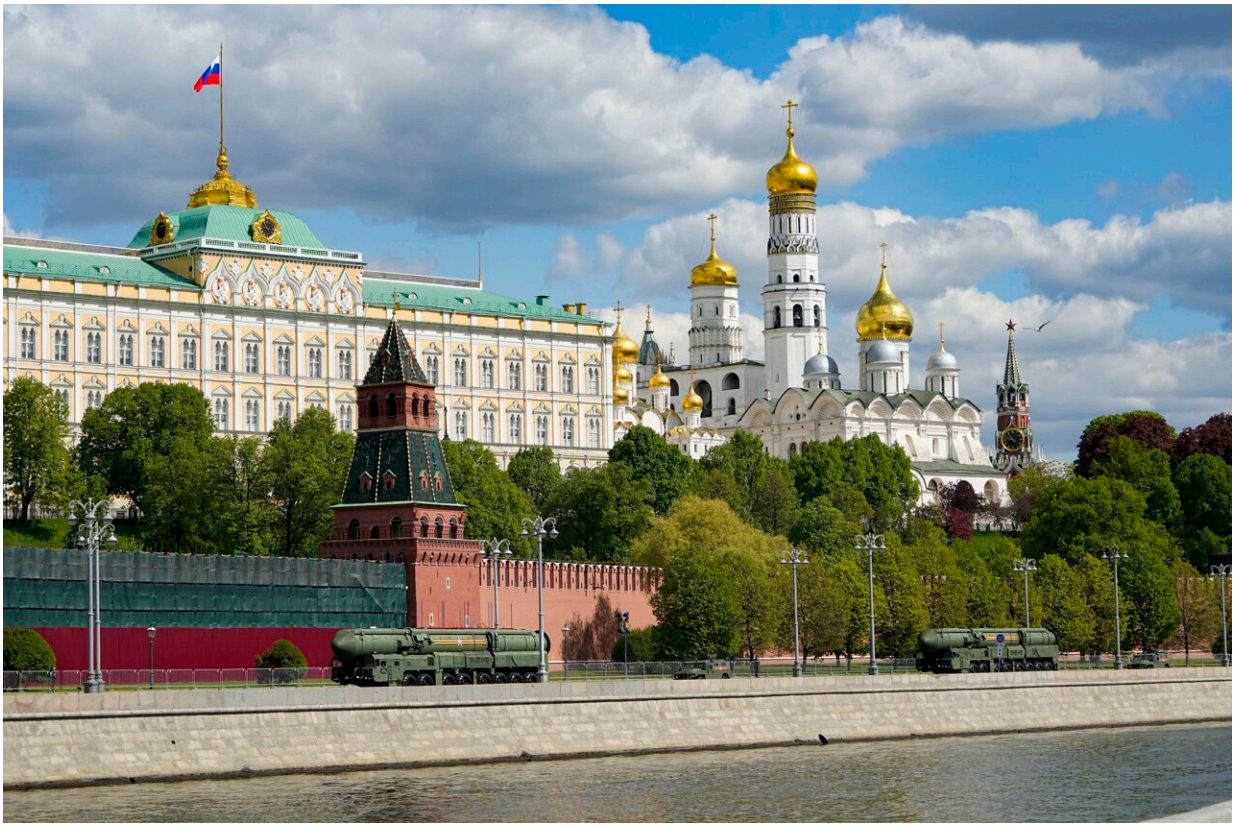
US busts Russian cyber operation in dozens of countries

May 9 2023, by Eric Tucker



Russian RS-24 Yars ballistic missiles drive along the embankment next to the Kremlin wall after the Victory Day military parade in Moscow, Russia, Tuesday, May 9, 2023, marking the 78th anniversary of the end of World War II. Credit: AP Photo/Alexander Zemlianichenko

The Justice Department said Tuesday that it had disrupted a long-

running Russian cyberespionage campaign that stole sensitive information from computer networks in dozens of countries, including the U.S. and other NATO members.

Prosecutors linked the spying operation to a unit of Russia's Federal Security Service, or FSB, and accused the hackers of stealing documents from hundreds of computer systems belonging to governments of NATO members, an unidentified journalist for a U.S. news organization who reported on Russia, and other select targets of interest to the Kremlin.

"For 20 years, the FSB has relied on the Snake malware to conduct cyberespionage against the United States and our allies—that ends today," Assistant Attorney General Matthew Olsen, the head of the Justice Department's National Security Division, said in a statement.

The specific targets were not named in court papers, but U.S. officials described the espionage campaign as "consequential," having successfully exfiltrated sensitive documents from NATO countries and also targeted U.S. government agencies and others in the U.S.

The Russian operation relied on the malicious software known as Snake to infect computers, with hackers operating from what the Justice Department said was a known FSB facility in Ryazan, Russia.

U.S. officials said they'd been investigating Snake for about a decade and came to regard it as the most sophisticated malware implant relied on by the Russian government for espionage campaigns. They said Turla, the FSB unit believed responsible for the malware, had refined and revised it multiple times as a way to avoid being shut down.

The Justice Department, using a warrant this week from a federal judge in Brooklyn, launched what it said was a high-tech operation using a specialized tool called Perseus that caused the malware to effectively self-

destruct. Federal officials said they were confident that, based on the impact of its operation this week, the FSB would not be able to reconstitute the malware implant.

Citation: US busts Russian cyber operation in dozens of countries (2023, May 9) retrieved 5 May 2024 from https://techxplore.com/news/2023-05-russian-cyber-dozens-countries.html