Swindled Blackcat affiliate wants money from Change Healthcare ransom

By Menlo Labs

Published: 2024-03-06 · Archived: 2026-04-05 20:16:24 UTC

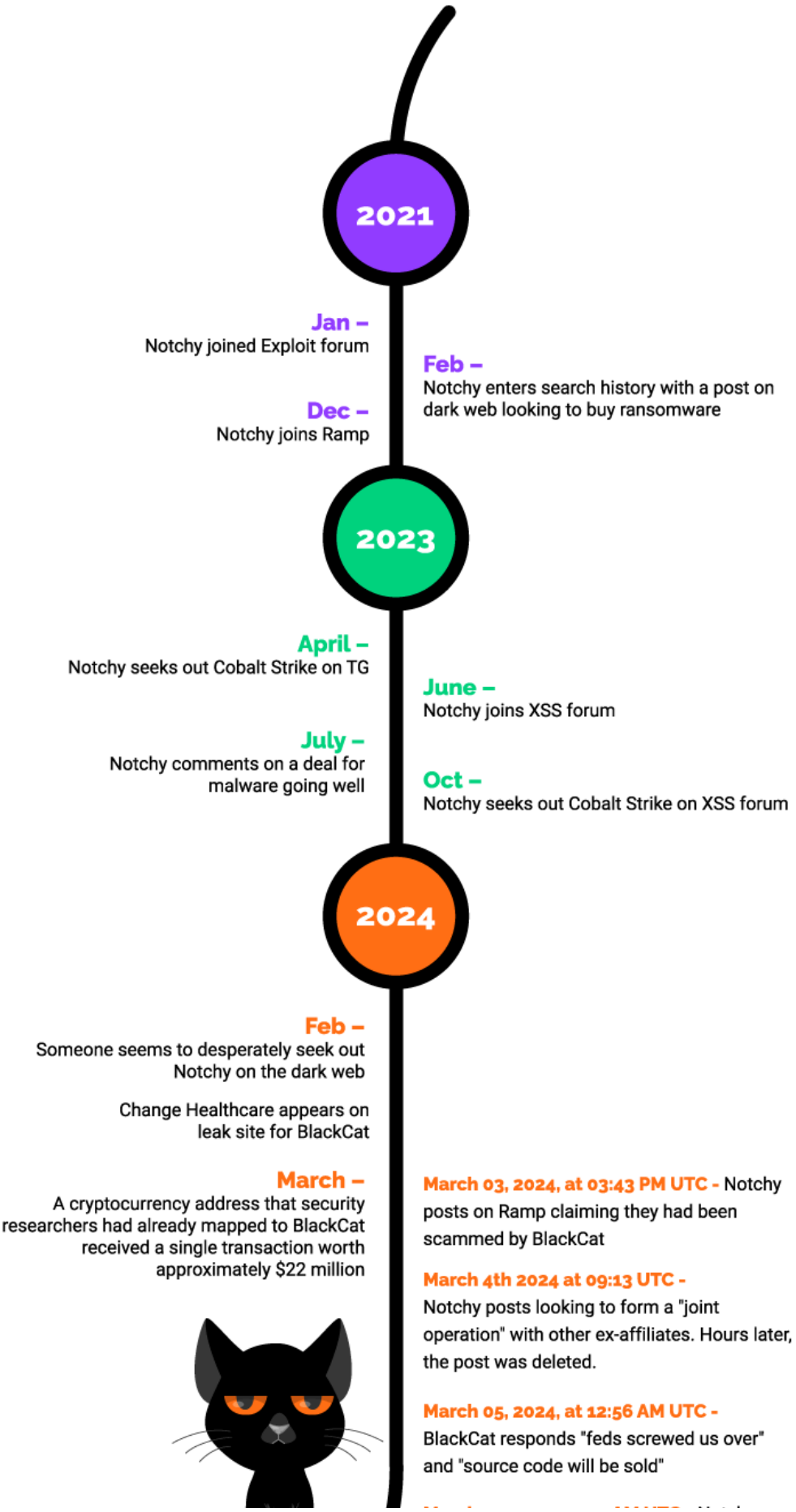
The U.S. healthcare giant, Change Healthcare, has reportedly made a $22 million ransom payment to the notorious BlackCat ransomware group (ALPHV). This payment comes as the company grapples with efforts to restore services following a cyberattack that has caused widespread disruptions to prescription drug services across the nation for several weeks.

