Ransomware gang plans to call victim's business partners about attacks

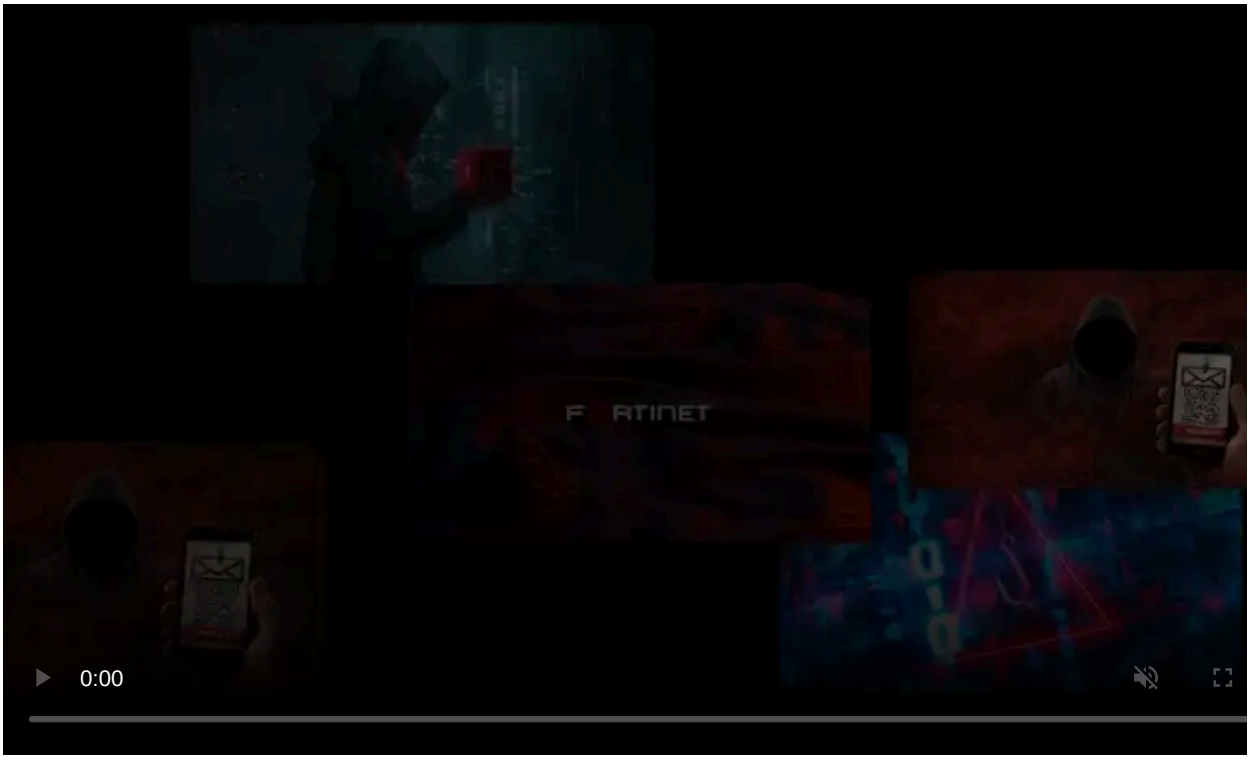
By Lawrence Abrams

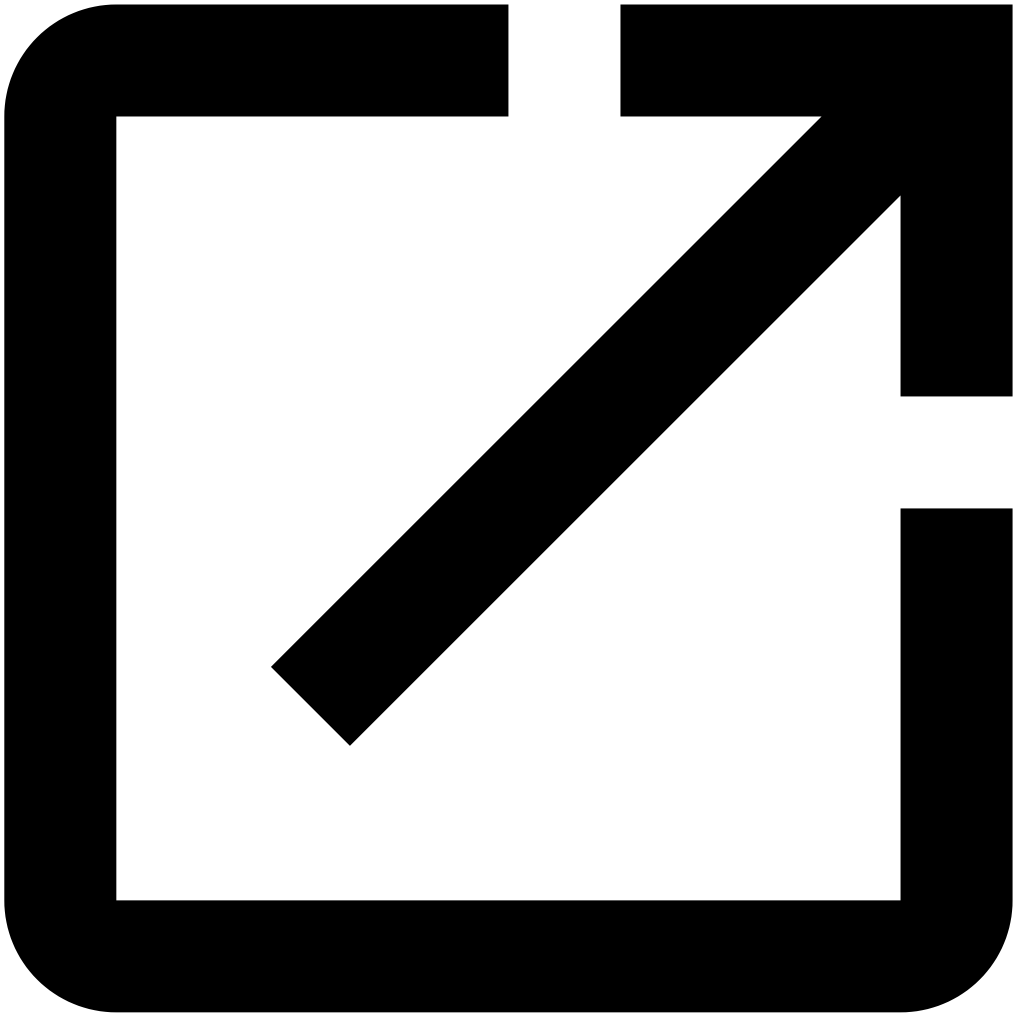
Published: 2021-03-06 · Archived: 2026-04-06 00:02:40 UTC

The REvil ransomware operation announced this week that they are using DDoS attacks and voice calls to journalists and victim's business partners to generate ransom payments.

The REvil ransomware operation, also known as Sodinokibi, is a ransomware-as-a-service (RaaS) where the ransomware operators develop the malware and payment site, and affiliates (adverts) compromise corporate networks to deploy the ransomware.

