

## U.S. offers \$10 million reward for leaders of REvil ransomware

By Lawrence Abrams

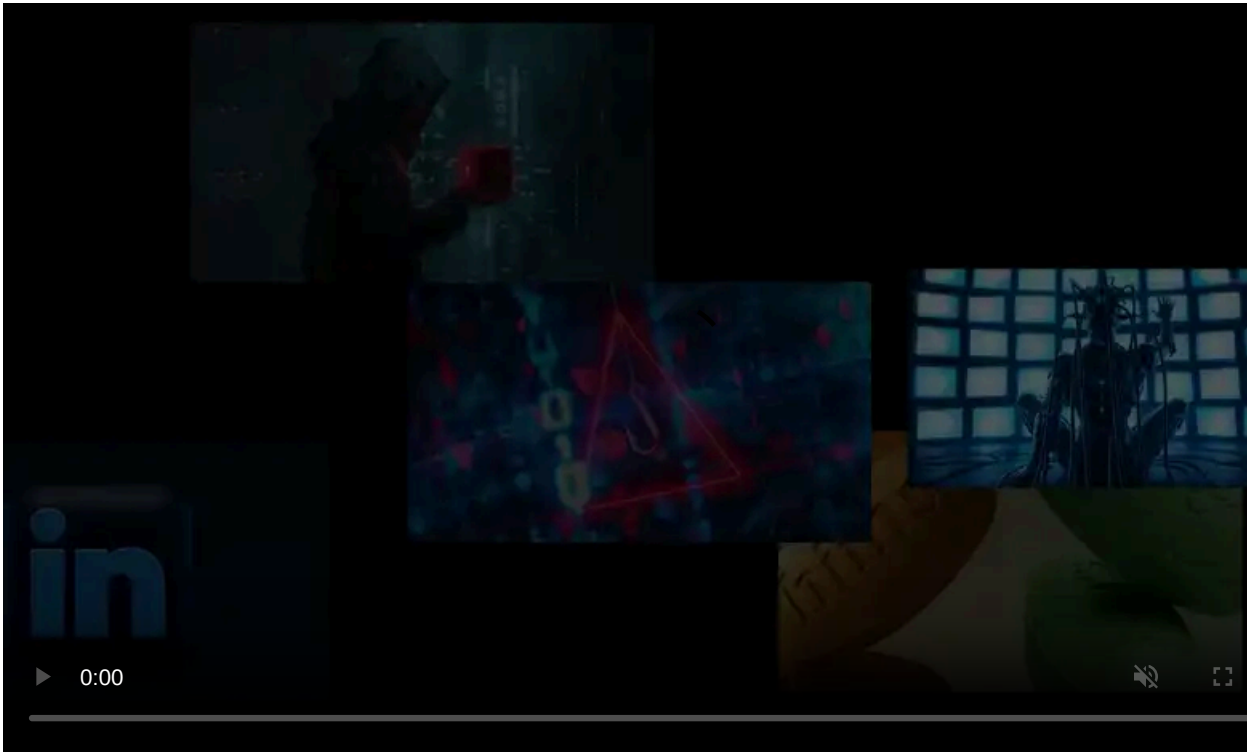
Published: 2021-11-09 · Archived: 2026-04-05 18:28:08 UTC



The U.S. is offering up to \$10 million for identifying or locating leaders in the REvil (Sodinokibi) ransomware operation, including \$5 million leading to the arrest of affiliates.

This bounty is being offered as part of the Department of State's [Transnational Organized Crime Rewards Program](#) (TOCRP), which rewards informants for information that leads to the arrest or conviction of individuals in transnational organized crime groups.

Like the reward offered for information on [DarkSide ransomware members](#), the amount rewarded for information depends on the person's role in the REvil/Sodinokibi operation.



Visit Advertiser website [GO TO PAGE](#)

The Department of State is offering a reward of up to \$10,000,000 for information leading to the identification or location of any individual holding a key leadership position in the Sodinokibi ransomware variant transnational organized crime group," the Department of State [announced](#) today.

"In addition, the Department is offering a reward offer of up to \$5,000,000 for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a Sodinokibi variant ransomware incident.

The REvil ransomware gang is responsible for numerous high-profile attacks against [Kaseya](#), [JBS](#), [Coop](#), [Travellex](#), [GSMLaw](#), [Kenneth Cole](#), and [Grupo Fleury](#).

When ransomware gangs attempt to evade law enforcement, they commonly rebrand under a new name. For example, the [GandCrab operation rebranded as REvil in 2019](#) after they began receiving too much attention from the media and law enforcement.

Similarly, other ransomware operations have also rebranded in the past, including:

- [DarkSide to BlackMatter](#)
- [Maze to Egregor](#)
- [Bitpaymer to DoppelPaymer](#) to [Grief](#)
- [Nemty to Nefilim to Karma](#)

As the Department of Statement announcement states, "Sodinokibi variant ransomware," this reward will also apply to new ransomware operations created by the REvil gang in the future.

Today was also filled with numerous announcements regarding the [arrest and indictments of multiple REvil gang members](#). These arrests included an REvil hacker linked to the Kaseya ransomware attack and the [seizure of \\$6 million in cryptocurrency](#) obtained through REvil ransom demands.

To further disrupt the financial operations of ransomware groups, the U.S. also announced [sanctions against the Chatex cryptocurrency exchange](#) for assisting ransomware gangs in laundering and cashing out ransom payments.



### [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/us-offers-10-million-reward-for-leaders-of-revil-ransomware/>