BURR FORMAN LLP

# U.S. and Europe Target Top Ransomware Cartel

Articles / Publications
12.10.2021

RELATED CAPABILITIES

Cybersecurity & Data Privacy

An international law-enforcement effort has led to the arrest of multiple individuals affiliated with the most prolific ransomware cartel operating today. In November, Justice Department officials announced indictments and an arrest of hackers associated with REvil (a.k.a. Sodinokibi), a Russian-speaking cyber gang linked to a number of high-profile cybersecurity incidents over the past year, including ransomware attacks against Miami-based software firm Kaseya Ltd. and the world's largest meat supplier.

Specifically, on November 08, 2021, the DOJ indicted two men (a 28-year-old Russian national named Yevgeniy Polyanin and a 22-year-old Ukrainian named Yaroslav Vasinskyi) for their alleged affiliation with REvil. The separate indictments against each man allege computer crimes and conspiracy to commit fraud and money laundering. Vasinskyi, who was arrested at the Polish border at the request of U.S. officials, is alleged to have been behind the Kaseya attacks noted above, where the data of between 800 and 1,500 of Kaseya's software customers was encrypted in a July 2021 REvil ransomware deployment. Those affected by that incident included major Swedish pharmacies and grocery chains using Kaseya software.

The indictment against Polyanin, the Russian national, alleges his involvement in REvil ransomware attacks against several victims, including public and private entities in Texas during the summer of 2019. Polyanin is believed to have been behind several-thousand ransomware attacks that netted $13 million in ransom payments from U.S. entities alone. The Department also seized over $6 million in funds traceable to ransomware payments allegedly received by Polyanin, whose whereabouts are unknown.

# U.S. and Europe Target Top Ransomware Cartel

Contemporaneous with these indictments, the Treasury Department added REvil leadership as an official target under the Transnational Organized Crime Rewards Program, offering up to a $10 million reward for information leading to the identification or location of anyone holding a "key leadership position in the Sodinokibi/REvil ransomware" group. Also on November 8th, Europol and Romanian authorities announced the arrest of two men responsible for roughly 5,000 Sodinokibi/REvil infections. This activity was part of an international effort called operation "GoldDust," which investigated a REvil predecessor known as GandCrab and involved 17 countries, Europol, Eurojust, and INTERPOL. The international community made a number of other arrests of individuals with REvil / GandCrab links in 2021, including hackers found in South Korea and Kuwait.

A ransomware attack is a type of extortion in which hackers gain unauthorized access to a system, lock-up the victim's data through encryption, and demand payment to unlock or 'decrypt' the data. Often times, the bad actors may also advise the victims that they will release stolen files to the public unless they receive additional payments. According to IBM's threat-intelligence index, REvil stole roughly 21.6 terabytes of data, and accounted for at least $123 million worth of global ransomware payments in 2020 (a significant portion of the estimated $416 million in reported ransomware payments in the U.S. that year). The White House reported $590 million of reported ransomware payments occurring through the first half of 2021 alone, indicating an alarming uptick in the volume and/or success of success-rate of these attacks. What's more, a number of 2021's ransomware attacks affected key resources or infrastructure. Ransomware has therefore become a national-security priority, which explains the unprecedented domestic and international coordination targeting REvil.

These arrests and indictments are not the U.S. government's first confrontation with REvil, however. In July 2021, after a REvil-linked ransomware attack against the world's biggest meatpacker, sites affiliated with REvil on the dark web were shut down. U.S. authorities did not immediately take credit for that incident, but it was reported by the Washington Post that U.S. Cyber Command in coordination with a foreign government hacked into the REvil's servers and again blocked its website in October, 2021.

With these developments, the Biden administration has signaled its intent to make good on President Biden's promise to Vladimir Putin in June 2021 that the U.S. "would take action to hold cybercriminals accountable." It is widely believed that most ransomware developers are based in Russia, which hampers law-enforcement options for the U.S. and Europe because Russia does not have extradition treaties with many Western countries. While it seems unlikely that Russia will assist in the arrest or prosecution of Polyanin or others like him, the escalation in the international community's fight against ransomware and other cybercrimes in recent months has been remarkable.

However, some commentators fear that other cyber gangs that maintain different ransomware strands may fill the void as REvil is targeted or dismantled. Examples of upstarts include the PYSA ransomware (standing for "protect your data, amigo"), which has targeted schools across the U.S. and UK this year. Companies should applaud and encourage the government's recent efforts to mitigate and prosecute cybercrimes, but these efforts are not expected to have an effect on the risks or threat landscape in the near-term. Businesses of all sizes should proactively and regularly take a careful inventory of their system security/ risks, incident response plan, and insurance coverage to limit their losses and liability in the

event of a ransomware incident.