As part of this deal, the REvil developers earn between 20-30% of ransom payments, and the affiliates make the remaining 70-80%.


F RTINET
0:00



To pressure victims into paying a ransom, ransomware gangs have increasingly turned to a double-extortion tactic, where attackers steal unencrypted files that they threaten to release if a ransom is not paid.

Now using VOIP calls and DDoS attacks

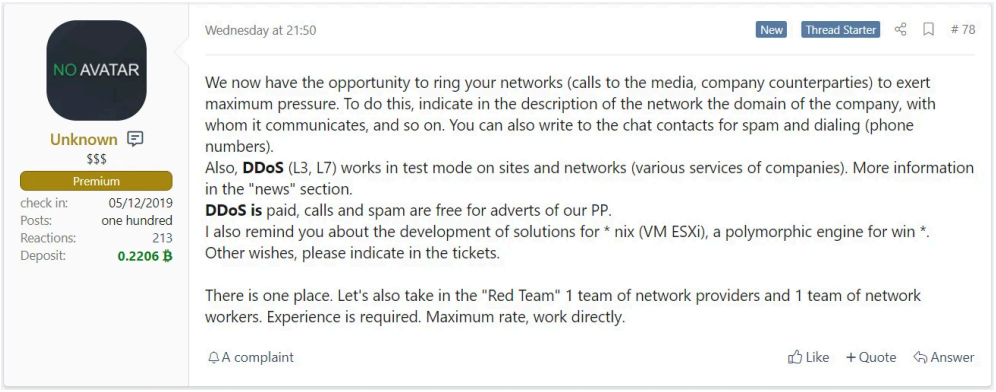
In February, the REvil ransomware operation posted a job notice where they were looking to recruit people to perform DDoS attacks and use VOIP calls to contact victims and their partners.

