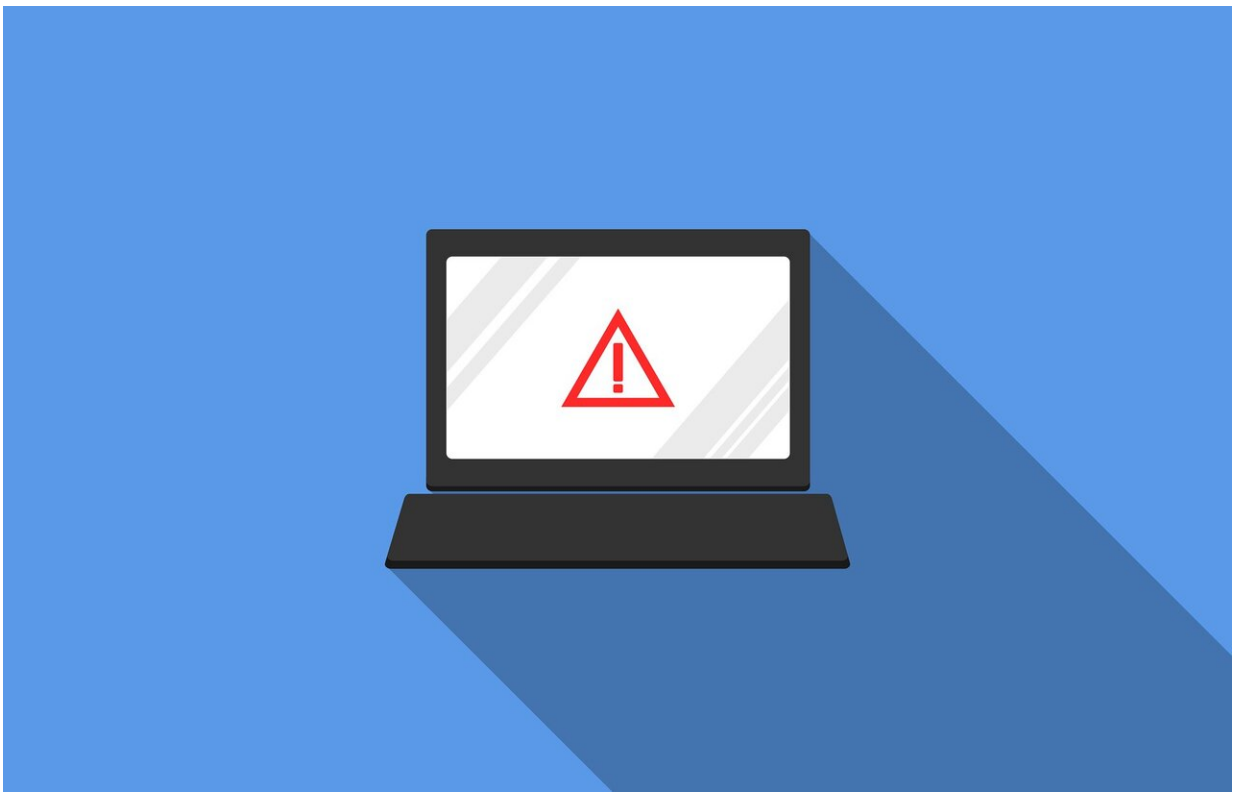
Microsoft, Samsung, Okta 'hacked'. Are these the Russian cyberattacks we were warned about?

March 24 2022, by Amanda Pérez Pintado



Credit: Pixabay/CC0 Public Domain

Shortly after President Joe Biden warned of possible Russian cyberattacks, a group of hackers this week made news after targeting

Microsoft and authentication service provider Okta.

But experts cautioned against linking the incident with Russia and the ongoing war with Ukraine.

"Obviously, if you just look at timing, you can be suspicious of it, but we don't see any direct links between these individual incidents, from Okta to Microsoft, and Russia," said Rick Holland, chief information security officer at the security firm Digital Shadows. "It's evolving, and things could change."

The group behind this week's attacks, Lapsus$, seemingly emerged in Dec. 2021 and began by focusing on Portuguese-language and South American organizations, Holland said.

Lapsus$ has since moved on to global targets including Nvidia and Samsung.

Microsoft said in a blog post Wednesday that the hackers gained limited access to its system through a single account. The company said "no customer code or data was involved in the observed activities."

Okta, meanwhile, said in a statement that about 2.5% of its costumers may have had their information viewed or acted upon after the company had denied it had been breached.

Holland said that, while high-profile targets like Microsoft and Okta may get widespread attention, they're "only a drop in the bucket."

"Sometimes, with some of the extortion crews, they never become public because the extortion actors are dealing with the companies directly," Holland said.

Small businesses are more vulnerable to ransomware, as they have less staffing and resources to counter cyberattacks.

Bracing for "destructive" Russian cyberattacks

On Monday, Biden again alerted Russia may be preparing to launch cyberattacks in response to the economic sanctions imposed on Moscow by the U.S. He urged the private sector to " "harden your cyber defenses."

"The magnitude of Russia's cyber capacity is fairly consequential and it's coming," Biden said at the Business Roundtable Quarterly Meeting in Washington.

Russian cyberattacks against the country may be "destructive," said John Bambenek, principal threat hunter at the firm Netenrich.

"If they launched attacks, they're going to be disruptive in nature, knocking things offline, knocking critical infrastructure offline," Bambenek said.

He said Russian attacks may target critical infrastructure like oil production or food supply chains, noting that last year, a group believed to be based in Russia forced the temporary shutdown of the Colonial Pipeline.

"That was ransomware, but at the end of the day, it's like knocking important pieces of critical infrastructure offline that creates large scale disruption," Bambenek said, referring to the Colonial Pipeline hack.

Holland, meanwhile, said the most significant threat companies should worry about is extortion.

"Certain companies need to worry about intellectual property theft and things along those lines," Holland said. "But generally speaking, extortion is at the top of every company's threat model."

The White House said in a statement that much of the country's critical infrastructure "is owned and operated by the private sector" and encouraged businesses to take steps like using multi-factor authentication, and backing up and encrypting data "to protect the critical services on which all Americans rely."