New American

Written by **Veronika Kyrylenko** on May 28, 2021

Microsoft: USAID Breach Signals Return of Russian Hackers Behind 2020 SolarWinds Attack

The hacker group Nobelium, which was behind the massive 2020 SolarWinds attack, is currently trying to access the e-mail systems of thousands in Western governments, think tanks, and NGOs, according to a statement released Thursday by Microsoft.

Nobelium, which is widely believed to be run by Russia's Foreign Intelligence Service, or SVR, have targeted roughly 3,000 e-mail accounts at more than 150 organizations in 24 countries, according to Microsoft. The hacking attempts were first identified in January of this year but have been ongoing, according to the tech company.

Six wanted Russian military intelligence officers is displayed before a news conference at the Department of Justice in 2020 /AP Images

At least a quarter of the targeted organizations are involved in international development, and humanitarian and human rights work, said Tom Burt, Microsoft's corporate vice president of customer security and trust. The attacks were launched by gaining access to the e-mail marketing account of the U.S. Agency for International Development (USAID), which falls under the State Department.

"Nobelium," Burt said, "accessed the USAID's account with Constant Contact, a mass-mailing service."

In an e-mailed statement, a spokesperson for Constant Contact said that the compromise of USAID's account on its platform was "an isolated incident" and that the company has temporarily disabled accounts that may have been impacted.

On Wednesday, e-mails were sent to various companies and users that looked to be from the USAID, including some that read "special alert" and "Donald Trump has published new documents on election fraud," Microsoft said. If users click the link, a malicious file gets installed in their system that allows Nobelium access to the compromised machines.

"These attacks appear to be a continuation of multiple efforts by Nobelium to target government agencies involved in foreign policy as part of intelligence gathering efforts," Burt said.

"By piggybacking on software updates and now mass email providers," the company wrote, the Russian hackers increased "the chances of collateral damage in espionage operations and undermines trust in the technology ecosystem."

Microsoft did not say whether or how many attempts were successful. It said many e-mails in the high-volume campaign would have been blocked by automated systems.

The White House says it is "aware of the incident" that impacted USAID and is "monitoring the situation closely" — but noted that so far, the impact "appears to be limited."

The attack comes a month after the U.S. government explicitly said that the SolarWinds hack was

carried out by SVR, a successor to the foreign spying operations of the Soviet KGB. The accusation was laughed off and mocked by SVR's director Sergei Naryshkinan just three weeks after the Colonial Pipeline cyberattack was allegedly carried out by the DarkSide hacker group in Russia.

Michael Orlando, acting director of the National Counterintelligence and Security Center says that the countries such as Russia, China, and Iran create safe havens for criminal hackers, since the corrupt governments do nothing to stop them as long as hackers target their adversaries.

President Biden insisted Russian officials have "some responsibility to deal with this [cyberattack]," seeming to take an aggressive stance against Russia's malicious actions.

In April, the Biden administration announced a sweeping series of sanctions against Russia over election interference, cyber hacking, and other "harmful foreign activities," such as Russia offering "bounties" for Taliban attacks against U.S. troops.

"I was clear with president Putin that we could have gone further, but I chose not to do so, I chose to be proportionate," Biden added, implying the possibility of further sanctions.

Biden decisively claimed "I made it clear to President Putin, in a manner very different from my predecessor, that the days of the United States rolling over in the face of Russia's aggressive actions — interfering with our election, cyber attacks, poisoning its citizens — are over," and later called Putin "killer."

Despite the loud words, Biden's handling of the Colonial Pipeline cyberattack turned out to be toothless. Instead of punishing the hackers who disrupted the work of the major U.S. pipeline and caused gas shortages across the whole East Coast, Biden distanced himself from the situation, allowing the hackers to get $4.4 million richer by collecting a ransom from the U.S. company, which is believed to encourage future attacks.

Meanwhile, Russia denies its involvement in the attack on Microsoft. The Kremlin's spokesman Dmitry Peskov on Friday said the allegations from Microsoft were "unfounded" and "abstract."

"It's an abstract statement. It's like if we said we believe a large threat is coming from Microsoft and the software. It will be the same unfounded accusation," Peskov said in a daily briefing call with reporters.

When asked if the incident would affect the scheduled Geneva summit on June 16 between Biden and Putin, Peskov replied: "It doesn't seem so to us."

Despite the newly introduced sanctions, and Biden's show-offish bravado, the Kremlin seems not to be threatened by them, meaning the cyberattacks from its jurisdiction will likely continue.