Since then, the BlackCat (ALPHV) ransomware gang has shut down its servers, reportedly after allegedly scamming an affiliate involved in the Optum attack out of $22 million. The Tox messaging platform, used by the BlackCat ransomware operator, now displays a message in russian: “Все выключено, решаем,” meaning "Everything is off, we decide."

This move may be connected to claims made by an individual identifying themselves as a long-time ALPHV/BlackCat affiliate involved in the Optum attack. They allege that ALPHV suspended their affiliate account and fled with a $22 million ransom, supposedly paid by Optum for the Change Healthcare attack.

What we know

Timeline


2021
Jan –
Notchy joined Exploit forum
Dec –
Notchy joins Ramp
Feb –
Notchy enters search history with a post on dark web looking to buy ransomware
2023
April –
Notchy seeks out Cobalt Strike on TG
July –
Notchy comments on a deal for malware going well
June –
Notchy joins XSS forum
Oct –
Notchy seeks out Cobalt Strike on XSS forum
2024
Feb –
Someone seems to desperately seek out Notchy on the dark web
Change Healthcare appears on leak site for BlackCat
March –
A cryptocurrency address that security researchers had already mapped to BlackCat received a single transaction worth approximately $22 million
March 03, 2024, at 03:43 PM UTC - Notchy posts on Ramp claiming they had been scammed by BlackCat
March 4th 2024 at 09:13 UTC -
Notchy posts looking to form a "joint operation" with other ex-affiliates. Hours later, the post was deleted.
March 05, 2024, at 12:56 AM UTC -
BlackCat responds "feds screwed us over" and "source code will be sold"

March 05, 2024 03:32 AM UTC - Notchy responds to BlackCat telling them to give them their money.

Compromised American healthcare data

Reports from the Menlo Labs Threat Intelligence team suggest Change Healthcare's operations could affect the healthcare data of nearly every American. This is concerning given the vast amount of data involved - around 4TB of US citizens' data is reportedly held by a swindled ex-affiliate of ALPHV/BlackCat. The compromised information encompasses a wide array of personal and medical details, notably including data from critical national healthcare programs such as Medicare and TRICARE.

The leakage of such sensitive data not only poses a direct threat to the privacy and security of millions of beneficiaries, but also has broader implications for national security. Given the extensive and detailed nature of the information potentially accessed, this incident underscores the vital importance of enhancing cybersecurity measures around critical healthcare infrastructure and data systems.

While it's reasonable to assume their significant influence across the American healthcare landscape, claims of their total control over all Americans' healthcare data should be approached cautiously without solid evidence. Additionally, as of February 28th, 2024, Change Healthcare was still listed on the site.

The situation surrounding Change Healthcare has seen a significant shift, with the emerging BlackCat ransomware group scandal and suggestions of involvement by Chinese state-sponsored entities. However, these allegations of

Chinese state-sponsored associations lack validation, and we are closely monitoring developments. While it's plausible that the purported BlackCat affiliate is associated with a Chinese nation-state operation, arriving at a definitive conclusion necessitates substantial evidence from credible sources.

Analyst comment: *some of our HUMINT sources with direct contact to Notchy says it's high probability that Notchy is associated with China Nation-State groups.*

