Microsoft warns Russian, Chinese and Iranian hackers targeting US election 2020

11/09/2020 18:13 by admin

Most of the hacking attempts by Russian, Chinese and Iranian agents were halted by Microsoft security software and the targets notified, he said. The company would not comment on who may have been successfully hacked or the impact.

Microsoft: Russian, Chinese and Iranian hackers targeting US election 2020

Boston: The same Russian military intelligence outfit that hacked the Democrats in 2016 has renewed vigorous U.S. election-related targeting, trying to breach computers at more than 200 organizations including political campaigns and their consultants, Microsoft said Thursday.

The intrusion attempts reflect a stepped-up effort to infiltrate the U.S. political establishment, the company said. â€œWhat weâ€™ve seen is consistent with previous attack patterns that not only target candidates and campaign staffers but also those who they consult on key issues,â€• Tom Burt, a Microsoft vice president, said in a blog post. U.K. and European political groups were also probed, he added.

Most of the hacking attempts by Russian, Chinese and Iranian agents were halted by Microsoft security software and the targets notified, he said. The company would not comment on who may have been successfully hacked or the impact.

Although U.S. intelligence officials said last month that the Russians favor President Donald Trump and the Chinese prefer his Democratic challenger, former Vice President Joe Biden, Microsoft noted Thursday that Chinese state-backed hackers have targeted â€œhigh profile individuals associated with the election,â€• including people associated with the Biden campaign.

Chinaâ€™s hackers largely gather intelligence for economic and political advantage, while Russia tends to weaponize stolen data to destabilize other governments.

Microsoft did not assess which foreign adversary poses the greater threat to the integrity of the November presidential election. The consensus among cybersecurity experts is that Russian interference is the gravest. Senior Trump administration officials have disputed that, although without offering any evidence.

â€œThis is the actor from 2016, potentially conducting business as usual,â€• said John Hultquist, director of intelligence analysis at the cybersecurity firm FireEye. â€œWe believe that Russian military intelligence continues to pose the greatest threat to the democratic process.â€•

The Microsoft post shows that Russian military intelligence continues to pursue election-related targets undeterred by U.S indictments, sanctions and other countermeasures, Hultquist said. It interfered in the 2016 campaign seeking to benefit the Trump campaign by hacking the Democratic National Committee and emails of John Podesta, the campaign manager of Hillary Clinton, and dumping embarrassing material online, congressional and FBI investigators have found.

The same GRU military intelligence unit, known as Fancy Bear, that Microsoft identifies as being behind the current election-related activity also broke into voter registration databases in at least three states in 2016, though there is no evidence it tried to interfere with voting.

Microsoft, which has visibility into these efforts because its software is both ubiquitous and highly rated for security, did not address whether U.S. officials who manage elections or operate voting systems have been targeted by state-backed hackers this year. U.S. intelligence officials say they have so far not seen no evidence of infiltrations.

Thomas Rid, a Johns Hopkins geopolitics expert, said he was disappointed by Microsoftâ€™s refusal to differentiate threat level by state actor. â€œTheyâ€™re lumping in actors that operate in a very different fashion, probably to make this sound more bipartisan,â€• he said. â€œI just donâ€™t understand why.â€•

Microsoft said in the past year it has observed attempts by Fancy Bear to break into the accounts of people directly and indirectly affiliated with the U.S. election, including consultants serving Republican and Democratic campaigns and national and state party organizations â€" more than 200 groups in all.

Also targeted was the center-right European Peopleâ€™s Party, the largest grouping in the European Parliament. A party spokesperson said the hacking attempts were unsuccessful. The German Marshall Fund of the United States, a think tank, was another target. A spokesperson said there was no evidence of intrusion.

Microsoft did not say whether Russian hackers had attempted to break into the Biden campaign but did say that Chinese hackers from the state-backed group known as Hurricane Panda â€œappears to have indirectly and unsuccessfullyâ€• targeted the Biden campaign through non-campaign email accounts belonging to people affiliated with it.

The Biden campaign did not confirm the attempt, although it said in a statement that it was aware of the Microsoft report.

Iranian state-backed hackers have unsuccessfully tried to log into accounts of Trump campaign and administration officials between May and June of this year, the blog said. â€œWe are a large target, so it is not surprising to see malicious activity directed at the campaign or our staff,â€• Trump campaign deputy press secretary Thea McDonald said. She declined further comment.

Tim Murtaugh, the campaignâ€™s communications director, said: â€œPresident Trump will beat Joe Biden fair and square and we donâ€™t need or want any foreign interference.â€•

In June, Google disclosed that Hurricane Panda had targeted Trump campaign staffers while Iranian hackers tried to breach accounts of Biden campaign workers. Such phishing attempts typically involve forged emails with links designed to harvest passwords or infect devices with malware.

Although both Attorney General William Barr and National Security Advisor Robert Oâ€™Brien have said China represents the greatest threat to U.S. elections, Microsoftâ€™s only mention of a Trump administration official targeted by Chinese hackers is â€œat least one prominent individual formerly associatedâ€• with the administration.

Graham Brookie, director of digital forensic research at The Atlantic Council, disputes Barr and Oâ€™Brienâ€™s claim that China poses the greater threat to this yearâ€™s election. His lab is at the forefront of unearthing and publicizing Russian disinformation campaigns.

Brookie confirmed that his employer was among targets of Hurricane Panda but said there was no evidence the hacking attempts, which he said were unsuccessful, had anything to do with the 2020 election.

â€œWe have every indication that this was an instance of cyber-espionage, information gathering, as opposed to electoral interference,â€• he said.

By contrast, Brookie said, â€œitâ€™s pretty evident that the Russian attempts (Microsoft disclosed) were focused on electoral processes and groups working on that.â€•

Microsoft noted a shift toward greater automation in Fancy Bear methods for trying to steal peopleâ€™s log-in credentials, which previously largely relied on phishing. In recent months, the group has employed so-called brute-force attacks that barrage an account login with short rapid bursts of potential passwords. It has also used a different method that makes only intermittent login attempts to avoid detection.

Fancy Bear has also stepped up its use of the Tor anonymizing service to hide its hacking, Microsoft said.

- AP