FBI seized $2.3M from affiliate of REvil, Gandcrab ransomware gangs

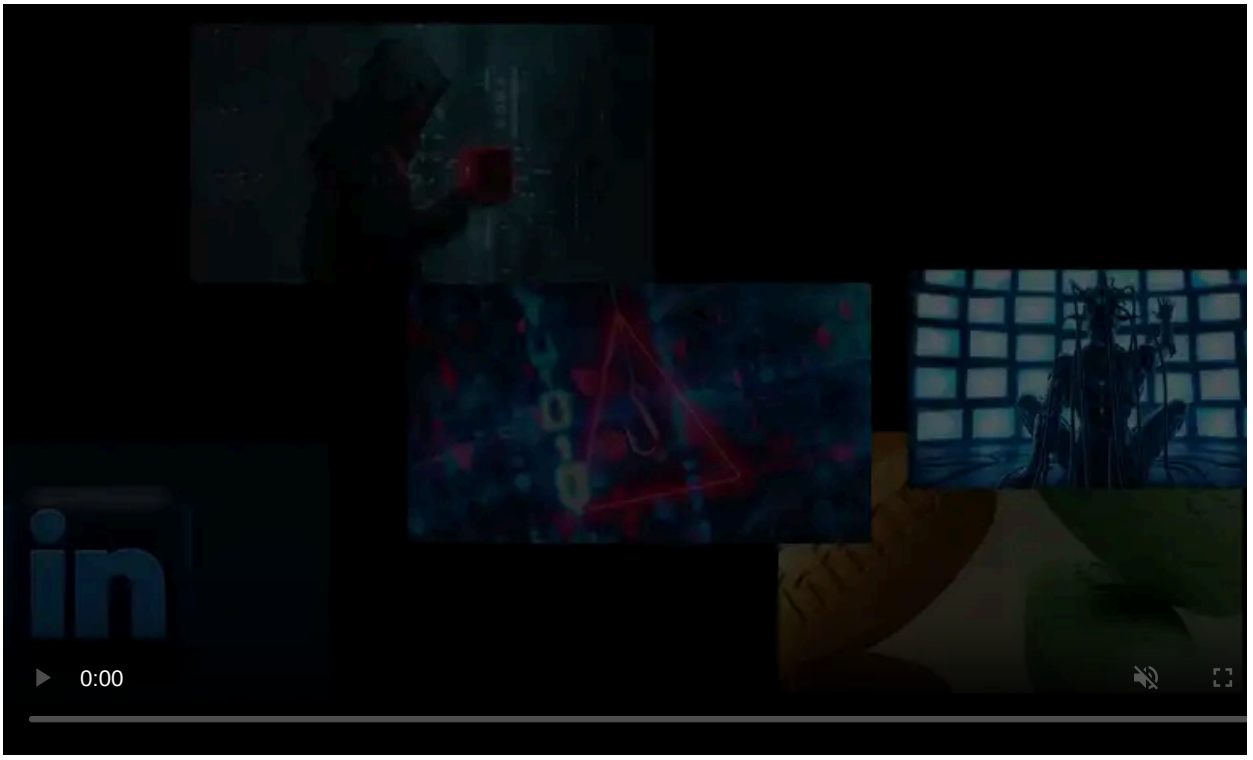
By Lawrence Abrams

Published: 2021-11-30 · Archived: 2026-04-05 17:47:38 UTC

The FBI seized $2.3 million in August from a well-known REvil and GandCrab ransomware affiliate, according to court documents seen by BleepingComputer.

In a complaint unsealed today, the FBI seized 39.89138522 bitcoins worth approximately $2.3 million at current prices ($1.5 million at time of seizure) from an Exodus wallet on August 3rd, 2021.

Exodus is a desktop or mobile wallet that owners can use to store cryptocurrency, including Bitcoin, Ethereum, Solana, and many others.


0:00

The FBI does not state how they gained access to the wallet other than that it is in their custody, indicating that they likely gained access to the wallet's private key or secret passphrase.

"The United States of America files this verified complaint in rem against 39.89138522 Bitcoin Seized From Exodus Wallet ("the Defendant Property") that is now located and in the custody and management of the Federal Bureau of Investigation ("FBI") Dallas Division, One Justice Way, Dallas Texas," reads the United States' Complaint for Forfeiture.

The complaint goes on to say that the wallet contained REvil ransom payments belonging to an affiliate identified as "Aleksandr Sikerin, a/k/a Alexander Sikerin, a/k/a Oleksandr Sikerin" with an email address of 'engfog1337@gmail.com.'

While the FBI does not indicate the online alias of the threat actor, the name 'engfog' in the email address is tied to a well-known GandCrab and REvil/Sodinokibi affiliate known as 'Lalartu.'

Targeting affiliates

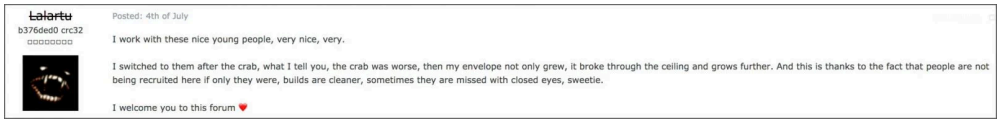
The GandCrab and REvil organizations operated as Ransomware-as-a-Service (RaaS), where core operators partner with third-party hackers, known as affiliates.

As part of this arrangement, the core operators will develop and manage the encryption/decryption software, payment portal, and data leak sites. The affiliates are tasked with hacking corporate networks, stealing data, and deploying ransomware to encrypt devices.

Any ransom payments would then be split between the affiliate and core operators, with the operators generally earning 20-30% of the ransom and affiliates making the rest.

In a REvil report by McAfee, researchers followed the money trail for a well-known threat actor known as 'Lalartu,' an affiliate for the GandCrab and REvil ransomware operations.

In 2019, the threat actor posted to a Russian-speaking hacking forum admitting they worked with GandCrab and switched to REvil after the former operation shut down.



Post by Lalartu on Russian-speaking hacking forum
Source: McAfee

After the report was released, security researcher Alon Gal attempted to track down the real identity of Lalartu.

As part of his research, Gal tracked Lalartu to the aliases' Engfog' or 'Eng_Fog,' which matches the 'engfog1337@gmail.com' email address listed in the FBI complaint.

After further conversations with security researchers, BleepingComputer has confirmed that Lalartu had been identified as 'Aleksandr Sikerin,' who is named in the complaint

In November, the Department of Justice announced that the FBI seized $6 million in ransoms paid to the REvil ransomware gang.

It is unclear if this $2.3 million is part of the previously announced number or additional ransoms seized by the FBI.

Law enforcement's continued strategy of disrupting the economics and affiliate systems of ransomware operations is paying off.

This activity has led to numerous arrests and infrastructure takedowns, including:

- The disruption of the Netwalker ransomware operation and the arrest of an affiliate in Canada.
- The arrest of the two Egregor operation members led to the shutting down of the organization.

- The arrest of 12 individuals believed to be linked to ransomware attacks against 1,800 victims in 71 countries.
- The arrest of a Ukrainian national believed to be behind the Kaseya ransomware attack.

The arrests and seizure of infrastructure are also spooking ransomware gangs into shutting down their operations, including REvil in October and BlackMatter in July.

BleepingComputer has contacted the FBI with questions about the seized bitcoins and is awaiting a response.

Update 11/30/21: Updated with correct current value of seized bitcoins.

Source: https://www.bleepingcomputer.com/news/security/fbi-seized-23m-from-affiliate-of-revil-gandcrab-ransomware-gangs/