DOJ Attacks Back Against REvil – Arrests and Seizure of $6.1M Ransom AND Knocks Them Offline

Department of Justice officials announced the arrests of five members of the ransomware criminal enterprise, REvil. REvil has been tied to over 7k ransomware attacks and hundreds of millions in ransoms, including the attack on meat supplier JBS and Miami-based technology company Kaseya. JBS paid $11M in ransom but Kaseya refused to negotiate with the cybercriminals. The arrests were part of an international investigation, Operation GoldDust, involving law enforcement agencies from 17 countries. Members of REvil were identified through wiretapping and seizure of REvil infrastructure – and, exploiting REvil tactics against its members.

Officials recovered $6.1M worth of cryptocurrency previously owned by Polyanin, who has also been indicted but not arrested (with extradition from Russia unlikely). Law enforcement agents recognize that seizure of millions squarely smacks REvil and serves as a deterrent to other attackers.

Working with the FBI, Romanian firm Bitdefender in September released a free decryptor for all REvil attacks that occurred before July 13.

> "Since mid-September this year, the Sodinokibi/REvil decryptor has helped more than 1,400 companies in 83 countries recover their files and save over $550 million in unpaid ransom."
>
> Bogdan Botezatu, Director of Threat Research, Bitdefender.

Tom Kellermann, Head of Cybersecurity Strategy at VMWare and an adviser to the U.S. Secret Service on cybercrime investigations, said, "The FBI, in conjunction with Cyber Command, the Secret Service and like-minded countries, have truly engaged in significant disruptive actions against these groups.”“REvil was top of the list.” Kellermann credited this success as deriving from the determination by U.S. Deputy Attorney General Lisa Monaco that ransomware attacks on critical infrastructure should be treated as a national security issue akin to terrorism.

President Biden commented on the investigation, "We are bringing the full strength of the federal government to disrupt malicious cyber activity and actors, bolster resilience at home, address the

abuse of virtual currency to launder ransom payments, and leverage international cooperation to disrupt the ransomware ecosystem and address safe harbors for ransomware criminals."

REvil may have been scamming some affiliates. Earlier this year, malware reverse-engineering specialists on the Russian-language Exploit cybercrime forum analyzed REvil samples and reported finding a backdoor that could be used by administrators to decrypt systems and files encrypted using the malware. Apparently, REvil's developers gave themselves a backdoor so they could negotiate directly with victims yet pretend to the responsible affiliate the victim had declined to pay.

Law enforcement and intelligence cyber specialists were able to hack REvil's computer network infrastructure, obtaining control of at least some of their servers. A leadership figure known as "0_neday," who had helped restart the group's operations after an earlier shutdown, said REvil's servers had been hacked by an unnamed party. "The server was compromised, and they were looking for me," 0_neday wrote on a cybercrime forum last weekend and first spotted by security firm Recorded Future. "Good luck, everyone; I'm off."

When gang member 0_neday and others restored those websites from a backup last month, he unknowingly restarted some internal systems that were already controlled by law enforcement.

> “The REvil ransomware gang restored the infrastructure from the backups under the assumption that they had not been compromised,” Oleg Skulkin, Head of Digital Forsenics and Incident Response Team, Group-IB. “Ironically, the gang's own favorite tactic of compromising the backups was turned against them.”

Karen Heumann, G2M Communications