Ransomwhere project wants to create a database of past ransomware payments

By Catalin Cimpanu

Published: 2022-12-12 · Archived: 2026-04-05 16:15:37 UTC

A new website launched this week wants to create a crowdfunded, free, and open database of past ransomware payments in the hopes of expanding visibility into the broader picture of the ransomware ecosystem.

Named Ransomwhere, the new portal is the personal project of Jack Cable, a Stanford University student and a security researcher for the Krebs Stamos Group.

The website allows victims of ransomware attacks or cybersecurity professionals to submit a copy of a ransom note, along with the size of the ransom demand and the Bitcoin address where victims made the payment, which would then be indexed in a public database.

This database, void of any personal or victim-identifying information, would be made available as a free download for the cybersecurity community and law enforcement officials via the Ransomwhere site.

Improving cybersecurity research into a known blind spot

The idea behind the site is to create a central system that tracks payments sent to ransomware gangs in order to more accurately estimate the size and profits of their operations, about which very little is known.

"I was inspired by Katie Nickels's tweet that no one really knows the full impact of cybercrime, and especially ransomware," Cable told *The Record* in an interview on Thursday.

"After seeing that there's currently no single place for public data on ransomware payments, and given that it's not hard to track bitcoin transactions, I started hacking it together."

> Seriously, though, I think this is a huge part of the problem, especially around the ransomware ecosystem, but for cybercrime in general. No one knows the real impact, so it's hard to know if actions change that impact or not.
>
> — Katie Nickels (@likethecoins) June 8, 2021

The project is only one day old but has already captivated the infosec community, which has been having problems tracking ransomware payments since most security firms don't collaborate or don't share this kind of information publicly or even privately with each other.

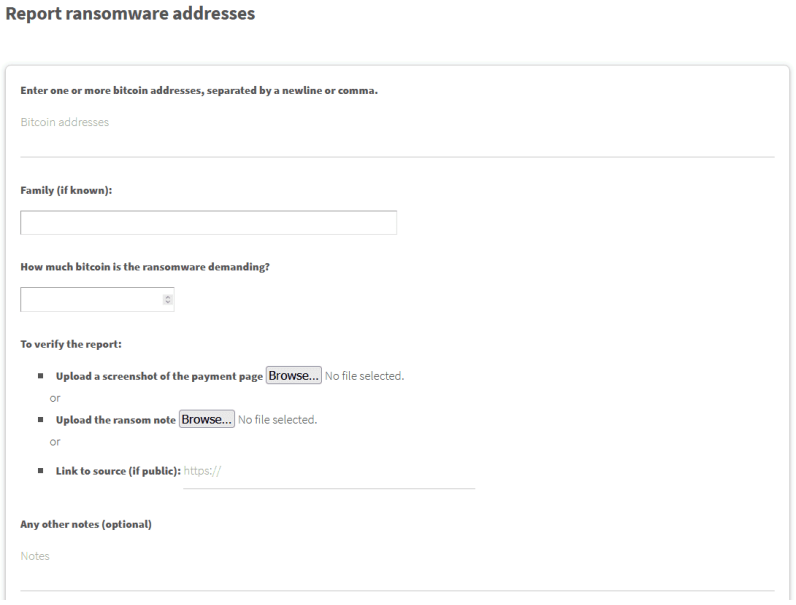
Having ransomware payment data shared anonymously and via a third-party service like Ransomwhere removes some of the barriers in the cybersecurity community, such as non-disclosure agreements and business rivalries.

But for the time being, Cable is relying on public submissions to expand the site's database. However, the researcher told *The Record* that he is also exploring "ways of partnering with companies in the security or blockchain analysis space to integrate data that they may already have on ransomware actors" and expand Ransomwhere with data that is currently not public or disclosed by the victims directly.

Bitcoin analysis firms such as Chainalysis, and some security vendors, have worked in the past to gather Bitcoin addresses seen in malware samples and ransom notes and then detect if any payments have been made to those addresses. This is how some companies have been able to estimate the earnings of several ransomware gangs, such as:

- Maze/Egregor: $75 million
- Ryuk: $150 million
- REvil: $123 million
- Netwalker: $25 million

However, this kind of in-depth research has only been carried out for the larger ransomware cartels, and there are still blind spots when it comes to estimating the size of other ransomware operations, a place where data collected via Ransomwhere might help.



Running a site like Ransomwhere also comes with its disadvantages. One of them being that its database can be easily polluted via tainted or fake submissions.

To counter this, Cable said he plans to vet all submissions.

"For now, it's just myself vetting reports," the researcher told *The Record*. "At some point, I may add a voting system for individuals to help out flagging reports that might be fake."

Additionally, Cable is also urging malware researchers to contact him directly and have data added to the database as a trusted source.

"I'm active on various Slack groups and can be reached via Twitter or email. As long as researchers can share bitcoin addresses and the ransomware family, I can add it," Cable said.

ID-Ransomware collaboration

Right now, the launch of the Ransomwhere project is eerily similar to when Michael Gillespie launched ID-Ransomware in early 2016 as a simple site where victims could upload their ransom note, and the site would tell them the name of the ransomware family that encrypted their data and where they could find help in recovering files.

ID-Ransomware provided a never-before-seen feature to ransomware victims and the cybersecurity community, and the site has become a go-to tool for many incident responders.

Because the site is so popular with the cybersecurity community, a collaboration between the two would be more than ideal, for both Cable and the cybersecurity industry, as a whole.

"I've been talking with Michael and am a big fan of his work," Cable said. "We're discussing ways of integration, both to collect bitcoin addresses from IDR, as well as providing more information to IDR users based on Ransomwhere's data."

But this is not the only way Ransomwhere could grow, the researcher told us.

"It could also be interesting to explore tracking downstream bitcoin addresses -- e.g. once the criminals receive a payment, where do they go? As the project goes on, I may explore doing it myself or partnering with firms that specialize in this," he said.

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
