Two Russians charged in 'Evil Corp' global cybertheft ring

December 5 2019, by Michael Balsamo and Frank Bajak

Credit: CC0 Public Domain

The Justice Department unsealed charges Thursday against the alleged leader and a top associate of a Russian cybercriminal gang that U.S. and British officials say developed and distributed malware used to steal at least $100 million from banks and other financial institutions in more than 40 countries over the past decade.

Separately, the Treasury Department said that in collaboration with Britain's National Crime Agency, it was freezing all assets of the two Russian men, along with 15 other associates and seven Russian-based

organizations including Evil Corp., their alleged umbrella group.

Charged in a 10-count indictment filed in federal court in Pittsburgh were Evil Corp.'s alleged leader, Maksim V. Yakubets, 32, of Moscow, and administrato r Igor Turashev, 38, from Yoshkar-Ola, Russia. The charges include conspiracy, computer hacking, wire fraud and bank fraud. The two men have not been arrested; their whereabouts are unknown. Russia and the U.S. do not have an extradition treaty.

The British agency called Evil Corp. "the world's most harmful cyber crime group" and posted pictures on Twitter of Yakubets with his customized Lamborghini sports car and his 2017 wedding, on which it said he'd spent more than $300,000. The State Department and the FBI are offering a $5 million reward for information leading to Yakubets' arrest and conviction, calling it the largest reward ever offered for an accused cybercriminal.

In a statement, Treasury officials also accused Yakubets of recruiting cybercriminals for Russia's government. According to the statement, he began working for FSB, a successor to the KGB spy agency, in 2017 and was tasked to work on projects including "acquiring confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf." The Treasury's press office would not elaborate on those projects.

Prosecutors say the charges filed Thursday stem from the creation of malware "Bugat" (also known as "Dridex" and "Kridex") that automates the theft of credentials used to log into banks and other financial institutions. It was typically delivered through phishing emails that tricked users into entering their personal information at fake online banking websites, investigators said. The online thieves would then make unauthorized withdrawals .

Yakubets, who used the online moniker "aqua," and Turashev are accused in the indictment of targeting two banks, a school district and four companies in Pennsylvania—a petroleum business, building supply company, vacuum and thin film deposition technology company and metal manufacturer—as well as a gun manufacturer.

The cybersecurity company FireEye said in an email that in the past year it has seen instances of Dridex infections being used not just for cybertheft but also for distribution of ransomware to infected machines.

"Today's announcement should make clear to those engaged in cybercrime that we will identify you, we will unmask you, and we will prosecute you, no matter how much effort it requires or how long it takes," said Assistant Attorney General Brian Benczkowski, who heads the Justice Department's criminal division.

Yakubets is also being charged in a separate case in Nebraska with conspiring to commit bank fraud in connection with other malware, authorities said.

Yakubets and his co-conspirators are alleged to have victimized 21 specific municipalities, banks, companies and nonprofit organizations in California, Illinois, Iowa, Kentucky, Maine, Massachusetts, New Mexico, North Carolina, Ohio, Texas, and Washington.

The case is not the first involving the cyberracketeering ring. Two co-conspirators of Yakubets, both Ukrainian nationals, were extradited after their 2014 indictment and pleaded guilty to conspiracy charges, investigators said.

Citation: Two Russians charged in 'Evil Corp' global cybertheft ring (2019, December 5)