CATEGORIES

Select Category

RECENT POSTS

NYDFS Issues Guidance on Artificial Intelligence-related Cybersecurity Risks

Green Light for the Enforcement of NIS 2 in Limited EU Countries Only

EDPB Adopts Opinion on the Use of Processors and Sub-processors

DOJ Unseals Indictment of Evil Corp Member, While OFAC Announces New Evil Corp Sanctions

Belgian Data Protection Authority Publishes Guidance on the Interplay between the GDPR and the AI Act

DOJ Unseals Indictment of Evil Corp Member, While OFAC Announces New Evil Corp Sanctions

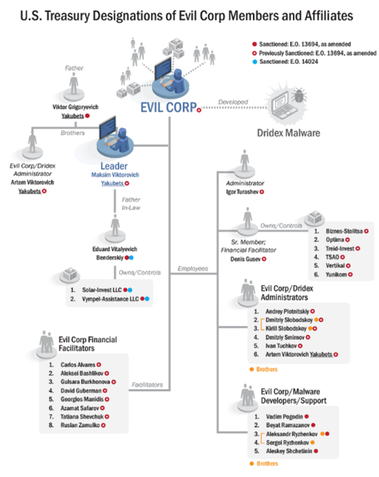
October 9, 2024 By Kim Peretti, Kellen Dwyer, Kelly Hagedorn and Andrew Rice

On October 1, 2024, the Department of Justice ("DOJ") unsealed an indictment against Aleksandr Viktorovich Ryzhenkov (Александр Викторович Рыженков), a member of the ransomware group Evil Corp. The indictment charges Ryzhenkov with several violations of the Computer Fraud & Abuse Act, as well as conspiring to commit money laundering, arising from his use of a ransomware strain called "BitPaymer." In addition to his alleged work with Evil Corp, the United Kingdom's National Crime Agency ("NCA") has reported that Ryzhenkov is also a suspected affiliate of LockBit, another ransomware group which the FBI disrupted in February of 2024 and of which the DOJ indicted one of its leaders in May of 2024. Concurrent with the unsealing of the indictment, the United States Treasury Department's Office of Foreign Asset Control ("OFAC") announced that it had added Ryzhenkov, along with six other Evil Corp related persons, to its Specially Designated Nationals and Blocked Persons List ("SDN List").

DOJ's decision to unseal this indictment, which was filed under seal in March of 2023, is notable because Ryzhenkov remains at large and is believed to reside in Russia. Historically, the Justice Department has indicted Russian cybercriminals under seal and waited for the criminals to travel to a friendly country from which they could be extradited. Here, by contrast, DOJ appears to be using a "name, shame, and sanction" strategy against criminal hackers, which may be indicative of a larger shift in DOJ's cybercrime strategy to favor disruption over arrest and prosecution.

The addition of Ryzhenkov and the other Evil Corp related individuals to OFAC's SDN List is also notable. This is the fourth time this year that OFAC has added an individual ransomware actor to its SDN list. Companies considering paying a ransom will need to conduct increased due diligence to ensure that any payment does not go to any sanctioned individual. This will be a difficult task given that ransomware actors, in addition to being opaque and dishonest, frequently change their affiliation. Ryzhenkov, for instance, appears to have worked with both Evil Corp and LockBit. Victims dealing with any ransomware group, therefore, must ask whether the group may be affiliated with a sanctioned individual.

Evil Corp itself, along with several of its members, were added to the SDN List in 2019. The chart below, which was released by the Treasury Department, shows the group's membership and structure, along with the individuals who have been sanctioned.



Filed Under: Cybercrime, Cybersecurity, Digital Crimes, International, Ransomware, Russia
Tagged With: Cybercrime, Cybersecurity, Digital Crimes, International, Ransomware, Russia

About Kim Peretti

A former DOJ cybercrime prosecutor and former director of PwC's cyber forensics group, Kim delivers top of the line cyber risk management and information security counsel to her clients. As co-leader of our Privacy, Cyber & Data Strategy Team, Kim is recognized by select publications and is frequently quoted by the media.
[Read Bio]

About Kellen Dwyer

Kellen Dwyer is partner and co-leader of Alston & Bird's National Security & Digital Crimes practice. He previously served in the Justice Department in several cyber and national security roles. As an assistant U.S. attorney in the Eastern District of Virginia, he obtained a computer hacking indictment against Julian Assange and represented the United States at Assange's extradition hearings in London.
[Read Bio]

About Andrew Rice

Drawing on a broad array of experiences, Andrew uses his astute knowledge and unique insights to help clients find solutions to their complex matters.
[Read Bio]

Search this website

This blog is a service of Alston & Bird's Privacy, Cyber & Data Strategy team and focuses on key data privacy and data security issues.

RECEIVE EMAIL NOTIFICATIONS WHEN NEW POSTS ARE ADDED.

Email *

- select country -

SUBSCRIBE!

THE DIGITAL DOWNLOAD
Click here to see the editions

PRIVACY & CYBER EVENTS
Click here to see upcoming and past events

PRIVACY & CYBER MAILINGS
Click here to sign up

@ALSTONPRIVACY
Click here to follow us on Twitter