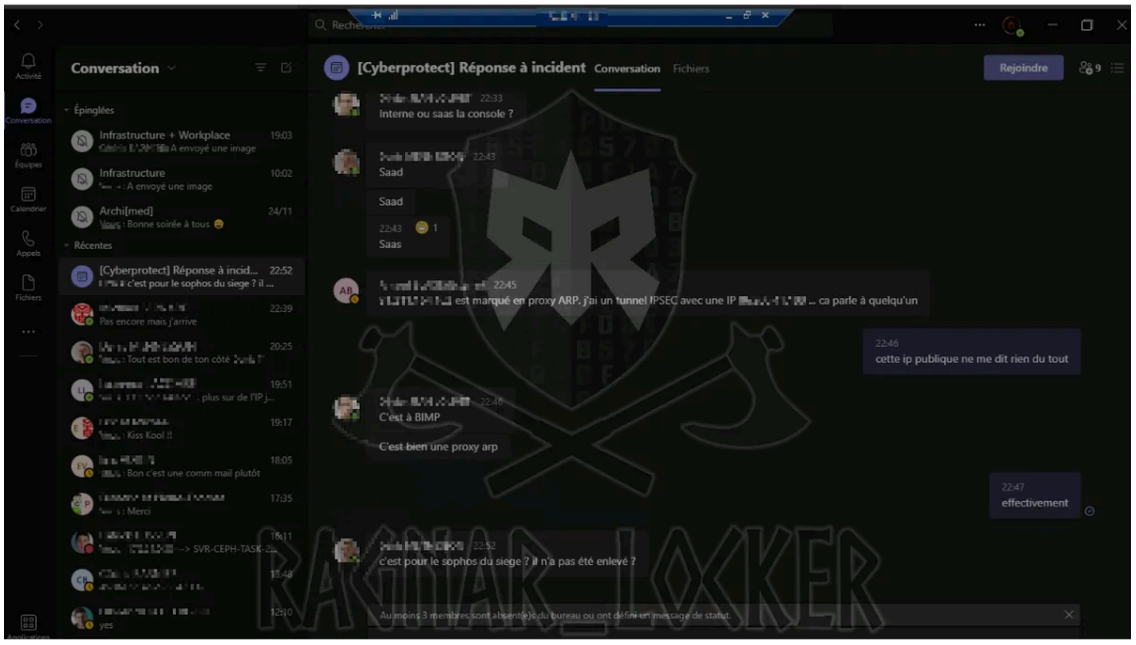
Ragnar Locker reminds breach victims it can read the on-network incident response chat rooms

By Joe Uchill

Published: 2021-12-03 · Archived: 2026-04-05 23:21:49 UTC



Redacted version of Ragnar Locker's screen capture, including watermark added by Ragnar Locker. Potentially identifying details about the victims or attack have been removed.

On Thursday, the Ragnar Locker ransomware group published the first batch of files stolen from a French computer and electric goods store it had victimized. Along with the archives were a series of screenshots taken while on the victim's network, including one from inside an incident response chat.

Ragnar Locker had been monitoring their victims as they discussed how to respond.

It is common for security teams to forget that chats and email accounts that live on breached networks will no longer be secure, a variety of breach responders, negotiators, and preparation consultants told SC Media.

"What I've found is that a lot of times in playbooks communications are addressed mostly as from a standpoint of when to address whom within the organization or externally. It's not as much about the integrity of those communications," said Trevin Edgeworth, director of Bishop Fox's red team practice.

There is an easy fix: during crisis planning, prepare out-of-band communications, anything from dedicated crisis consumer email accounts to secure chat apps.

Forgetting that, they say, has made many breaches worse.

"We've seen before where the attacker intercepted an Excel spreadsheet with the containment and eradication strategy," said David Wong, vice president of Mandiant Consulting. "So after we said that on Saturday at midnight, we're gonna reset those accounts, we're gonna block their IPs, we're gonna shut down the systems, Friday night, right before we're about to do what we're gonna do, they create backdoors elsewhere in their network from different infrastructure."

It is not just a matter of making breaches more persistent. During ransomware attacks, ransomware actors can catch victims discussing bringing in negotiators or police against the demands of a ransom note, or overhear strategic discussions of pricing. "You don't want them to hear you say, 'We can afford $10 million. We think we can get them down to $2 million if we offer them $500,000," said Wong.

Setting up out-of-band communications in advance is key to having them available in an emergency. Setting up a new communications system adds another wrinkle to the chaos around a breach, especially since you cannot use communications systems that may have been breached to coordinate moving to that new system.

Personal email accounts may not be a reasonable option for out-of-band contact. While the actors behind a breach might not have access to them, if someone sues the company over a breach, those accounts may be open to a subpoena, noted Wong.

In the end, communications is one of a number of oft-overlooked services an enterprise may rely on to handle a breach that could be disrupted during a breach.

"What companies don't realize is how short a path it is from domain compromise to doing other damage," said Edgeworth. "Gaining complete control of a domain is to having access to the most sensitive areas of your organization, be that your messaging and communications, or your customer data repositories, or your data backups. It's all coming off of that domain compromised."

Get essential knowledge and practical strategies to protect your organization from ransomware attacks.
