Microsoft: Russian-backed hackers targeting cloud services

25 October 2021, by Alan Suderman

Credit: CC0 Public Domain

Microsoft said Monday the same Russia-backed hackers responsible for the 2020 SolarWinds breach continue to attack the global technology supply chain and have been relentlessly targeting cloud service companies and others since summer.

The group, which Microsoft calls Nobelium, has employed a new strategy to piggyback on the direct access that cloud service resellers have to their customers' IT systems, hoping to "more easily impersonate an organization's trusted technology partner to gain access to their downstream customers." Resellers act as intermediaries between giant cloud companies and their ultimate customers, managing and customizing accounts.

"Fortunately, we have discovered this campaign during its early stages, and we are sharing these developments to help cloud service resellers, technology providers, and their customers take timely steps to help ensure Nobelium is not more successful," Tom Burt, a Microsoft vice president, said in a blog post.

The Biden administration downplayed Microsoft's announcement. A U.S. government official briefed on the issue who insisted on anonymity to discuss the government's response noted that "the activities described were unsophisticated password spray and phishing, run-of-the mill operations for the purpose of surveillance that we already know are attempted every day by Russia and other foreign governments."

The Russian Embassy did not immediately reply to a request for comment.

U.S. and Russian ties have already been strained this year over a string of high-profile ransomware attacks against U.S. targets launched by Russia-based cyber gangs. U.S. President Joe Biden has warned to Russian President Vladimir Putin to get him to crack down on ransomware criminals, but several top administration cybersecurity officials have said recently that they have seen no evidence of that.

Supply chain attacks allow hackers to steal information from multiple targets by breaking into a single product they all use. The U.S. government has previously blamed Russia's SVR foreign intelligence agency for the SolarWinds hack, a supply-chain hack which went undetected for most of 2020, compromised several federal agencies and badly embarrassing Washington.

The hacking campaign is called SolarWinds after the U.S. software company whose product was used in that effort. The Biden administration in April placed new sanctions against six Russian companies that support the country's cyber efforts in response to the SolarWinds hack.

Microsoft has been observing Nobelium's latest campaign since May and has notified more than 140 companies targeted by the group, with as many as 14 believed to have been compromised. The attacks have been increasingly relentless since July, with Microsoft noting that it had informed 609

customers that they had been attacked 22,868 times by Nobelium, with a success rate in the low single digits. That's more attacks than Microsoft had flagged from all nation-state actors in the previous three years.

"Russia is trying to gain long-term, systematic access to a variety of points in the technology supply chain and establish a mechanism for surveilling – now or in the future – targets of interest to the Russian government," Burt said.

Microsoft did not name any of the hackers' targets in their latest campaign. But cybersecurity firm Mandiant said it had seen victims in both Europe and North America.

Mandiant Chief Technology Officer Charles Carmakal said the hackers' method of going after resellers make detection difficult.

"It shifts the initial intrusion away from the ultimate targets, which in some situations are organizations with more mature cyber defenses, to smaller technology partners with less mature cyber defenses," he said.