4-CNET-Microsoft warns that Russian

Featured Politics Social Media Privacy Misinformation

Microsoft warns that Russian hackers used US agency to mount huge cyberattack

Hackers behind the SolarWinds attack gained access to the email system of a US aid agency, says Microsoft.

Carrie Mihalcik

May 28, 2021 2:47 p.m. PT

Carrie Mihalcik

Senior Editor / News

Carrie Mihalcik has lived on both coasts and can definitively say that Chesapeake Bay blue crabs are the best. She's been reporting and editing for more than a decade, including at the National Journal in Washington, DC, and CurrentTV in San Francisco. She's currently a Senior Editor at CNET focused on breaking news.

See full bio

James Martin/CNET

Microsoft has disclosed a widescale cyberattack it says is operated by hackers linked to Russian intelligence, the same ones behind the SolarWinds hack . The hackers gained access to an email system used by the US Agency for International Development, a State Department agency focused on foreign aid, and sent malicious emails to "around 3,000

individual accounts across more than 150 organizations," according to a threat alert Microsoft sent Thursday.

The hackers appeared to target "many humanitarian and human rights organizations," Tom Burt, a vice president at Microsoft, said in a post Thursday . Organizations in the US received the largest share of attacks, but Burt noted that targeted victims spanned at least 24 countries.

Some of the malicious emails were sent as recently as this week, and Microsoft said attacks may be ongoing. The attacks appear to be a continuation of efforts by Russian hackers to "target government agencies involved in foreign policy as part of intelligence gathering efforts," Burt said.

Related stories

Colonial Pipeline, post-hack: US issues new cybersecurity regulations

This newly disclosed cyberattack comes just over a month after the US officially imposed sanctions against Russia for alleged election interference and malicious cyberactivity, including the widespread SolarWinds hack . Key intelligence agencies had already said Russia was the likely origin of the SolarWinds hack, which used tainted software from IT management company SolarWinds to penetrate multiple US federal agencies and at least 100 private companies.

In an interview with CNN on Friday, Defense Secretary Lloyd Austin said the US has a "number of offensive options" to respond to cyberattacks, though he didn't specifically refer to this latest attack.

"The cyber domain is really important, it is a part … of the battlespace, it's a part of the architecture, something that we have to not only pay attention to, but we have to be dominant in," Austin told CNN.

USAID spokesperson Pooja Jhunjhunwala said the agency is "aware of potentially malicious email activity from a compromised Constant Contact email marketing account," adding that a "forensic investigation" into the incident is ongoing.

A spokesperson for the US Cybersecurity and Infrastructure Security Agency said that CISA is working with “the FBI and USAID to better understand the extent of the compromise and assist potential victims.”

Phishing emails that looked authentic

Microsoft said it had been tracking this new hacking campaign since January 2021 but that the situation escalated significantly on Tuesday when hackers “leveraged the legitimate mass-mailing service, Constant Contact, to masquerade as a US-based development organization and distribute malicious URLs to a wide variety of organizations and industry verticals.” Due to the high volume of malicious emails sent, some might have been caught by spam filters but others likely made it past automated systems to the intended inboxes, Microsoft said.

If a person clicked on the link in the email, it would upload a malicious file that could give the hackers “persistent access to compromised systems,” according to Microsoft. This could potentially allow for the hackers to “conduct action-on objectives, such as lateral movement, data exfiltration, and delivery of additional malware.”

When reached for comment, a spokesperson for Constant Contact told CNET that the company has disabled impacted accounts.

“We are aware that the account credentials of one of our 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,” the spokesperson said.

Neither the White House nor the Russian embassy in Washington responded to requests for comment.

An example of the malicious emails sent by hackers that appeared in an alert from USAID.

Microsoft

Get the CNET Home newsletter

Modernize your home with the latest news on smart home products and trends. Delivered Tuesdays and Thursdays.