

# U.S. Department of Justice Disrupts Hive Ransomware Variant

[justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant](https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant)



Press Release

Thursday, January 26, 2023

**For Immediate Release**

Office of Public Affairs

**FBI Covertly Infiltrated Hive Network, Thwarting Over \$130 Million in Ransom Demands**

The Justice Department announced today its months-long disruption campaign against the Hive ransomware group that has targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and critical infrastructure.

Since late July 2022, the FBI has penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay \$130 million in ransom demanded. Since infiltrating Hive's network in July 2022, the FBI has provided over 300 decryption keys to Hive victims who were under attack. In addition, the FBI distributed over 1,000 additional decryption keys to previous Hive victims. Finally, the department announced today that, in coordination with German law enforcement (the German Federal Criminal Police and Reutlingen Police Headquarters-CID Esslingen) and the Netherlands National High Tech Crime Unit, it has seized control of the servers and websites that Hive uses to communicate with its members, disrupting Hive's ability to attack and extort victims.

"Last night, the Justice Department dismantled an international ransomware network responsible for extorting and attempting to extort hundreds of millions of dollars from victims in the United States and around the world," said Attorney General Merrick B. Garland. "Cybercrime is a constantly evolving threat. But as I have said before, the Justice Department will spare no resource to identify and bring to justice, anyone,

anywhere, who targets the United States with a ransomware attack. We will continue to work both to prevent these attacks and to provide support to victims who have been targeted. And together with our international partners, we will continue to disrupt the criminal networks that deploy these attacks.”

“The Department of Justice’s disruption of the Hive ransomware group should speak as clearly to victims of cybercrime as it does to perpetrators,” said Deputy Attorney General Lisa O. Monaco. “In a 21st century cyber stakeout, our investigative team turned the tables on Hive, swiping their decryption keys, passing them to victims, and ultimately averting more than \$130 million dollars in ransomware payments. We will continue to strike back against cybercrime using any means possible and place victims at the center of our efforts to mitigate the cyber threat.”

“The coordinated disruption of Hive’s computer networks, following months of decrypting victims around the world, shows what we can accomplish by combining a relentless search for useful technical information to share with victims with investigation aimed at developing operations that hit our adversaries hard,” said FBI Director Christopher Wray. “The FBI will continue to leverage our intelligence and law enforcement tools, global presence, and partnerships to counter cybercriminals who target American business and organizations.”

“Our efforts in this case saved victims over a hundred million dollars in ransom payments and likely more in remediation costs,” said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department’s Criminal Division. “This action demonstrates the Department of Justice’s commitment to protecting our communities from malicious hackers and to ensuring that victims of crime are made whole. Moreover, we will continue our investigation and pursue the actors behind Hive until they are brought to justice.”


“Cybercriminals utilize sophisticated technologies to prey upon innocent victims worldwide,” said U.S. Attorney Roger Handberg for the Middle District of Florida. “Thanks to the exceptional investigative work and coordination by our domestic and international law enforcement partners, further extortion by HIVE has been thwarted, critical business operations can resume without interruption, and millions of dollars in ransom payments were averted.”

Since June 2021, the Hive ransomware group has targeted more than 1,500 victims around the world and received over \$100 million in ransom payments.

Hive ransomware attacks have caused major disruptions in victim daily operations around the world and affected responses to the COVID-19 pandemic. In one case, a hospital attacked by Hive ransomware had to resort to analog methods to treat existing patients and was unable to accept new patients immediately following the attack.

Hive used a ransomware-as-a-service (RaaS) model featuring administrators, sometimes called developers, and affiliates. RaaS is a subscription-based model where the developers or administrators develop a ransomware strain and create an easy-to-use interface with which to operate it and then recruit affiliates to deploy the ransomware against victims. Affiliates identified targets and deployed this readymade malicious software to attack victims and then earned a percentage of each successful ransom payment.

Hive actors employed a double-extortion model of attack. Before encrypting the victim system, the affiliate would exfiltrate or steal sensitive data. The affiliate then sought a ransom for both the decryption key necessary to decrypt the victim's system and a promise to not publish the stolen data. Hive actors frequently targeted the most sensitive data in a victim's system to increase the pressure to pay. After a victim pays, affiliates and administrators split the ransom 80/20. Hive published the data of victims who do not pay on the Hive Leak Site.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Hive affiliates have gained initial access to victim networks through a number of methods, including: single factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocols; exploiting FortiToken vulnerabilities; and sending phishing emails with malicious attachments. For more information about the malware, including technical information for organizations about how to mitigate its effects, is available from CISA, visit <https://www.cisa.gov/uscert/ncas/alerts/aa22-321a>  .

Victims of Hive ransomware should contact their local FBI field office for further information.

The FBI Tampa Field Office, Orlando Resident Agency is investigating the case.

Trial Attorneys Christen Gallagher and Alison Zitron of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Chauncey Bratt for the Middle District of Florida are prosecuting the case.

The Justice Department also recognizes the critical cooperation of the German Reutlingen Police Headquarters-CID Esslingen, the German Federal Criminal Police, Europol, and the Netherlands Politie, and significant assistance was provided by the U.S. Secret Service, U.S. Attorney's Office for the Eastern District of Virginia, and U.S. Attorney's Office for the Central District of California. The Justice Department's Office of International Affairs and the Cyber Operations International Liaison also provided significant assistance. Additionally, the following foreign law enforcement authorities provided substantial assistance and support: the Canadian Peel Regional Police and Royal Canadian Mounted Police, French Direction Centrale de la Police Judiciaire, Lithuanian Criminal Police Bureau, Norwegian National Criminal Investigation Service in collaboration with the Oslo Police District, Portuguese Polícia Judiciária, Romanian Directorate of Countering Organized Crime, Spanish Policia Nacional, Swedish Police Authority, and the United Kingdom's National Crime Agency.

Updated January 26, 2023

---

## Topic

Cybercrime

Press Release Number: 23-99