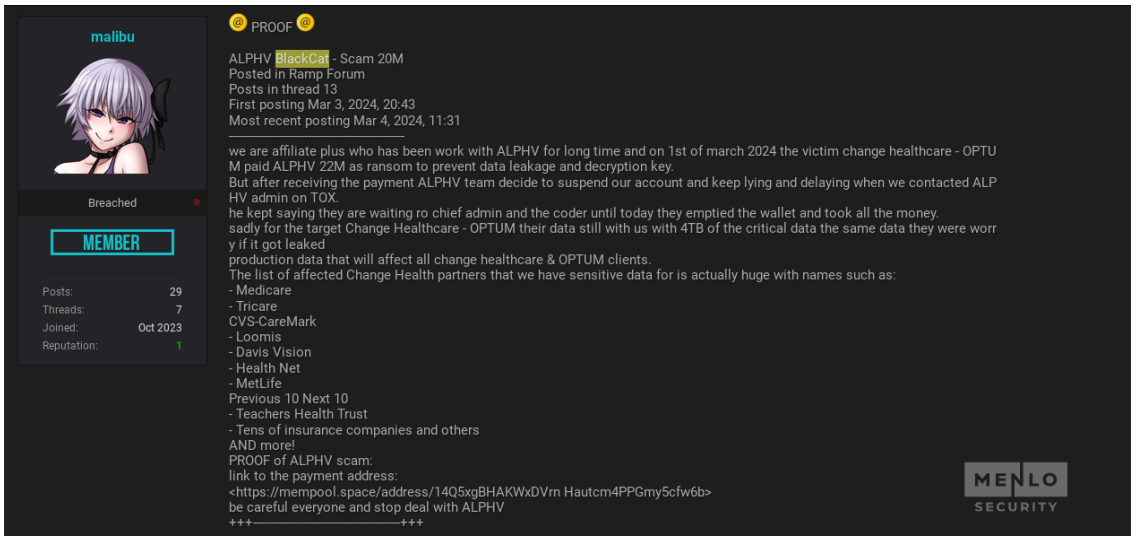
Many analysts in the community have commented on the unfolding story, suggesting, 'This appears to be a classic exit scam'. In such a scam, perpetrators feign operational shutdown, covertly misappropriate their collaborators' funds, and potentially re-emerge under a different guise. Our analysis aligns with this perspective, leading us to consider an exit scam is a highly probable explanation. Below, we present the evidence that underpins our conclusion, alongside potential implications for stakeholders and the broader cybersecurity ecosystem.

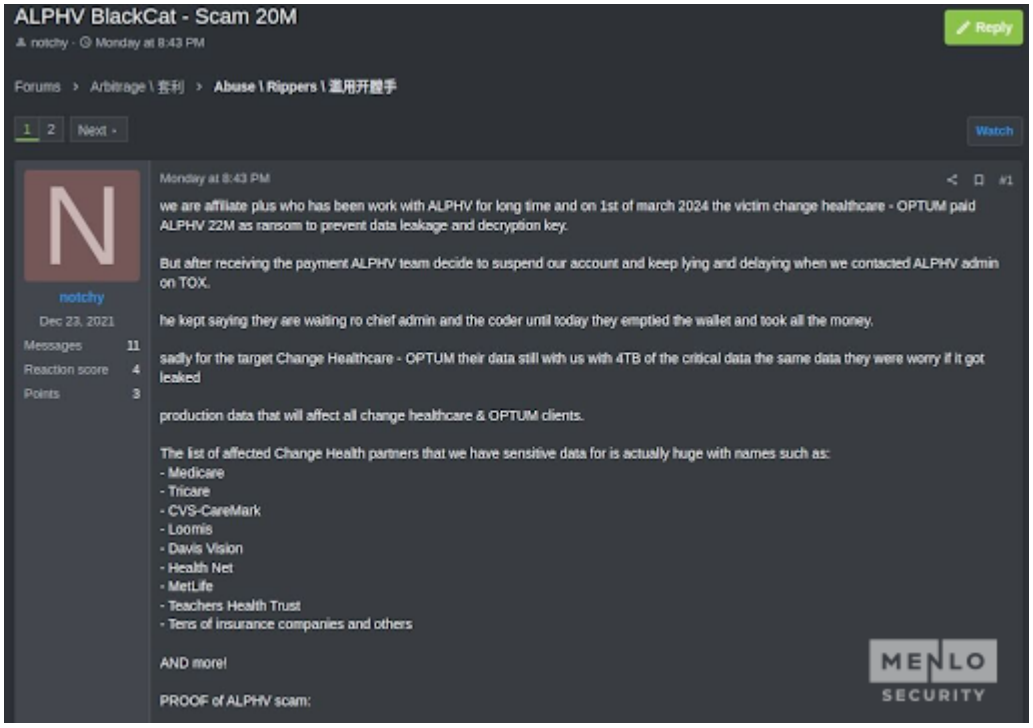
Notchy emerges on dark web forums

Analyst Comment: *Please be advised that the following analysis was conducted in a secure environment, employing industry-standard methodologies for data collection. Information had to be redacted and/or removed due to its sensitivity. We may be able to provide more information in a TLP Red environment.*

