There's a Clear Line From the REvil Ransomware to Russia

By Jeremy Kirk

Archived: 2026-04-05 16:17:00 UTC

Fraud Management & Cybercrime , Next-Generation Technologies & Secure Development , Ransomware

Two Companies Have REvil Data; They Don't Appear Eager to Help (jeremy_kirk) • July 13, 2021

A screenshot of a negotiating portal set up by the REvil ransomware group (Source: SecurityScorecard)

Threat intelligence researchers are looking closely at REvil, the ransomware gang that infected up to 1,500 companies in a single swoop. A look at part of the group's online infrastructure shows clear lines to Russian and U.K. service providers that, in theory, could help law enforcement agencies but don't appear eager to help.

See Also: Gen AI Stalls, Shadow AI Rises: A CISO Concern

On July 2, affiliates of REvil exploited several vulnerabilities in remote management software called the Virtual System Administrator from Miami-based Kaseya.

The vulnerabilities, combined with a series of clever maneuvers, allowed REvil to distribute ransomware to up to 60 Kaseya customers, which are mostly managed service providers. Once on those MSPs' systems, REvil used VSA to push ransomware down to many of their customers, which included small businesses and municipalities (see: *Kaseya: Up to 1,500 Organizations Hit in Ransomware Attack*).

The damage may not be as bad it could be, as the attackers didn't delete Volume Shadow Copy, a Windows backup feature. One MSP in the Netherlands, VelzArt, reported on its blog of successful efforts to restore its customers' systems, albeit with very long days on the job.

Still, some infected organizations have been negotiating ransom payments with REvil via the group's web-based customer service portals. And one of those portals has been left with fewer protections, which, in theory, could help law enforcement agencies.

Ransom Chat Portal

To start the ransom payment process, a victim goes to a website with their assigned user ID. Then, the victim enters a private key found in their ransom note, which brings up a chat dialog, the ransom amount being demanded and the time left before the ransom amount rises due to nonpayment.

REvil typically creates those customer service sites using the anonymity system Tor, which is short for The Onion Router. With Tor, it's possible to set up a "hidden" website that masks the normal technical information. It's nearly impossible to figure out where a hidden site is actually hosted.

But REvil has also set up a regular website, decoder[dot]re, for negotiations in case Tor is blocked in a particular country. That site, which is hosted in Russia, has been included in ransom notes found in REvil ransomware victims since at least January, says Gene Yoo, chief executive officer of Los Angeles-based Resecurity, which investigates cybercrime and data breaches.

"It is obvious that the Russian government can’t not be aware about this malicious activity," Yoo says. "These details add clear connections between REvil and Russia. Hopefully, it will be properly investigated to contain this malicious activity damaging the business of thousands of companies globally."

After meeting with President Joe Biden in mid-June, Russian President Vladimir Putin dismissed accusations that Russia's IP space was the source of major cyberattacks.

"It is not a valid technical comment," says Alex Holden, CTO of Hold Security, a Wisconsin-based threat intelligence company. "Here we see another example of crime emanating from Russia."

Clearnet Mirror

Because it's on the clearnet, Resecurity as well as other researchers have been looking into decoder[dot]re's network addresses and DNS records, which reveal several touch points that investigators could query.

> You have two ways:
>
> 1) [Recommended] Using a TOR browser!
> a) Download and install TOR browser from this site: https://torproject.org/
> b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/64F9D9A943E5E574
>
> 2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
> a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
> b) Open our secondary website: http://decoder.re/64F9D9A943E5E574
>
> Warning: secondary website can be blocked, thats why first variant much better and more available.
>
> When you open our website, put the following data in the input form:
> Key:

The REvil gang gives instructions to victims on how to pay a ransom by visiting a negotiation site that is either a Tor hidden service or a regular website, decoder[dot]re. (Source: Resecurity)

Of course, domain name registration information can be faked and hosting can be purchased anonymously. But at the same time, threat actors have been known to make glaring operational security mistakes. And even a slip-up in something as minor as reusing an email address can unravel an online mystery, as the investigation into the Silk Road online market showed.

Decoder[dot]re appears to have been purchased on Dec. 18, 2020, from TLD Registrar Solutions, which is based in the U.K., according to RiskIQ's Reputation Lookup database.

Passive DNS records show the domain has been hosted since January by a Russian IT services company called JCS IOT, which develops internet of things solutions and offers cloud hosting services, virtualization and dedicated servers. JCS IOT also seems to be the parent IoT solutions company for a Russian hosting provider called FirstVDS. The two companies have the same legal entity as an owner and the same contact address.

