The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia-Linked Hacking Groups Targeting the U.S.: What You Need to Know

July 13, 2021



The cyberattacks are now a major point of contention in already strained ties between Washington and Moscow. **defense.gov**

Russia-based hacker groups have been accused of massive ransomware attacks on major U.S. businesses and government agencies in the past year.

The attacks, which have breached U.S. government agencies in addition to private enterprises, are now a major point of contention in already strained ties between Washington and Moscow, with U.S. President Joe Biden's administration repeatedly warning the Kremlin regarding its alleged links to cybercriminal groups.

Ransomware attacks involve hackers infiltrating a computer network, "kidnapping" an organization's files and threatening to publish or delete them if a large ransom isn't paid. Former British intelligence cyber chief Marcus Willett has called the ransomware scourge "arguably more strategically damaging than state cyberspying."

Here's an overview of who is behind the hacks, why the U.S. is worried and how the

cybercriminals have been linked to the Kremlin:

Colonial Pipeline hack

The **DarkSide** criminal hacking group rose to notoriety following its attack on the **Colonial Pipeline**, a major U.S. fuel pipeline, which disrupted fuel distribution along the southeastern U.S.

DarkSide is believed to be based in Russia but Biden has said U.S. intelligence has no evidence that their work is state-sponsored.

On May 7, Colonial Pipeline reported to the FBI that its computer network was compromised by a hacker group called DarkSide and that it had received and paid a ransom demand of approximately 75 bitcoins.

Last month, the U.S. Justice Department announced that it had seized 63.7 bitcoins currently valued at approximately $2.3 million that had been paid to DarkSide as ransom.

According to Gemini Advisory analytics, the DarkSide group are regarded as prolific professionals in their field and even possess their own code of ethics and customer service, serving as an intermediary by providing services and assistance to other hackers.

DarkSide later announced that it was shutting down, citing pressure from the U.S., but The New York Times cited cybersecurity experts as saying that the announcement may be a ruse.

JBS and Kaseya hacks

The FBI has linked Russia-based hacker group **REvil** to the cyberattack on **JBS**, the world's biggest meat processor which ended up paying an $11 million ransom.

The JBS attack took place within three weeks of the Colonial Pipeline attack, exposing vulnerabilities in the systems of U.S. corporations and government agencies.

REvil has also been linked to the massive cyber attack on U.S. software company Kaseya, which serves over 40,000 customers in the U.S. and worldwide.

REvil demanded $70 million in ransom following the Kaseya hack, which affected an estimated 1,500 businesses.

SolarWinds hack

A Russia-based group called **Nobelium** has been linked to the massive 2020 **SolarWinds** hack that compromised about 100 U.S. companies — including Microsoft, Intel and Cisco — in addition to a dozen government agencies including the Treasury, Justice and Energy departments and the Pentagon.

Washington has accused Russia of orchestrating the online assault, explicitly citing its Foreign Intelligence Service (SVR).

SolarWinds CEO Sudhakar Ramakrishna told NPR in April that the scale of the cyberattack was

unprecedented as about 18,000 customers who downloaded the SolarWinds software update had their information compromised.

In May, Microsoft reported a series of phishing attempts launched by Nobelium. A security update from Microsoft said that Nobelium has stepped up attacks, notably targeting government agencies involved in foreign policy as part of intelligence-gathering efforts.

How are they linked to the Kremlin?

The U.S. Treasury Department has accused Russia's intelligence services of cultivating and co-opting cybercriminals. U.S. intelligence agencies believe that Russian-speaking cybercriminals are shielded and often employed by the Russian government.

The hacker groups operate within the Russian-speaking ecosystem and remain wary of Western intelligence services infiltrating their forums, The Washington Post reported.

Cybersecurity experts say that the Kremlin grants tacit approval to cybercriminals on Russian territory as long as they don't target Russia or its allies, protecting them from prosecution.

In response to U.S. pressure to punish the hackers, Russian President Vladimir Putin said in 2016 that if hackers "did not break Russian law, there is nothing to prosecute them for in Russia."

What are the broader international implications?

Since taking office in January, Biden has repeatedly called on Moscow to take responsibility for the cyber attacks, warning that if the Kremlin does not take action, the U.S. will. At their June 16 summit in Geneva, Biden presented President Vladimir Putin with a list of 16 areas of critical infrastructure that "should be off limits" to Russian cyberattacks.

Moscow denies any association with the hacking groups and has responded to questions on Russia's alleged harboring of cybercriminals by accusing the U.S. of the same.

In April, the U.S. slapped Russia with new sanctions in response to malicious cyber activities, accusing Russia's intelligence services of being behind the SolarWinds hack.

In May, DarkSide announced that it had lost control of its servers a day after Biden announced U.S. plans to disrupt the hackers behind the Colonial Pipeline cyberattack.

Russia's Constitution forbids the extradition of its own citizens to other countries, an issue that has forced American authorities to arrest suspected hackers once they exit Russia's borders.

Original url:
https://www.themoscowtimes.com/2021/07/13/russia-linked-hacking-groups-targeting-the-us-what-you-need-to-know-a74505