Related news

cyberscoop.com/russia-espionage-europe-human-rights/

June 1, 2021

government

Ex-US ambassador, anti-corruption activists in Ukraine were targets of suspected Russian phishing

An observer from the Organization for Security and Co-operation in Europe (OSCE) is seen at a demonstration in Odessa, Ukraine, on May 2. An OSCE employee is among the recent possible hacking targets of suspected Russian spies. (Photo by Pierre Crom/Getty Images)
Written by Sean Lyngaas
Jun 1, 2021 | CYBERSCOOP
An ex-U.S. ambassador to Russia, anti-corruption activists in Ukraine and election observers in other parts of Eastern Europe were among the apparent targets of a suspected Russian state-sponsored hacking effort, according to data linked to the spying operation that a researcher shared with CyberScoop.

The list offers classic examples of organizations that Russian spies might want to infiltrate, including those working to expose graft, combat disinformation and promote secure elections. It also points to the persistent threats that small nonprofits face from well-resourced hackers, as well as the long-running alleged Russian efforts to undermine democratic institutions.

Microsoft on May 27 said hackers had used a breached account belonging to the U.S. Agency for International Development, a U.S. government agency, to send phishing emails to some 3,000 email accounts at 150 organizations in 24 countries (U.S. officials estimated an even broader set of targets: 7,000 accounts and 350 organizations.)

Microsoft blamed the same Russian hacking group that exploited SolarWinds software to breach U.S. government agencies — a group the White House has tied to Russia's SVR foreign intelligence agency.

The U.S. government says it is still investigating the campaign impersonating USAID and has yet to attribute the activity to a known group. Neither Microsoft nor U.S. officials named the targets of the campaign.

Multiple employees at the Anti-Corruption Action Centre (AntAC), a non-governmental organization that campaigns against corruption in Ukraine's government, received phishing emails, but none clicked on the malicious code, according to co-founder Vitaliy Shabunin.

AntAC is among "those who are pushing Ukraine out of the Russian sphere of influence," Shabunin said by phone from Kyiv, Ukraine's capital. "We are pushing these [democratic] reforms to be part of the Western world."

"It's understandable for me why Russians would want to spy on us," he said.

It is also just one organization targeted in a would-be digital dragnet.

By plugging files used in the hacking campaign to VirusTotal, a platform for analyzing malicious code, Joe Slowik, a senior manager at security firm Gigamon, found email addresses associated with the service that the attackers used to track the phishing emails. Three other intelligence analysts corroborated Slowik's findings.

Among the apparent intended recipients of the phishing campaign was Alexander "Sandy" Vershbow, who was the deputy secretary general of North Atlantic Treaty Organization from 2012 to 2016 and the U.S. ambassador to Russia from 2001 to 2005. Russia sees NATO as a threat to its interests in Europe, and has allegedly used influence operations and hacking to try to undermine the bloc.

Vershbow, now a fellow at the Atlantic Council think tank, did not respond to a request for comment. The Atlantic Council declined to comment.

Another apparent target of the hackers was an employee of the Organization for Security and Cooperation in Europe (OSCE), an inter-government organization that works on arms control and police reform in former Soviet and Eastern Bloc countries. An OSCE spokesperson said the organization was aware of the phishing attempts and was closely monitoring the situation.

“Like many international organizations, the OSCE is a frequent target of cyber threats. It takes such incidents very seriously,” the statement continued. “The OSCE takes all possible measures to respond to and mitigate such attacks to protect all parts of the Organization.”

EU DisinfoLab, a Brussels-based nonprofit that pushed back on alleged Russian disinformation activity around the coronavirus vaccine, was also an intended recipient of the phishing emails, according to the Virus Total data. Alexandre Alaphilippe, EU DisinfoLab’s executive director, declined to comment.

The Department of Homeland Security’s cyber division said May 29 that it had yet to see “significant impact on federal government agencies” from the phishing campaign, while Microsoft said May 28 there wasn’t evidence of “any significant number of compromised organizations at this time.” The Justice Department on May 28 seized two internet domains that, the department said, the hackers were using to distribute and control their malicious code.

The seizure “was aimed at disrupting the malicious actors’ follow-on exploitation of victims, as well as identifying compromised victims,” the Justice Department said in a press release. “However, the actors may have deployed additional backdoor accesses between the time of the initial compromises and last week’s seizures.”

Russian government officials routinely deny involvement in hacking operations, including the campaign that exploited software made by U.S. federal contractor SolarWinds.

For Shabunin, though, it is familiar territory.

“We are pretty aware of such kinds of threats, and we have training all the time and the protocols to deal with them,” said Shabunin, whose house was burned down last year in apparent retaliation for his anti-corruption work.

Shabunin wants other NGOs to be vigilant. He said the phishing lure sent by the hackers, which referenced conspiracy theories pushed by former President Donald Trump, would be bizarre coming from USAID. The agency funds some of AntAC’s work, but doesn’t dabble in partisan politics.

Some U.S. lawmakers reacted with anger to the latest alleged Russian hacking, with the House Intelligence Committee chairman floating the idea of tightening sanctions. But the apparent target list reflects the type of Russian spying that has been going on for decades rather than any sort of escalation in cyberspace with the Biden administration. It also shows that U.S. officials have to be wary of Russian espionage long after they've left public service.

As for Shabunin, his organization is busy preparing to host a conference next week on disinformation threats to democracy with the presidents of Ukraine and Moldova.

"It's part of [the] job," Shabunin said of dealing with cyberthreats.