Five affiliates to Sodinokibi/REvil unplugged

By Europol

Published: 2021-11-08 · Archived: 2026-04-05 16:07:03 UTC

- 

Updated on 8 November at 18:30

On 4 November, Romanian authorities arrested two individuals suspected of cyber-attacks deploying the Sodinokibi/REvil ransomware. They are allegedly responsible for 5 000 infections, which in total pocketed half a million euros in ransom payments. Since February 2021, law enforcement authorities have arrested three other affiliates of Sodinokibi/REvil and two suspects connected to GandCrab. These are some of the results of operation GoldDust, which involved 17 countries*, Europol, Eurojust and INTERPOL. All these arrests follow the joint international law enforcement efforts of identification, wiretapping and seizure of some of the infrastructure used by Sodinokibi/REvil ransomware family, which is seen as the successor of GandCrab.

Anti-REvil team set up in Europe

Since 2019, several large international corporations have faced severe cyber-attacks, which deployed the Sodinokibi/REvil ransomware. France, Germany, Romania, Europol and Eurojust reinforced the actions against this ransomware by setting up a Joint Investigation Team in May 2021. Bitdefender, in collaboration with law

enforcement, made a tool available on the No More Ransom website that would help victims of Sodinokibi/REvil restore their files and recover from attacks made before July 2021. In the beginning of October, a Sodinokibi/REvil affiliate was arrested at the Polish border after an international arrest warrant was issued by the US. The Ukrainian national is suspected of perpetrating the Kaseya attack, which affected up to 1 500 downstream businesses and for which Sodinokibi/REvil asked a ransom of about €70 million. Additionally, in February, April and October 2021 authorities in South Korea arrested three affiliates involved in the GandCrab and Sodinokibi/REvil ransomware families, which had more than 1 500 victims. On 4 November, Kuwaiti authorities arrested another GandGrab affiliate, meaning a total of seven suspects linked to the two ransomware families have been arrested since February 2021. They are suspected of attacking about 7 000 victims in total.

GoldDust' links to GandCrab

Since 2018, Europol has supported a Romanian-led investigation which targets the GandCrab ransomware family and involved law enforcement authorities from a number of countries, including the United Kingdom and the United States. With more than one million victims worldwide, GandCrab was one of the world's most prolific ransomware families. These joint law enforcement efforts resulted in the release of three decryption tools through the No More Ransom project, saving more than 49 000 systems and over €60 million in unpaid ransom so far. The investigation also looked at the affiliates of GandCrab, some of whom are believed to have moved towards Sodinokibi/REvil. Operation GoldDust was also built up on leads from this previous investigation targeting GandCrab.

Decrypt with No More Ransom

The support from the cybersecurity sector has proven crucial for minimising the damage from ransomware attacks, still the biggest cybercrime threat. Many partners have already provided decryption tools for a number of ransomware families via the No More Ransom website. Bitdefender supported this investigation by providing key technical insights throughout the entire investigation, along with decryption tools for both of these highly prolific ransomware families to help victims recover their files. KPN and McAfee Enterprises are other private sector partners that have also supported this investigation, by providing technical expertise to law enforcement.

Currently, No More Ransom has decryption tools for GandCrab (V1, V4 and V5 up to V5.2 versions) and for Sodinokibi/REvil. The Sodinokibi/REvil decryption tools helped more than 1400 companies decrypt their networks, saving them almost €475 million in potential losses. The tools made available for both ransomware families enabled more than 50 000 decryptions, for which cybercriminals had asked about €520 million in ransom.

Europol's support

Europol facilitated the information exchange, supported the coordination of operation GoldDust and provided operational analytical support, as well as cryptocurrency, malware and forensic analysis. During the action days, Europol deployed experts to each location and activated a Virtual Command Post to coordinate the activities on the ground. The international cooperation enabled Europol to streamline victim mitigation efforts with other EU countries. These activities prevented private companies from falling victim to Sodinokibi/REvil ransomware.

The Joint Cybercrime Action Taskforce (J-CAT) at Europol supported the operation. This standing operational team consists of cyber liaison officers from different countries who work from the same office on high profile cybercrime investigations.

*Participant countries: Australia, Belgium, Canada, France, Germany, the Netherlands, Luxembourg, Norway, Philippines, Poland, Romania, South Korea, Sweden, Switzerland, Kuwait, the United Kingdom, the United States

* Participating organisations: Europol, Eurojust and Interpol

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime, and other serious and organised crime forms. Europol also works with many non-EU partner states and international organisations. From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

Empact

The European Multidisciplinary Platform Against Criminal Threats (EMPACT) tackles the most important threats posed by organised and serious international crime affecting the EU. EMPACT strengthens intelligence, strategic and operational cooperation between national authorities, EU institutions and bodies, and international partners. EMPACT runs in four-year cycles focusing on common EU crime priorities.