In light of numerous researchers referencing the above photo, we conducted a thorough analysis of discussions on Ramp—a dark web forum known for its entry barrier, either a $500 USD fee or admin approval—to glean insights into this thread. Below, we outline key takeaways from the forum discussions, emphasizing the parts that shed light on the evolving situation.

On March 03, 2024, at 03:43 PM UTC, a forum user identified as 'notchy' initiated a thread claiming to be the affiliate responsible for the ransomware attack on Change Healthcare. According to Notchy' despite the company's alleged payment of the ransom, they have not received their promised compensation.





Analyst Comment: *Ramp enforces a rule where individuals accused of fraud are given a chance to present their defense. This was exemplified in an administrative post tagging the user '@BlackCat46:*

"You have the opportunity to respond before I make a decision, provide your logs and your point of view on the problem. The defendant has not appeared on the forum since August 22 last year, if anyone has the opportunity, notify him through the contacts you know about this claim."

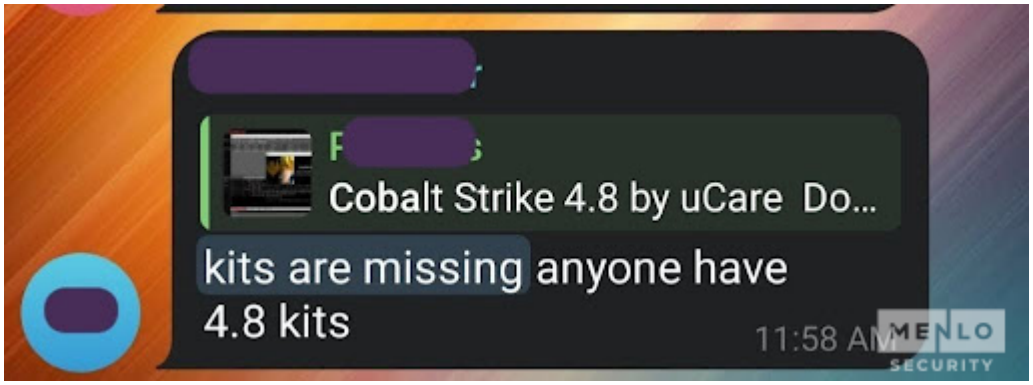
Subsequent observations in the thread, as of March 05, 2024, at 12:56 AM UTC, revealed activity possibly indicating the group's presence under an alternate name, "@ransom." This post, originally in Russian, is translated below:

"There is no point in making excuses, but we knew about the problem, tried to solve it, the advertiser was told to wait, we could now send our personal correspondence among ourselves, where we are shocked by what is happening and try to outbid transactions with a larger commission, but this makes no sense because we decided to completely close the project, we can officially declare that the feds screwed us over. The source code will be sold, negotiations are already underway on this matter. Thank you all for being with us. You can delete your account, I won't go to court again, we don't have other accounts on other forums, it's all fake."