Today, a security researcher known as 3xp0rt discovered that REvil has announced that they were introducing new tactics that affiliates can use to exert even more pressure on victims.

These new tactics include a free service where the threat actors, or affiliated partners, will perform voice-scrambled VOIP calls to the media and victim's business partners with information about the attack.

The ransomware gang is likely assuming that warning businesses that their data may have been exposed in an attack on of their partners, will create further pressure for the victim to pay.

REvil is also providing a paid service that allows affiliates to perform Layer 3 and Layer 7 DDoS attacks against a company for maximum pressure.

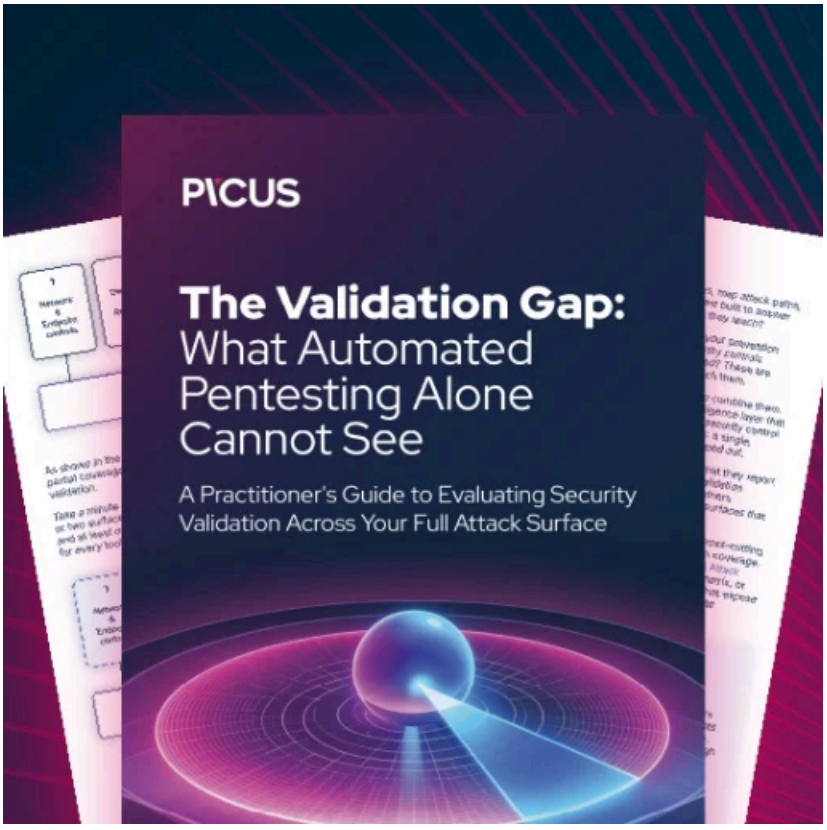


Forum post announcing new REvil extortion features

A Layer 3 attack is commonly used to take down the company's Internet connection. In contrast, threat actors would use a Layer 7 attack to take down a publicly accessible application, such as a web server.

In October, we reported that the SunCrypt and Ragnar Locker ransomware operations had begun to use DDoS attacks against victims to pressure them to pay. In January 2021, the Avaddon ransomware gang began using this tactic as well, so it is not surprising to see other operations begin utilizing these attacks as well.

While VOIP calls to victims to exert pressure have been used by numerous ransomware operations, BleepingComputer is not aware of calls made to journalists or victim's business partners.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/ransomware-gang-plans-to-call-victims-business-partners-about-attacks/