REvil ransomware deposits $1 million in hacker recruitment drive

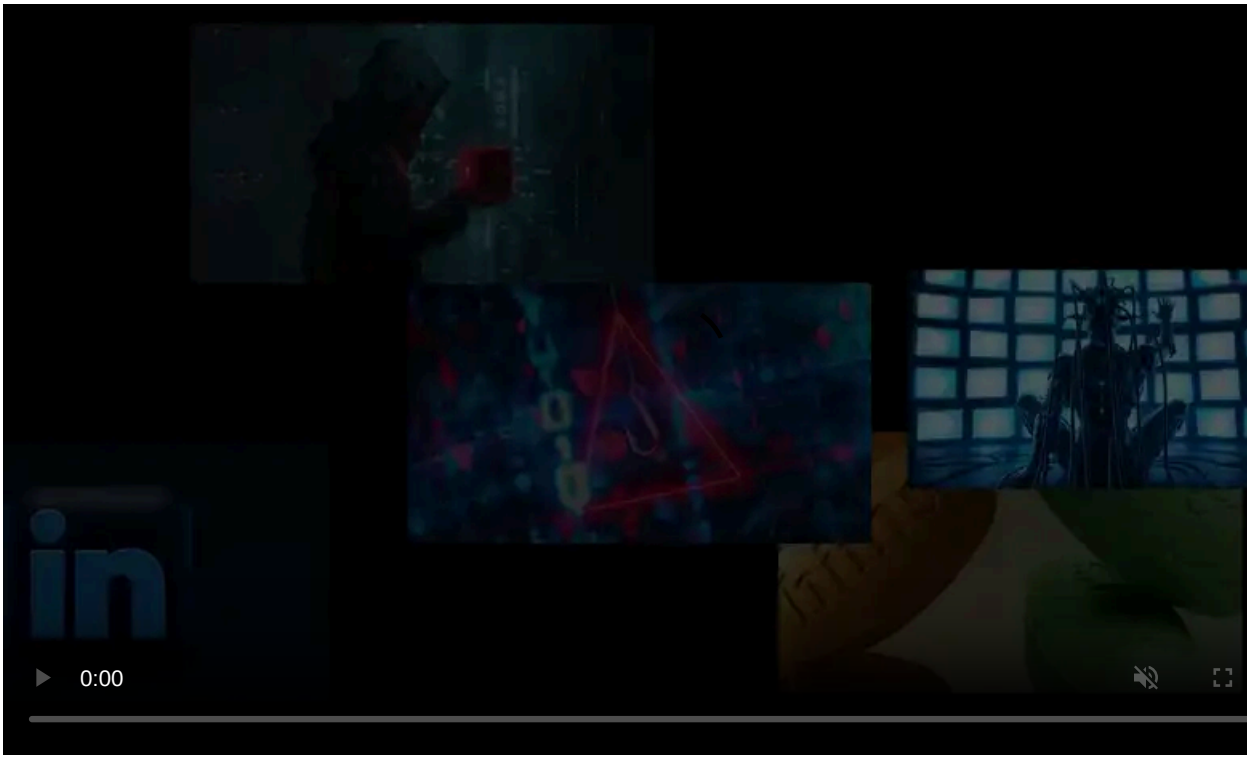
By Lawrence Abrams

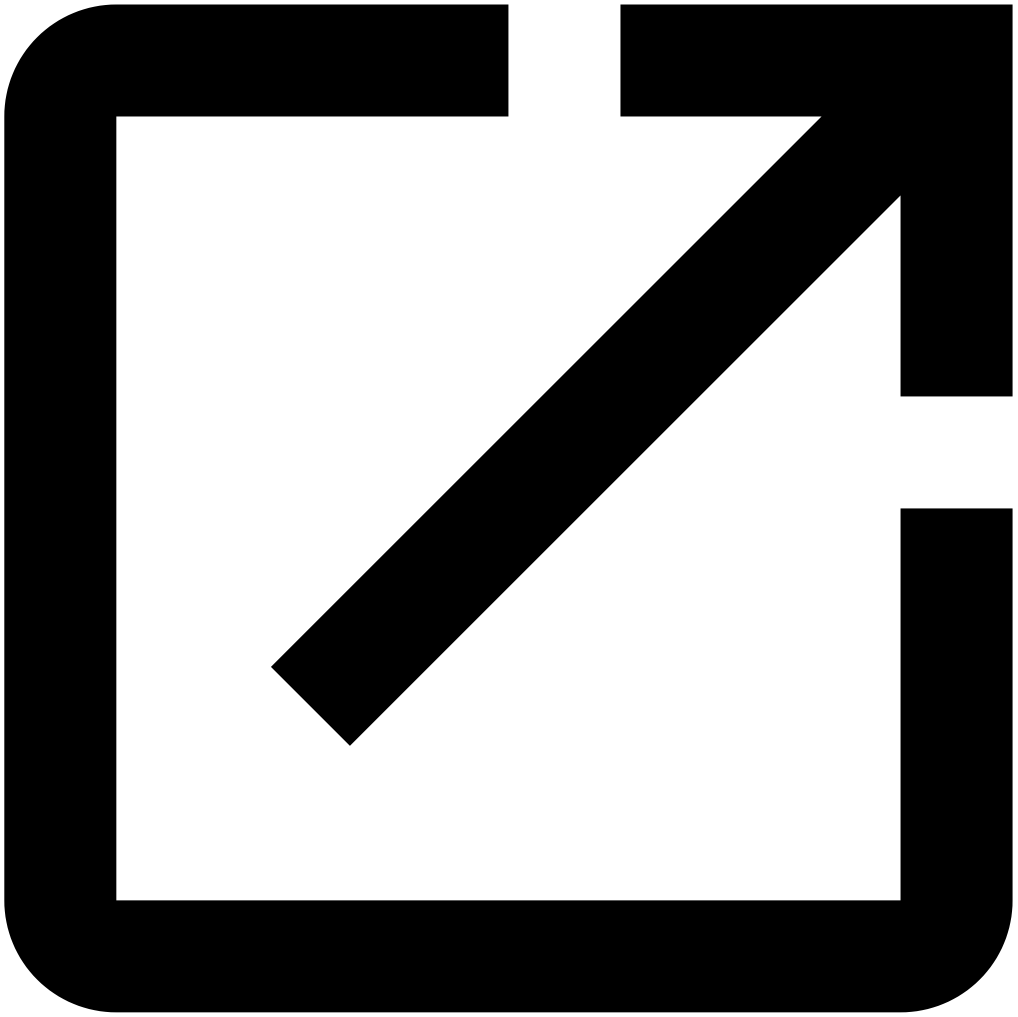
Published: 2020-09-28 · Archived: 2026-04-05 17:57:23 UTC

The REvil Ransomware (Sodinokibi) operation has deposited $1 million in bitcoins on a Russian-speaking hacker forum to prove to potential affiliates that they mean business.

Many ransomware operations are conducted as a Ransomware-as-a-Service (RaaS), where developers are in charge of developing the ransomware and payment site, and affiliates are recruited to hack businesses and encrypt their devices.

As part of this arrangement, the ransomware developers receive a 20-30% cut, and an affiliate gets 70-80% of the ransom payments they generate.


0:00



Visit Advertiser websiteGO TO PAGE

The REvil RaaS is a private operation, which means that potential affiliates are vetted and interviewed before they are allowed to join the program.

REvil deposits $1 million on a hacker forum

In an update to a forum post that they use to recruit affiliates, REvil announced today that they are once again recruiting new affiliates to distribute their ransomware.

As part of this recruitment drive, REvil is looking for teams of skilled hackers at penetration testing or experienced individuals.

"1. Teams that already have experience and skills in penetration testing, working with msf / cs / koadic, nas / tape, hyper-v and analogues of the listed software and devices;
2. People who have experience, but do not have access to work;"

To show potential affiliates that they mean business, REvil has deposited 99 bitcoins, or approximately $1 million, on the hacker forum.


Thus, we:
1. Expand the composition of the teams of acting advertisers with talented people;
2. We invite ready-made lineups to work with us;
All this is aimed at one thing - to increase the quality and quantity of waste material, which entails an increase in profits. But this does not mean that everyone will be accepted.

