REvil ransomware - what you need to know | Tripwire

By Graham Cluley

Published: 2021-04-22 · Archived: 2026-04-06 03:19:53 UTC

What is REvil?

REvil is an ambitious criminal ransomware-as-a-service (RAAS) enterprise that first came to prominence in April 2019, following the demise of another ransomware gang GandCrab.

The REvil group is also known sometimes by other names such as Sodin and Sodinokibi.

There's been plenty of ransomware before. What makes REvil so special?

REvil has gained a reputation for attempting to extort far larger payments from its corporate victims than that typically seen in other attacks. It is actively promoted underground cybercrime forums as the best choice for attacking business networks where there is more money to be made than infecting the computers of home users.

Aside from the many high profile companies and organisations who have fallen foul of REvil, it is stealing data from the computers and networks of its victims before they are encrypted. This is a technique of applying additional pressure on victims which is becoming more and more commonplace.

REvil threatens to release stolen data, by auctioning it off on its website (anachronistically called the "Happy Blog") if ransom demands are not met.

The "Happy Blog" lists recent victims of REvil, attaching a sample of the stolen data as proof that information has been exfiltrated from an organisation. The REvil gang even offers a "trial" decryption to prove to the victim that their files can be decrypted.

A countdown timer indicates when data leaks will be made public, applying more pressure to companies debating how they should respond.

> Hello - some of your files containing confidential information have been downloaded and are located on our servers. If you refuse to negotiate with us, all documents will be published on the blog and published by the media. If an agreement is reached, the data will be permanently deleted. We advise you to quickly contact us through the support chat.

Nasty. So simply restoring from a backup..?

…is not going to be enough. Yes, restoring your data from a secure, clean backup can help a company get back up and running again (if the backup hasn't itself been compromised, of course), but criminals still have a copy of your company's data.

Even if they are unsuccessful in selling your data to others in cybercrime forums, incalculable damage can be done to an organisation's brand and business relationships.

You said that REvil was Ransomware-as-a-service. What's that?

As online crime became more sophisticated, some malicious actors recognised that rather than spending all their time launching their own attacks they could actually lease out their expertise and infrastructure to other criminals - giving even those without technical ability a means to profit from ransomware.

Like software-as-a-service (SAAS)?

Precisely. Ransomware gangs have been known to offer 24/7 technical support, subscriptions, affiliate schemes, and online forums just like legitimate online companies. They know that offering a quality service to their (admittedly) criminally-minded clients will help both sides of the venture to become rich at the victim's expense.

But if an attacker is paying for a ransomware service from another criminal, can't they be tracked and identified?

Payments are typically made through cryptocurrency, keeping transactions anonymous.

Of course. How much money is the REvil enterprise making?

It's hard to be certain because it's not as though they're filing their accounts, but when interviewed the group's developers have claimed to be making more than US $100 million per year.

The developers of REvil are thought to pocket between 20-30% of the money extorted from victims of their ransomware, with the affiliate who ran the operation with the assistance of REvil's expertise and infrastructure receiving the rest.

How does the REvil ransomware infect an organisation in the first place?

There are a variety of methods an attacker could use to plant the malware. These include exploiting a vulnerability to gain access to a computer on your company's network, spear-phishing, or exploiting a third-party business partner.

In some cases, the attack may actually come from a client or partner who has already fallen victim to the hackers.

So what should my company be doing to protect ourselves from the REvil ransomware?

It's the same advice as with other ransomware.

You should still be making secure offsite backups. You should still be running up-to-date security solutions and ensuring that your computers are protected with the latest patches against newly-discovered vulnerabilities. You should still be using hard-to-crack, unique passwords to protect sensitive data and accounts as well as enabling multi-factor authentication. You should still be encrypting your sensitive data wherever possible. You should still

be educating and informing staff about risks and the methods used by cybercriminals to electronically infiltrate organizations.

If my company has been unlucky enough to have been hit by the REvil ransomware, should we pay the ransom?

That ultimately is a decision that only you can make. Bear in mind that the more companies that pay a ransom, the more likely it is that criminals will launch similar attacks in the future.

At the same time, you may feel that your business needs to make the difficult but pragmatic decision to pay the criminals if you feel your company cannot survive any other way.

Whatever your decision, you should inform law enforcement agencies of the incident and work with them to help them investigate who might be behind the attacks.

And remember this: paying the ransom does not necessarily mean you have erased the security problems that allowed you to be infected in the first place. If you don't find out what went wrong and why and fix it, then you could easily fall victim to further cybercrime attacks in the future.

Editor's Note: *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*
