Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware

home.treasury.gov/news/press-releases/sm845

December 5, 2019

Washington – Today the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) took action against Evil Corp, the Russia-based cybercriminal organization responsible for the development and distribution of the Dridex malware. Evil Corp has used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. This malicious software has caused millions of dollars of damage to U.S. and international financial institutions and their customers. Concurrent with OFAC's action, the Department of Justice charged two of Evil Corp's members with criminal violations, and the Department of State announced a reward for information up to $5 million leading to the capture or conviction of Evil Corp's leader. These U.S. actions were carried out in close coordination with the United Kingdom's National Crime Agency (NCA). Additionally, based on information obtained by the Treasury Department's Financial Crimes Enforcement Network (FinCEN), the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) released previously unreported indicators of compromise associated with the Dridex malware and its use against the financial services sector.

"Treasury is sanctioning Evil Corp as part of a sweeping action against one of the world's most prolific cybercriminal organizations. This coordinated action is intended to disrupt the massive phishing campaigns orchestrated by this Russian-based hacker group," said Steven

T. Mnuchin, Secretary of the Treasury. “OFAC’s action is part of a multiyear effort with key NATO allies, including the United Kingdom. Our goal is to shut down Evil Corp, deter the distribution of Dridex, target the “money mule” network used to transfer stolen funds, and ultimately to protect our citizens from the group’s criminal activities.”

Worldwide, cybercrime results in losses that total in the billions of dollars, while in the United States, financial institutions and other businesses remain prime targets for cybercriminals. Today’s action clarifies that, in addition to his involvement in financially motivated cybercrime, the group’s leader, Maksim Yakubets, also provides direct assistance to the Russian government’s malicious cyber efforts, highlighting the Russian government’s enlistment of cybercriminals for its own malicious purposes. Maksim Yakubets is not the first cybercriminal to be tied to the Russian government. In 2017, the Department of Justice indicted two Russian Federal Security Service (FSB) officers and their criminal conspirators for compromising millions of Yahoo email accounts. The United States Government will not tolerate this type of activity by another government or its proxies and will continue to hold all responsible parties accountable.

Today’s designations and indictments were issued in furtherance of previous international actions targeting Evil Corp in an effort to further disrupt and degrade the group’s ability to operate. In October 2015, the Department of Justice indicted Andrey Ghinkul for spreading the Dridex malware. At that same time, the Federal Bureau of Investigation and the NCA disrupted the global infrastructure utilized at the time by Evil Corp. Over the past several years, the NCA and the United Kingdom’s Metropolitan Police Service have arrested multiple individuals who enabled the activities of Evil Corp, including laundering stolen proceeds acquired through the Dridex malware.

As a result of today’s designations, all property and interests in property of these persons subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. Additionally, any entities 50 percent or more owned by one or more designated persons are also blocked. Foreign persons may be subject to secondary sanctions for knowingly facilitating a significant transaction or transactions with these designated persons.

Designation Targets

Today’s action targets 17 individuals and seven entities to include Evil Corp, its core cyber operators, multiple businesses associated with a group member, and financial facilitators utilized by the group. OFAC designated these persons pursuant to Executive Order (E.O.) 13694, as amended, which targets malicious cyber-enabled actors around the world, and as codified by the Countering America’s Adversaries Through Sanctions Act.


DRIDEX infection chain photo

Evil Corp is the Russia-based cybercriminal organization responsible for the development and distribution of the Dridex malware. The Dridex malware is a multifunctional malware package that is designed to automate the theft of confidential information, to include online banking credentials from infected computers. Dridex is traditionally spread through massive phishing email campaigns that seek to entice victims to click on malicious links or attachments embedded within the emails. Once a system is infected, Evil Corp uses compromised credentials to fraudulently transfer funds from victims' bank accounts to those of accounts controlled by the group. As of 2016, Evil Corp had harvested banking credentials from customers at approximately 300 banks and financial institutions in over 40 countries, making the group one of the main financial threats faced by businesses. In particular, Evil Corp heavily targets financial services sector organizations located in the United States and the United Kingdom. Through their use of the Dridex malware, Evil Corp has illicitly earned at least $100 million, though it is likely that the total of their illicit proceeds is significantly higher. As a result of this activity, Evil Corp is being designated pursuant to E.O. 13694, as amended, for engaging in cyber-enabled activities that have the effect of causing a significant misappropriation of funds or economic resources for private financial gain.