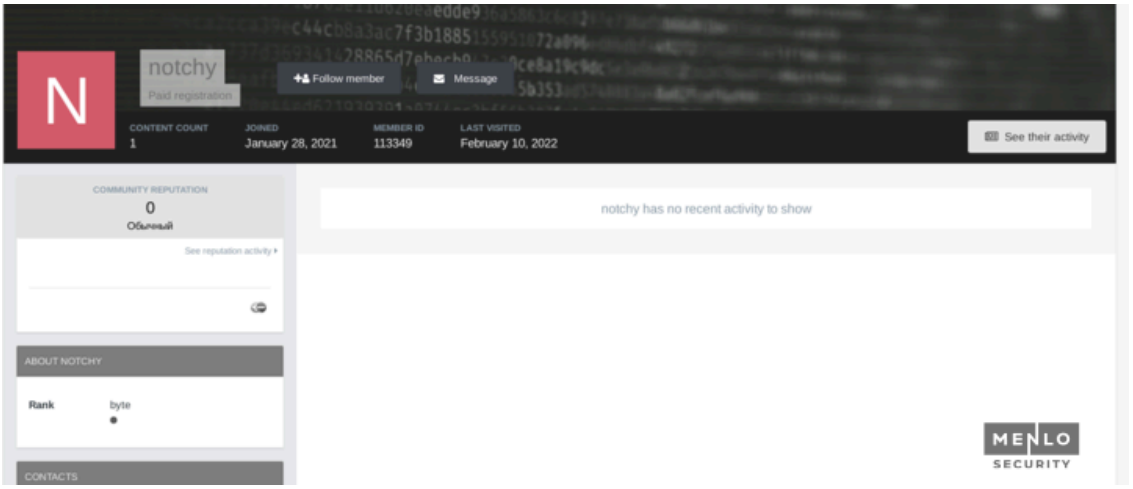
Notchy responded on March 05, 2024 03:32 AM UTC "@ransom stop blaming the feds. No one is idiot here to believe what you have said. return what you have stole and be a man with dignity"

Additionally, we found Notchy engaging on topics focused on ransomware as early as 2021 where he was looking to buy ransomware. On February 03, 2021 03:14 AM UTC he posted: "Looking for ransomware to buy or % basis I have multiple networks under my control (full domain + full access across managed swtiches & vlans) + multiple production servers hosting enterprise applications"

From the intelligence collected on Ramp we were able to get a Telegram username, and saw some messages from April of 2023 where Notchy was seeking out Cobalt Strike.

