3-CNBC-Russian hackers launch major cyberattack

TechCheck

The Russian hackers thought to be behind the catastrophic SolarWinds attack last year have launched another major cyberattack, Microsoft warned three weeks before President Joe Biden is to meet with Russian President Vladimir Putin.

Microsoft said in a blog post Thursday that the hacking group, known as Nobelium, had targeted over 150 organizations worldwide in the last week, including government agencies, think tanks, consultants and nongovernmental organizations.

They sent phishing emails — spoof messages designed to trick people into handing over sensitive information or downloading harmful software — to more than 3,000 email accounts, the tech giant said.

At least 25% of the targeted organizations are involved in international development, humanitarian and human rights work, said Tom Burt, Microsoft's corporate vice president of customer security and trust.

"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.

Organizations in at least 24 countries were targeted, Microsoft said, with the U.S. receiving the largest share of attacks.

The breach has been discovered three weeks before the Biden-Putin summit in Geneva on June 16.

It also comes a month after the U.S. government explicitly said that the SolarWinds hack was carried out by Russia's SVR, a successor to the

foreign spying operations of the Soviet KGB.

The Kremlin said Friday it does not have any information on the cyberattack and that Microsoft needs to answer more questions, including how the attack is linked to Russia, Reuters reported. The Kremlin did not immediately respond to CNBC's request for comment.

The hack explained

Microsoft said Nobelium gained access to an email marketing account used by the U.S Agency for International Development, the federal government's aid agency. The account is held on a platform called Constant Contact.

Zoom In Icon

Arrows pointing outwards

Burt said Nobelium used the account to "distribute phishing emails that looked authentic but included a link that, when clicked, inserted a malicious file."

The file contains a backdoor that Microsoft calls NativeZone, which can "enable a wide range of activities from stealing data to infecting other computers on a network," according to Burt, who said Microsoft is in the process of notifying customers who have been targeted. *[Rebuild]*

USAID said a forensic investigation into the breach is ongoing.

"The U.S. Agency for International Development became aware of potentially malicious email activity from a compromised Constant Contact email marketing account," a USAID spokesperson said in a statement shared with CNBC. "The forensic investigation into this security incident is ongoing. USAID has notified and is working with all appropriate Federal authorities, including the U.S. Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency."

A spokesperson for Constant Contact told CNBC the company is aware that the account credentials of one its customers were compromised and used by

a malicious actor to access the customer's Constant Contact accounts.

"This is an isolated incident, and we have temporarily disabled the impacted accounts while we work in cooperation with our customer, who is working with law enforcement," they said.

A CISA spokesperson told CNBC the agency is aware of the the potential compromise and that it was working with the FBI and USAID to better understand the extent of what's happened.

Steve Forbes, a government cybersecurity expert at domain name manager Nominet, outlined the dangers of these types of hacks.

"Phishing attacks are essentially a numbers game and the attackers are playing the odds," he said in a statement. "If they target 3,000 accounts, it only takes one employee to click on the link to establish a backdoor for the hackers in a government organization."

The SolarWinds attack, uncovered in December, turned out to be much worse than first expected. It gave the hackers access to thousands of companies and government offices that used SolarWinds IT software.

Microsoft President Brad Smith described that attack as "the largest and most sophisticated attack the world has ever seen."

Earlier this month, Russia's spy chief denied responsibility for the SolarWinds cyberattack but said he was "flattered" by the accusations from the U.S and the U.K. that Russian foreign intelligence was behind such a sophisticated hack.