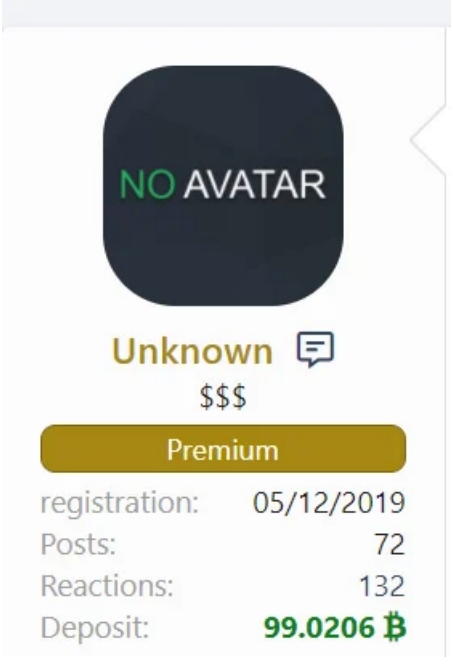
For your peace of mind and confidence, we have made a deposit of 1 million US dollars.

Last edited: Today at 15:29

Update to REvil recruitment post

This hacker forum allows members to deposit bitcoins into a wallet hosted by the site. Members can see other members' deposits, and the deposited bitcoins can be used to privately buy and sell illicit services or data through the forum.

As you can see below, the public-facing representative of REvil, known as Unknown, now has 99 bitcoins deposited on the hacker forum.



99 bitcoin deposit

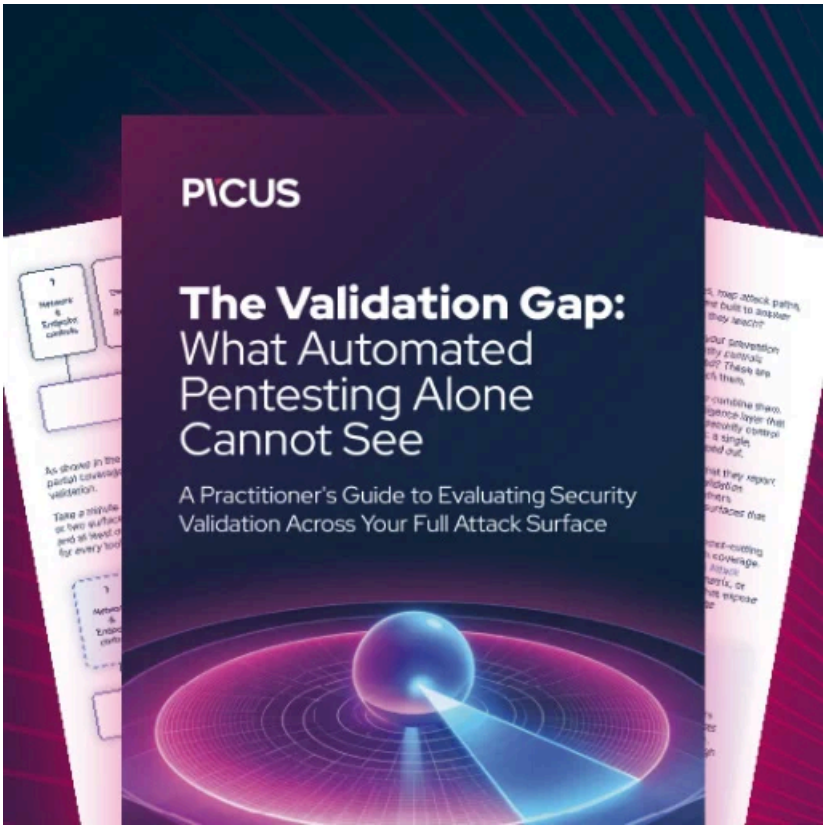
This deposit illustrates how much money ransomware operations are generating as they are publicly making a $1 million deposit as if it is not a big deal.

Furthermore, this deposit shows that they are not too concerned that the forum administrators could steal it.

As the hacker forum's owner manages the members' bitcoin wallets, the owner could pull an exit scam and abscond with the bitcoins.

Unfortunately, until victims refuse to pay multi-million dollar ransoms, this type of cybercrime with continue, and the threat actors will become richer.

Thx to Damian for the tip!



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/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/