

## Kaseya obtains universal decryptor for REvil ransomware victims

By Lawrence Abrams

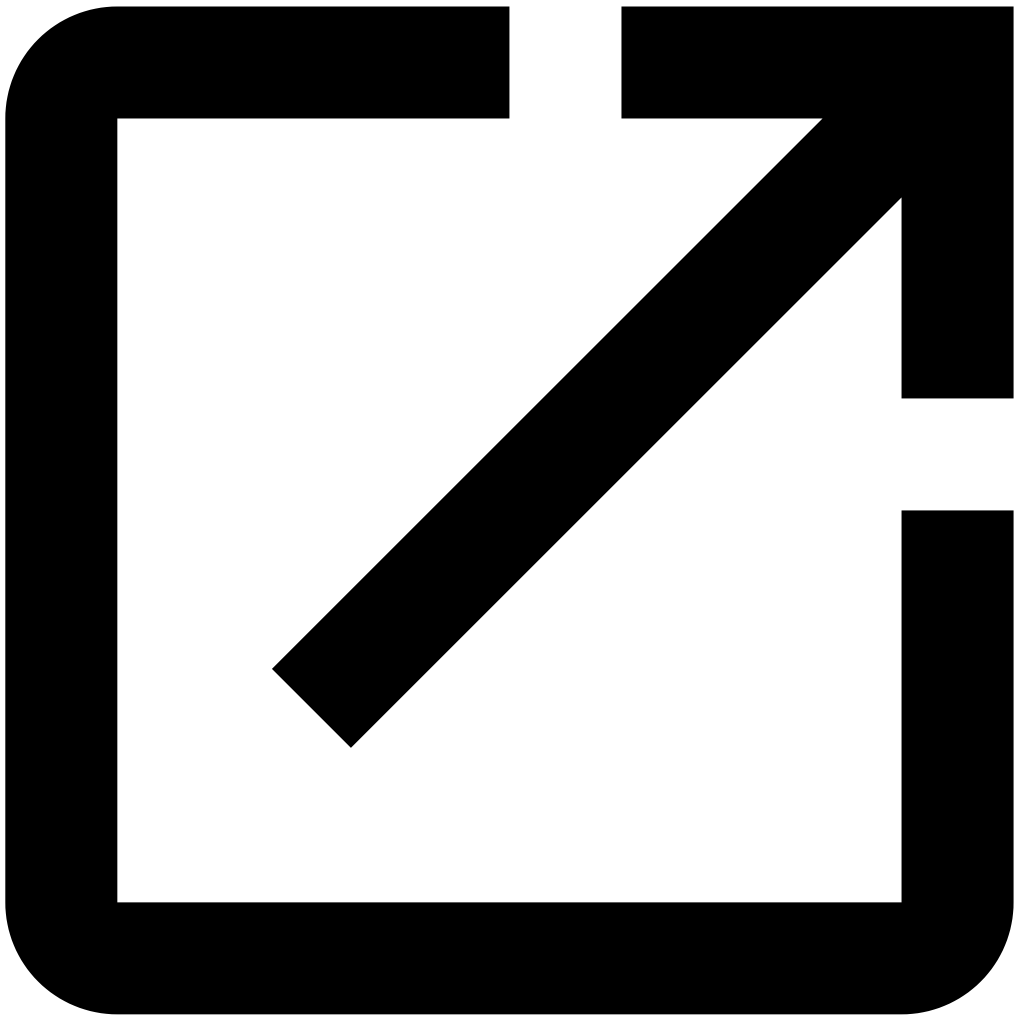
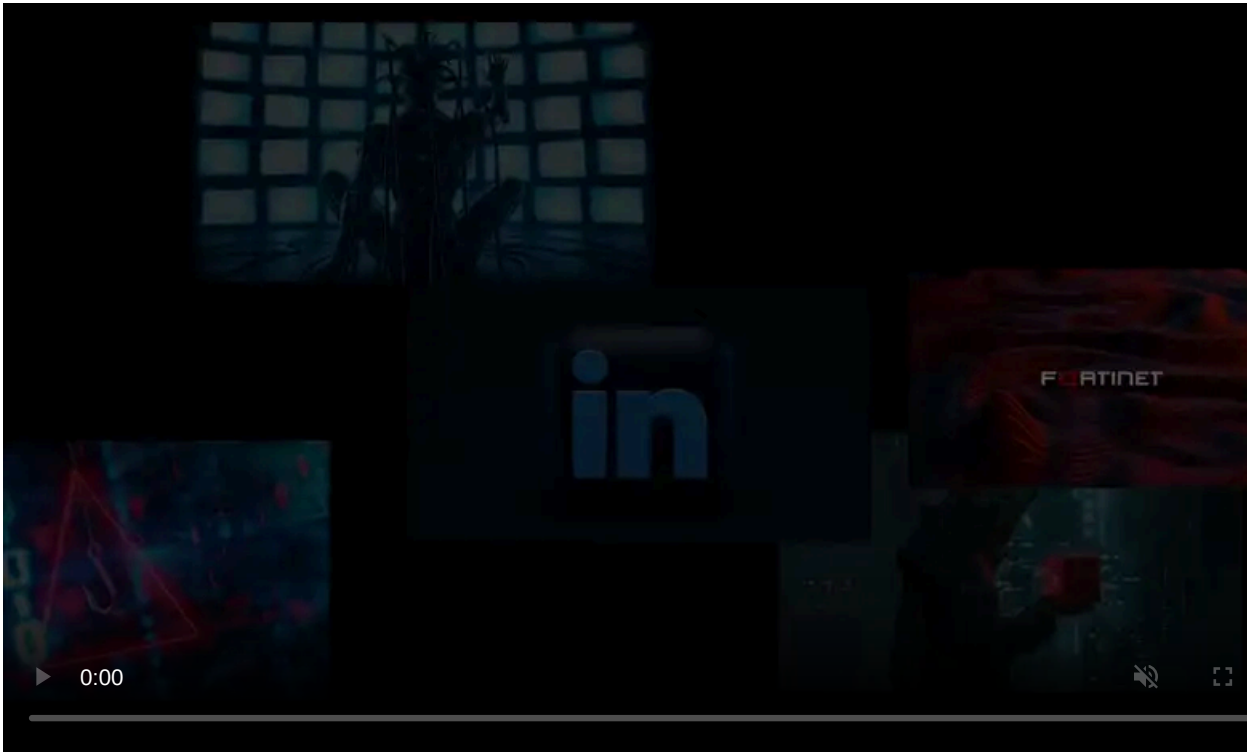
Published: 2021-07-22 · Archived: 2026-04-05 20:10:04 UTC