Evil Corp operates as a business run by a group of individuals based in Moscow, Russia, who have years of experience and well-developed, trusted relationships with each other. **Maksim Yakubets** (Yakubets) serves as Evil Corp's leader and is responsible for managing and supervising the group's malicious cyber activities. For example, as of 2017, Yakubets supervised Evil Corp actors who were attempting to target U.S. companies. As of 2015, Yakubets maintained control of the Dridex malware and was in direct communication with Andrey Ghinkul prior to the unsealing of his indictment. As a result, Yakubets is being designated pursuant to E.O. 13694, as amended, for having acted for or on behalf of and for providing material assistance to Evil Corp. Prior to serving in this leadership role for Evil Corp, Yakubets was also directly associated with Evgeniy Bogachev, a previously designated Russian cybercriminal responsible for the distribution of the Zeus, Jabber Zeus, and GameOver Zeus malware schemes. In particular, Yakubets was responsible for recruiting and managing a network of individuals responsible for facilitating the movement of money illicitly gained through the efforts spearheaded by Evgeniy Bogachev. Yakubets is the subject of an indictment and criminal complaint unsealed today by the Department of Justice, while the Department of State announced a $5 million reward for information leading to the capture of Yakubets.

In addition to his leadership role within Evil Corp, Yakubets has also provided direct assistance to the Russian government. As of 2017, Yakubets was working for the Russian FSB, one of Russia's leading intelligence organizations that was previously sanctioned pursuant to E.O. 13694, as amended, on December 28, 2016. As of April 2018, Yakubets was in the process of obtaining a license to work with Russian classified information from the FSB. As a result, Yakubets is also being designated pursuant to E.O. 13694, as amended,

for providing material assistance to the FSB. Additionally, as of 2017, Yakubets was tasked to work on projects for the Russian state, to include acquiring confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf.

Another key Evil Corp figure targeted today is **Igor Turashev** (Turashev). As of 2017, Turashev was involved in helping Evil Corp exploit victims' networks. As of 2015, Turashev served as an administrator for Yakubets and had control over the Dridex malware. As a result, Turashev is being designated pursuant to E.O. 13694, as amended, for having acted for or on behalf of and for providing material assistance to Evil Corp. Turashev is also the subject of an indictment unsealed today by the Department of Justice.

Denis Gusev (Gusev), a senior member of Evil Corp, is also being designated today for his active role in furthering Evil Corp's activities. As of 2017, Gusev was involved in helping Evil Corp move to a new office location and as of 2018, Gusev served as a financial facilitator for Evil Corp and its members. As a result, Gusev is being designated pursuant to E.O. 13694, as amended, for having acted for or on behalf of and for providing material assistance to Evil Corp.

Gusev also serves as the General Director for six Russia-based businesses. These entities include **Biznes-Stolitsa, OOO**, **Optima, OOO**, **Treid-Invest, OOO**, **TSAO, OOO**, **Vertikal, OOO**, and **Yunikom, OOO**. As a result, these entities are being designated pursuant to E.O. 13694, as amended, for being owned or controlled by Gusev.

In addition to Yakubets, Turashev, and Gusev, Evil Corp relies upon a cadre of core individuals to carry out critical logistical, technical, and financial functions such as managing the Dridex malware, supervising the operators seeking to target new victims, and laundering the proceeds derived from the group's activities. These additional core members of the group include **Dmitriy Smirnov**, **Artem Yakubets**, **Ivan Tuchkov**, **Andrey Plotnitskiy**, **Dmitriy Slobodskoy**, and **Kirill Slobodskoy**. As a result, these six individuals are being designated pursuant to E.O. 13694, as amended, for having acted for or on behalf of and for providing material assistance to Evil Corp.

To transfer the proceeds gained through their use of the Dridex malware, Evil Corp relies upon a network of money mules who are involved in transferring stolen funds obtained from victims' bank accounts to accounts controlled by members of Evil Corp. Previously, the NCA arrested multiple individuals in the United Kingdom suspected of laundering the criminal profits of cybercrime schemes, including those perpetrated by Evil Corp, through hundreds of accounts at various banks in the United Kingdom. Today, OFAC is designating eight Moscow-based individuals who have served as financial facilitators for Evil Corp. These individuals include **Aleksei Bashlikov**, **Ruslan Zamulko**, **David Guberman**, **Carlos Alvares**, **Georgios Manidis**, **Tatiana Shevchuk**, **Azamat Safarov**, and **Gulsara Burkhonova**. As a result, these eight individuals are being designated pursuant to E.O. 13694, as amended, for providing financial and material assistance to Evil Corp.

The Treasury Department's FinCEN and OCCIP announcement can be found here.

####

Use featured image

Off