Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data

⋮ 6/26/2024

Wednesday, June 26, 2024

For Immediate Release

Office of Public Affairs

Defendant is Alleged to Have Assisted with an Attack in Advance of Russia's February 2022 Invasion of Ukraine

Note: Concurrent with the return of the indictment, the U.S. Department of State's Rewards for Justice program is offering a reward of up to $10 million for information on Stigal's location or his malicious cyberactivity. Anyone possessing such information should contact Rewards for Justice here .

A federal grand jury in Maryland returned an indictment yesterday charging Amin Timovich Stigal (Амин Тимович Стигал), 22, a Russian citizen, with conspiracy to hack into and destroy computer systems and data. In advance of the full-scale Russian invasion of Ukraine, targets included Ukrainian Government systems and data with no military or defense-related roles. Later targets included computer systems in countries that were providing support to Ukraine, including the United States. Stigal remains at large.

"As alleged, the defendant conspired with Russian military intelligence on the eve of Russia's unjust and unprovoked invasion of Ukraine to launch cyberattacks targeting the Ukrainian government and later targeting its allies, including the United States." said Attorney General Merrick B. Garland. "The Justice Department will continue to stand with Ukraine on every front in its fight against Russia's war of aggression, including by holding accountable those who support Russia's malicious cyber activity."

"The GRU has repeatedly applied in cyberspace Russia's statecraft of indiscriminate destruction and intimidation," said Assistant Attorney General Matthew G. Olsen. "The Department will do its part to prevent and disrupt such malicious behavior that relies upon online services or infrastructure in the U.S., or that targets U.S. victims. We will also identify, pursue, and eventually hold to account those responsible for Russia's malicious actions, including the cybercriminals that the Russian government cultivates in furtherance of its malign agenda."

"Amin Timovich Stigal attempted to leverage malware to aid the Russian military in the invasion of Ukraine," said FBI Deputy Director Paul Abbate. "Today's indictment demonstrates the FBI's unwavering commitment to combat malicious cyber activities by our adversaries, and we will continue to work with our international partners to thwart attempts to undermine and harm our allies."

“Malicious cyber actors who attack our allies should know that we will pursue them to the full extent of the law,” said U.S. Attorney Erek L. Barron for the District of Maryland. “Cyber intrusion schemes such as the one alleged threaten our national security, and we will use all the technologies and investigative measures at our disposal to disrupt and track down these cybercriminals.”

“The indictment of Amin Stigal is yet another example of the FBI’s commitment to combating cyber threats both at home and internationally,” said Special Agent in Charge William J. DelBagno of the FBI Baltimore Field Office. “To those adversaries who seek to compromise our international partners’ systems, know you will be identified and you will face consequences for your actions. The FBI vows to continually pursue justice and disrupt malicious cyber actors.”

According to court documents, in Jan. 2022, Stigal and members of the Main Intelligence Directorate of the General Staff (GRU) of the Russian Federation (the Conspirators) conspired to use a U.S.-based company’s services to distribute malware known in the cybersecurity community as “WhisperGate” to dozens of Ukrainian government entities’ computer systems and destroy those systems and related data in advance of the Russian invasion of Ukraine. The United States government previously joined with allies and partners in May 2022 to attribute this cyber-attack to the Russian military and to condemn the attack and similar destructive cyber activities against Ukraine.

On Jan. 13, 2022, the Conspirators attacked multiple Ukrainian government networks, including the Ukrainian Ministry of International Affairs, the State Treasury, the Judiciary Administration, the State Portal for Digital Services, the Ministry of Education and Science, the Ministry of Agriculture, the State Service for Food Safety and Consumer Protection, the Ministry of Energy, the Accounting Chamber for Ukraine, the State Emergency Service, the State Forestry Agency, and the Motor Insurance Bureau. The Conspirators infected computers on these and other networks with malware called WhisperGate, which was designed to look like ransomware. However, as the indictment alleges, WhisperGate was actually a cyberweapon designed to completely destroy the target computer and related data.

In conjunction with these attacks, the Conspirators compromised several of the targeted Ukrainian computer systems, exfiltrated sensitive data, including patient health records, and defaced the websites to read: “Ukrainians! All information about you has become public, be afraid and expect the worst. This is for your past, present and future.” That same day, the Conspirators offered the hacked data for sale on the internet. The effort was aimed at sowing concern among the broader Ukrainian population regarding the safety of government systems and data.

In August 2022, the Conspirators also hacked the transportation infrastructure of a Central European country that was supporting Ukraine. The indictment further alleges that from Aug. 5, 2021, through Feb. 3, 2022, the Conspirators leveraged the same computer infrastructure they used in the Ukraine-related attacks to probe computers belonging to a federal government agency in Maryland in the same manner as they had initially probed the Ukrainian Government networks.

If convicted, Stigal faces a maximum penalty of five years in prison. A federal district court judge will determine any sentence after taking into account the U.S. Sentencing Guidelines and other statutory factors.

The FBI’s Baltimore Field Office is investigating the case with the support of the FBI’s Milwaukee and Boston Field Offices.

Assistant U.S. Attorneys Aaron S.J. Zelinsky and Robert I. Goldaris for the District of Maryland are prosecuting the case, with valuable assistance from the National Security Division's National Security Cyber Section.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Indictment

Updated June 28, 2024

Press Release Number: 24-815