Kaseya received a universal decryptor that allows victims of the July 2nd REvil ransomware attack to recover their files for free.

On July 2nd, the REvil ransomware operation [launched a massive attack](#) by exploiting a zero-day vulnerability in the Kaseya VSA remote management application to encrypt approximately sixty managed service providers and an estimated 1,500 businesses.

After the attack, the threat actors [demanded \\$70 million](#) for a universal decryptor, \$5 million for MSPs, and \$40,000 for each extension encrypted on a victim's network.



Visit Advertiser website [GO TO PAGE](#)

Happy Blog

Blog search

Search

## KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000\$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

### Revil's \$70 million ransom demand

Soon after, the [REvil ransomware gang mysteriously disappeared](#), and the threat actors shut down their payment sites and infrastructure.

While [most victims were not paying](#), the gang's disappearance prevented companies who may have needed to purchase a decryptor unable to do so.

Today, Kaseya has stated that they received a universal decryptor for the ransomware attack from a "trusted third party" and are now distributing it to affected customers.

"We can confirm we obtained a decryptor from a trusted third party but can't share anymore about the source," Kaseya's SVP Corporate Marketing Dana Liedholm told BleepingComputer.

"We had the tool validated by an additional third party and have begun releasing it to our customers affected."

While Kaseya would not share information about the key's source, they confirmed with BleepingComputer that it is the universal decryption key for the entire attack, allowing all MSPs and their customers to decrypt files for free.