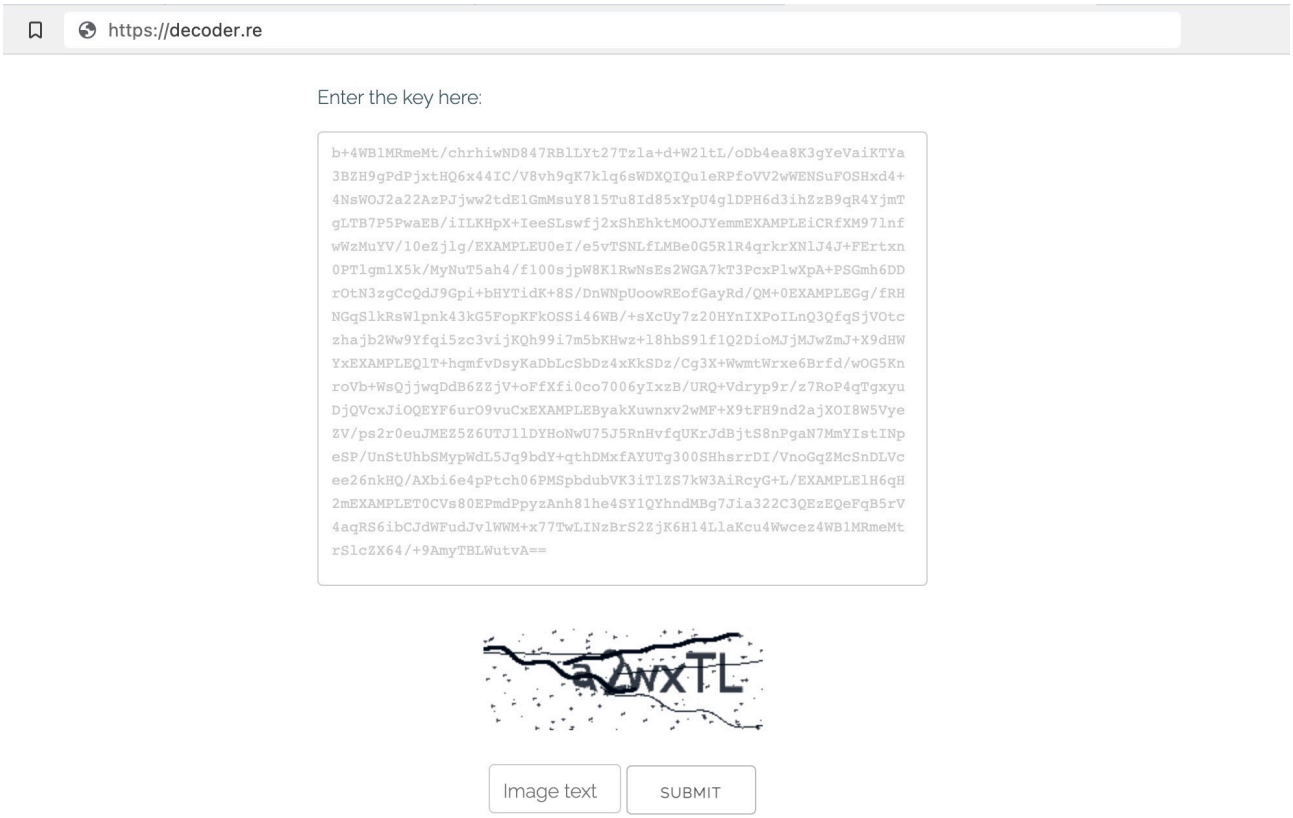
The primary DNS record resolves to 82[.]146.34.4, which is an IP hosted in Russia that has been linked to various other REvil operations, writes Ryan Sherstobitoff, vice president of cyberthreat research and intelligence at SecurityScorecard, a New York-based cybersecurity company.

Sherstobitoff tells me the cybercriminals behind the server have invariably used fake names. But there could be interesting information on the server, such as victims that the attackers have communicated with and possibly a Jabber server they use for their own chats, he says.

"We're also looking at where these guys actually operate," Sherstobitoff says. "These investigations are difficult for sure."

In the past couple of years, REvil has used other clearnet domains as secondary channels for its negotiating portals, including decoder[dot]cc and decryptor[dot]top. Those domains, however, are no longer active, and it appears decoder[dot]re is the replacement.

Decoder[dot]re is definitely affiliated with REvil, as it is a precise mirror of the Tor hidden portals used for negotiations, Yoo says. Using available ransomware samples and information collected from the victims, it's possible to log into victims' negotiation pages. Entering a message in the chat on decoder[dot]re can then be seen when logging into the same victim's chat window via one of REvil's Tor hidden negotiating portals.



A ransomware victim logs into decoder[dot]re using a user ID plus a private key that has been supplied in the ransom note.