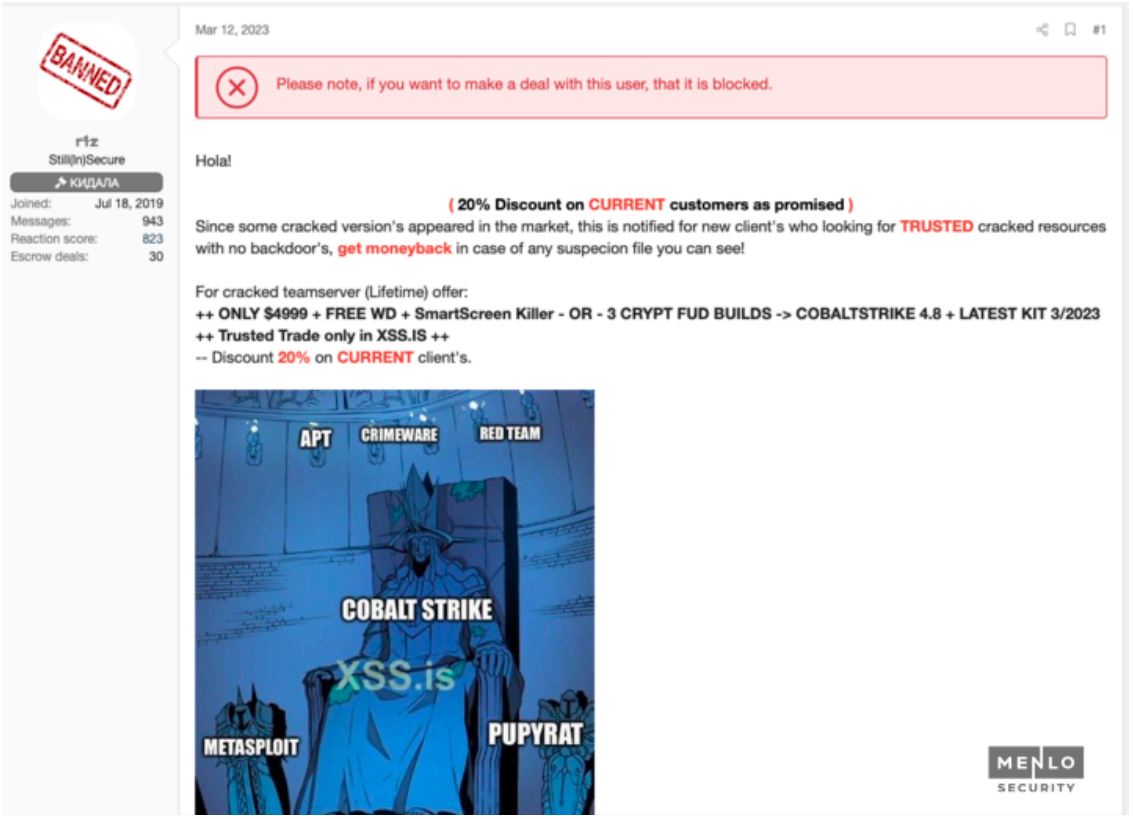


Further investigation reveals that the user Notchy is active not only on the Ramp forum but also on the Exploit forum, as evidenced by a screenshot provided.



Another interesting account with the username Notchy is an XSS Forum account. This is due to this account having commented on a post which sells malware. This comment was made on the October 10th stating “trusted seller and genuine products A+++”.

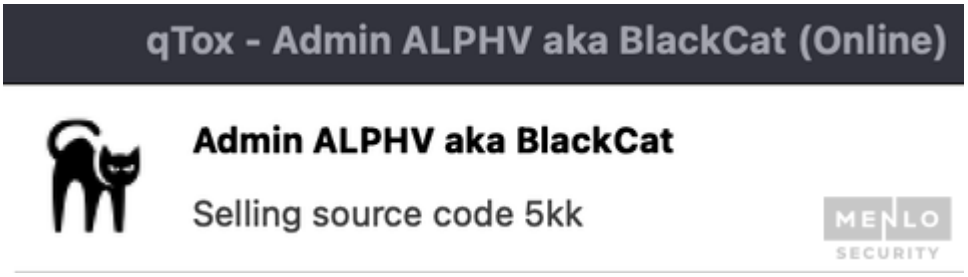
The malware purchased by Notchy reportedly includes SmartScreen Killer and the latest version of Cobalt Strike. We have also identified a potential hash associated with this malware purchase. Without more details on the Change Healthcare attack, we are unable to determine if this malware was used against them or not.



Nonetheless, this connection raises pertinent questions about the potential involvement of "notchy" in cyber activities beyond just the Ramp and Exploit forums.

Moving over to X (Twitter), we saw users talking about the exit scam that ALPHV/BlackCat are supposedly conducting . According to Fabian Wosar, “Since people continue to fall for the ALPHV/BlackCat cover up: ALPHV/BlackCat did not get seized. They are exit scamming their affiliates. It is blatantly obvious when you check the source code of the new takedown notice. You will see code like this”. The following picture was posted with the tweet.

Another X user shared this image purportedly showing BlackCat selling their source code. This information mirrors the initial discussions observed on the Ramp forum. This connection brings our investigation nearly full circle but also highlights the quickness-to-exit scene by disseminating and monetizing their tools possibly for the last time.



With the drama unfolding against the backdrop of Ramp's enigmatic forum discussions and the sagacious insights of observers, our story reaches a pause as we wait to see what will come in the near future. It's a powerful reminder that in the cyber world, where every shadow might hide a story and every byte could reveal a secret, uncertainty reigns supreme..

Next steps

The healthcare industry is urging the government to intervene and provide financial support to hospitals, particularly rural ones, to prevent them from running out of funds. Payment systems for hospitals and various health-related organizations have been severely impacted by the attack on Change, causing significant delays. Some hospitals are now at risk of running out of cash while awaiting a solution to the issue. Change Healthcare’s top priority will be to get its systems back online, while maintaining the data required for a thorough investigation, and the timeline would depend on many variables.

What Notchy will do and where the story goes is something we all will be watching. Notchy posted on March 4th 2024 at 09:13 UTC a request for others to join in a joint operation and then later had the post removed on Ramp. There is a risk that the ex-affiliate of ALPHV/BlackCat, who had his portion of the ransom money taken, may attempt to sell the stolen data privately on the darkweb to recoup what he lost. There is also the possibility we might see the release of BlackCat's internal data and intelligence leaked as a form of retaliation, coupled with the threat of double extortion. In such a scenario, they could still opt to release the data for free eventually.

Mitigating the fallout of the compromised information should be a top priority, as this is rumored to affect the majority of not only civilians but also federal and military personnel.