When asked whether they paid a ransom to receive a decryptor, Kaseya told BleepingComputer that they "can't confirm or deny that."

Emsisoft CTO Fabian Wosar told BleepingComputer that they were the third party who validated the key and will continue to aid Kaseya in their recovery efforts.

"We are working with Kaseya to support their customer engagement efforts. We have confirmed the key is effective at unlocking victims and will continue to provide support to Kaseya and its customers," Wosar told BleepingComputer.

It is unclear what caused the REvil ransomware operation to shut down and go into hiding, and multiple international law enforcement agencies have told BleepingComputer that they were not involved in their disappearance.

After the [attack on JBS](#) and Kaseya, the [White House's has pressured the Russian government](#) to do something about the ransomware gangs believed to be operating within Russia.

It is believed that the Russian government told the REvil ransomware gang to shut down and disappear to show that they were working with the USA.

As the decryptor was obtained after the REvil gang's disappearance, it is possible that Russia received it directly from the ransomware gang and shared it with US law enforcement as a gesture of goodwill.

When we asked the FBI if they were involved in the procurement of the decryption key, we were told that they do not comment on ongoing investigations.

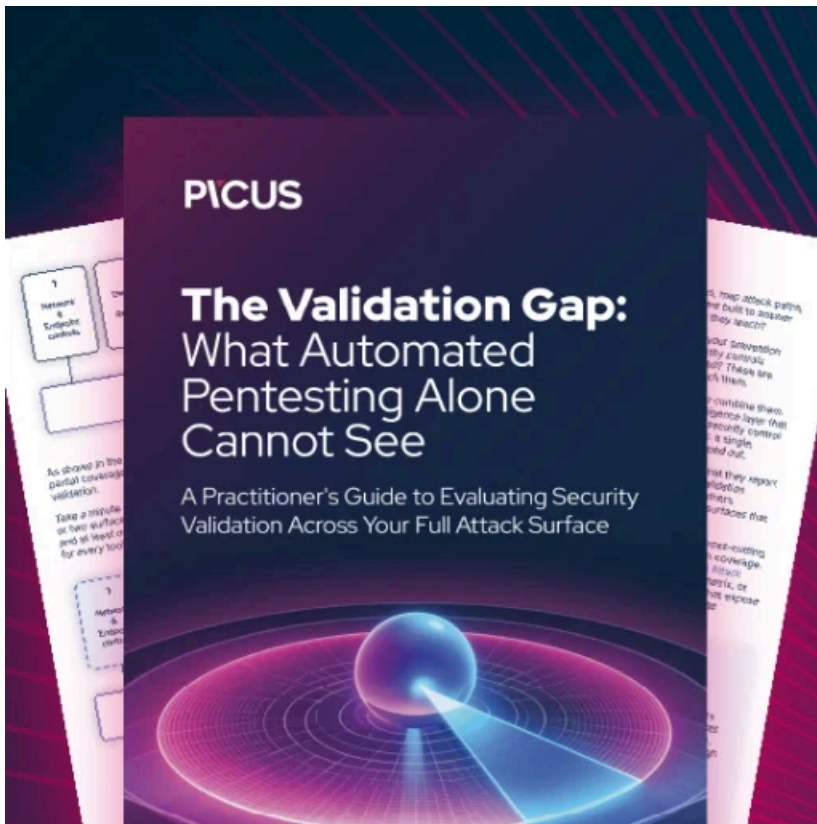
"The DOJ and FBI have an ongoing criminal investigation into the criminal enterprise behind the REvil/Sodinokibi ransomware variant and the actors responsible for the Kaseya ransomware attack specifically," the FBI told BleepingComputer.

"Per DOJ policy, we cannot comment further on this ongoing investigation."

REvil's disappearance is likely not the end of the gang's online activities.

In the past the [GandCrab ransomware operation shut down](#) and rebranded as REvil, and it is expected that REvil will resurface again as a new ransomware operation.

*Update 7/22/21 9:42 PM EST: Added Emsisoft and FBI statements.*



### **[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/kaseya-obtains-universal-decryptor-for-revil-ransomware-victims/>