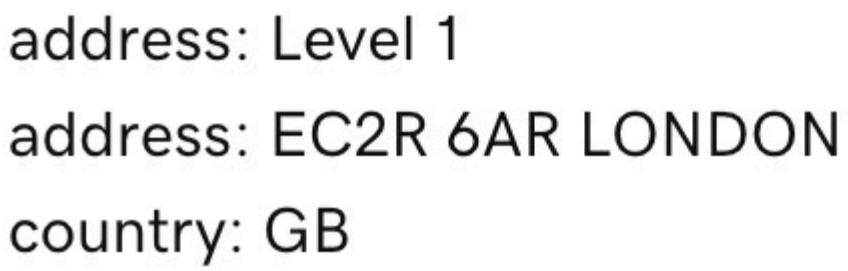
JCS IOT has an email address dedicated for accepting abuse complaints. I emailed that address along with others affiliated with the company and the associated company, FirstVDS. But I have received no replies to the emails I sent in Russian and English.

Registrar Responds

But TLD Registrar Solutions, which sold the domain name registration, did respond. It immediately became clear, however, that the company isn't in a hurry to revoke the registration.

The response to my email came from Lexie Kluss, who is on the support team of another domain name registrar, registered in the Bahamas, called Internet.bs.

domain: decoder.re
status: ACTIVE
hold: NO
holder-c: ANO00-FRNIC
admin-c: ANO00-FRNIC
tech-c: DA55158-FRNIC
zone-c: NFC1-FRNIC
nsl-id: NSL539493-FRNIC
registrar: TLD Registrar Solutions Ltd
Expiry Date: 2021-12-18T18:41:09Z
created: 2020-12-18T18:41:09Z
last-update: 2021-03-08T14:50:11Z
source: FRNIC
ns-list: NSL539493-FRNIC
nserver: ns1.goprodns.top
nserver: ns2.goprodns.top
source: FRNIC
registrar: TLD Registrar Solutions Ltd
type: Isp Option 1
address: 35-39 Moorgate



Part of the site's Whois data

According to Internet.bs' terms and conditions, TLD Registrar Solutions Ltd. is its parent company. TLD is listed as an accredited entity with the Internet Assigned Numbers Authority, the organization that oversees internet addressing and protocol issues.

Internet.bs has popped up before as a registrar of interest. Near the peak of the rogue pharmaceutical spam problems in 2012, Internet.bs was the registrar for nearly a third of thousands of rogue online pharmacies, according to this piece by computer security journalist Brian Krebs.

To add another complicating layer, Internet.bs has been owned since 2014 by the CentralNic Group PLC, which is listed on the London Stock Exchange. Tim Tsoriev, head of corporate communications for CentralNic, writes via email that "we are in contact with law enforcement, but we can't comment on active investigations."

Kluss writes that an investigation found it could take no action, that Internet.bs does not host the content, which is indeed true, and that the issue should be taken up with decoder[dot]re's hosting provider.

Incredibly, Kluss also writes that the company would comply with a law enforcement order for revoking the registration, but that "we feel that this type of request is a temporary resolution and not reflective in value of the risk associated with the act of interrupting the DNS for us as a registrar. By registering another domain with another registrar, any registrant can reinstate their content within a matter of minutes."

Kluss continued: "Due to the time and cost to Internet.bs to review all of the legal issues, we respectfully ask that you provide evidence to show that you have attempted to address these issues with the above-mentioned hosting providers without result before we re-investigate what actions, if any, we are able to take."

To paraphrase: Whomever is running the site will just go to another registrar, so why bother?

What's further interesting is that the statement supplied to me appears to be boilerplate used before by the company. Internet.bs provided a similar kind of statement to Slate in 2017 when the publication was enquiring about the registrar's role with BlackMattersUS[.]com. That website was believed to have been created by the Internet Research Agency, the notorious Russian content farm. The U.S. Justice Department alleged in a 2018 indictment the organization interfered with the 2016 presidential election.

Take It Offline?

Taking decoder[dot]re offline would raise an issue.

The portal is likely being used by organizations to communicate with their attackers. Although whether to pay ransoms is a contentious point of debate, it wouldn't help to make it more difficult for organizations already struggling with an infection to not have all options available, including paying for a decryption tool if it comes down to that.

The U.K. registrar should be easy for law enforcement officials to query. The Russian hosting company, JCS IOT, is obviously harder to probe. As Sherstobitoff says, those involved in the attack are using Russia as a safe haven.

The U.S. is pressing Russia for more cooperation in cracking down on ransomware criminals the U.S. alleges the country harbors. Pulling the threads around the decoder[dot]re domain might be a good place for the two countries to start cooperating in earnest - at least in theory.
