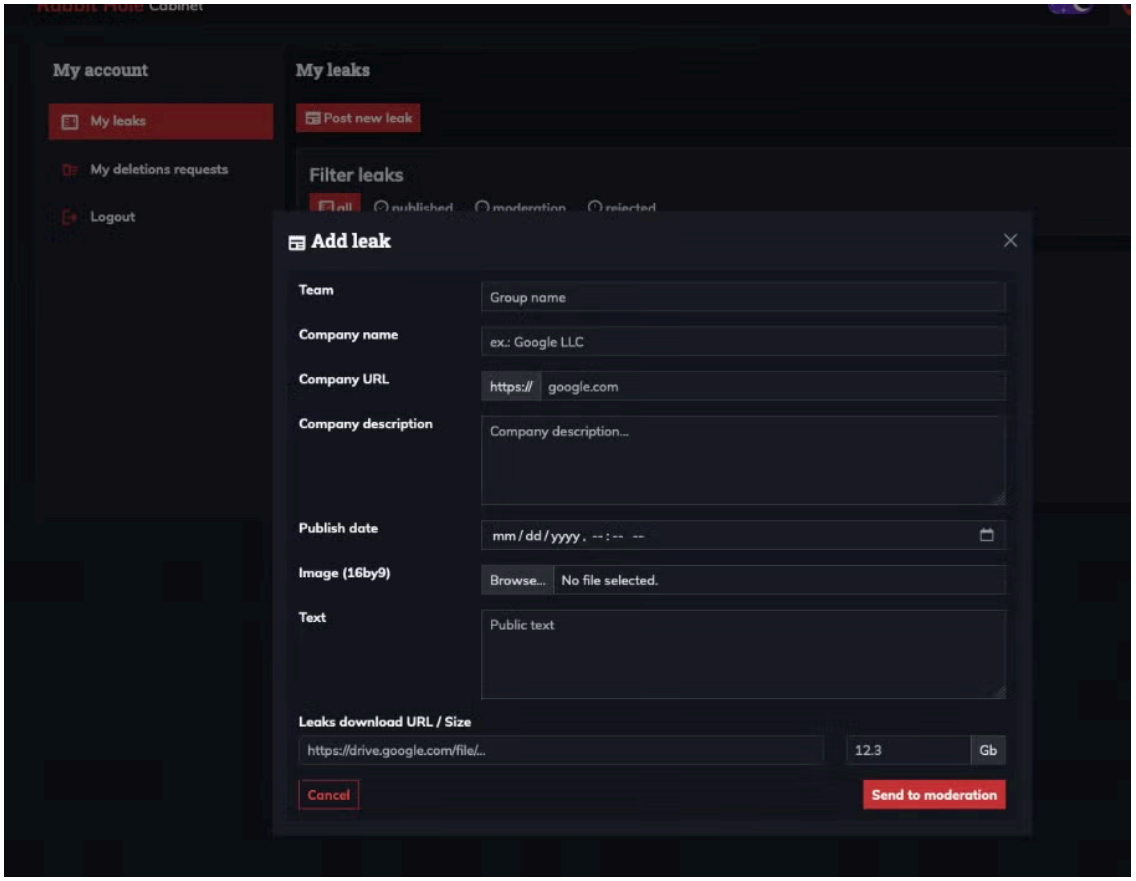
rabbit hole is not a ransom group, it is a general blog for small to medium sized teams. this blog was created in order to put pressure on corporations, due to the large number of publications from different teams – the rabbit hole offers you a haven where you can publish any leak [government institutions and hospitals are an exception]

Once a threat actor creates a Rabbit Hole account, victim leaks can be added, updated, and managed through its web portal. Each account manages their leaks through what is referred to as a ‘cabinet’ within the Rabbit Hole blog interface.



Rabbit Hole Blog Account “Cabinet”

When posting leak data, the user is able to supply information including who they are and who the victim is such as the name of the company, URL, company description, publish date/deadline, any associated images, and additional text to be included with the public leak description upon publication. The download URL for associated leaked data is also supplied via this interface.



New Leak creation on Rabbit Hole Blog

Once all details have been provided, they are submitted to higher level owners and managers of the Rabbit Hole blog. Moderators are then responsible for the ultimate public posting of the leak. The Rabbit Hole platform, ideal for emerging cybercriminals with little to no infrastructure or resources, could easily accommodate multiple small-time actors looking to monetize the same data leaks. We continue to monitor how this site develops.

Conclusion

As larger, established threat groups fold or re-brand, we can expect to see many affiliates cut out of pending payments. Since threat actors will hold onto exfiltrated data, the likelihood of that data being used to re-extort the victims is high and will continue to grow. While it may seem like common sense not to trust threat actors to hold up their end of a deal, the infosec community may continue to witness the fallout that happens when in-fighting and disagreements happen between cybercriminals as well as threat service providers and their affiliates.

The trust model upon which these RaaS agreements are created does not scale well, as most recently highlighted by security researchers monitoring the relationships between threat actors and affiliates in the ecosystem:

“Additionally, we saw a continuation of long-tailed data exfiltration defaults by threat actors in Q1, i.e., posting of information on a leak site after payment or “hostage trading” with other groups or individuals, which adds further evidence to the file on the lack of benefits to pay for suppressing a data leak or any confidence in a criminal actor keeping their word.”

As the ransomware and extortion landscape evolves, criminals will do what they need to do to protect their investments and paydays. Since affiliates carrying out a ransomware attack hold the actual data, they have the option to go elsewhere to monetize the data to collect payment. Organizations continue to be discouraged by global law enforcement agencies from paying ransoms when dealing with a cyberattack and to file a report with the IC3, contributing to greater cyber resilience to potential attacks.

Indicators

z5jixbfejdu5wtxd2baliu6hwzgcitlspnttr7c2eopl5ccfcjrhkqid[.]onion
ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion
h6tejafqdkdltppzj7q34enltmfnpxaf7cseslv6djgiukiii573xtid[.]onion

dispossessor[.]com/
dispossessor-cloud[.]com/
205[.]209.102[.]218

tox[:]CE742906B254399832E4ED6EC1DDA50D7942F9A4F3F0FE46C19E1737FF29EF67DDAF3AB87B44
tox[:]36712626ED19B307ECB3E971AFDFAA449607100383DBE4C064CCD5909355D908AECCF6180CDA

actor:DISPOSSESSOR
actor:plzdbmagain1037
actor:ViDoK
