OPINION

China hacks the US military and government — the Feds blame Microsoft

Microsoft could soon be in the hot seat in the wake of a Chinese hack aimed at the US government.

By Preston Gralla
Contributing Editor, Computerworld

AUG 17, 2023 3:00 AM PDT

Hidden in the basic infrastructure that runs the US military is a powerful piece of Windows-borne Chinese malware that can disrupt the communications systems, power grids, and water supplies at the military's bases around the world. One US congressional aide calls it a "ticking time bomb" that as *The New York Times* put it, "could give China the power to interrupt or slow American military deployments or resupply operations by cutting off power, water and communications to US military bases."

The ultimate impact could be even worse, the newspaper notes, because businesses and people use the same infrastructure.

That's not the only successful Chinese hack of Microsoft products targeting vital US institutions. Another targets Outlook and the cloud and has been used to break into the email accounts of US Commerce Secretary Gina Raimondo and various State Department officials. According to Microsoft, the hack, called Storm-0558, "focuses on espionage, data theft, and credential access."

[Bing's AI chatbot came to work for me. I had to fire it.]

These kinds of government-targeted hacks of Microsoft products have happened before. But this time, the response from the US government might be different. In the past, the company suffered no consequences from the attacks. Now, Congress might investigate — and one prominent senator has already urged multiple federal agencies to investigate Microsoft for breaking the law because of its negligence.

Hacking Outlook emails

The Chinese email hack didn't target the US military; it was aimed instead at federal institutions that could harm or help the Chinese economy. The most influential victim, Raimondo, heads the agency that banned the export of US technologies that it claims helps the Chinese military and is used to violate human rights. Among the banned products are semiconductor chips used for artificial intelligence and supercomputers.

Beijing leaders have complained loudly that the ban is a form of economic warfare. Behind the scenes, though, it's been doing more than complaining. It's hacked into the accounts not just of Raimondo, but also, the *Washington Post* reports, "the email accounts of a congressional staffer, a U.S. human rights advocate and U.S. think tanks."

The FBI claims that no classified information was accessed or stolen. That doesn't mean the breach isn't serious, though. Being able to read the private emails of Raimondo, State Department officials and others could offer China a tremendous amount of inside information about US plans for dealing with China in the future.

Former officials said the hack "would have allowed Beijing to see into diplomats' planning for a succession of high stakes visits to China in June and July by U.S. cabinet members, including Secretary of State Antony Blinken, Raimondo and US Treasury Secretary Janet Yellen," according to Newsweek.

The hack forged authentication tokens used by Outlook Web Access in Exchange Online (OWA) and Outlook.com, allowing Chinese hackers to get access to officials' email accounts and calendar items. US organizations and officials weren't the only victims — officials in Western Europe were hit, too.

[Related: Has Microsoft cut security corners once too often?]

The hack was first discovered June 16, around the time Blinken traveled to China. But Charlie Bell, executive vice president for Microsoft Security, said in a blog post the hack was launched on May 15 and has now been "mitigated" – the hole closed.

Targeting military infrastructure

The other hack, malware that targeted military infrastructure, was discovered in May when Microsoft found odd-looking code in telecommunications systems in Guam. The discovery worried US officials, because Guam has a port and massive air base that would likely be used in any US response to an invasion or blockade of Taiwan.

Microsoft blamed a Chinese government-sponsored hacking group, Volt Typhoon, for that attack. The hackers took particular care to cover their tracks and make the infection harder to discover. They melded the stream of their malicious traffic with "normal network activity by routing traffic through compromised small office and home office (SOHO) network equipment, including routers, firewalls, and VPN hardware. They have also been observed using custom versions of open-source tools to establish a command and control (C2) channel over proxy to further stay under the radar."

The company concluded: "Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises."

Federal security officials say the hacking campaign had been under way for at least a year. And they discovered that the hack aimed at targets well beyond Guam, including critical infrastucture and communications systems at military bases worldwide.

Because the attacks have been so well hidden, US officials aren't even sure of the extent of the problem. It's serious enough that there have been a series of meetings held in the White House's situation room, and the Biden Administration has briefed Congress, state governors and utility companies about it.

Congress steps in

Congress has begun investigations, focused for now on the email hack. It's looking beyond just Chinese culpability into whether Microsoft bears responsibility for poor security practices in its multi-billion-dollar contract with the government. That contract is now potentially at risk.

More than half a dozen senators from both parties wrote to the State Department, requesting more information about the hack, and about how Outlook can be better protected in the future. As these things go, it was pretty mild-mannered.

But to a certain extent, that was just a front. Sen. Eric Schmitt (R-MO) was the driving force behind the letter, and he has Microsoft in his cross-hairs. Only a few weeks before the letter was sent, Schmitt inserted a provision into the annual defense bill that orders Department of Defense CIO John Sherman to report to Congress on the "risks and benefits" of buying cybersecurity tools from Microsoft. Schmitt and others worry that relying on a single vendor for so much software and security tools leaves the US more vulnerable to hackers and spies.

Sen. Ron Wyden (D-OR) went even further. He wrote a scathing letter of his own to the US Cybersecurity and Infrastructure Security Agency (CISA), Justice Department and Federal Trade Commission demanding the agencies "hold Microsoft responsible for its negligent cybersecurity practices."

Wyden pointed to other federal security breaches, including the SolarWinds hacking campaign, that he argued had occurred because of Microsoft's lax security practices. He asked US Attorney General Merrick Garland to investigate "whether Microsoft's negligent practices violated federal law" and called on FTC head Lina Khan to determine whether Microsoft's privacy and data security practices "violated federal laws enforced by the Federal Trade Commission, including those prohibiting unfair and deceptive business practices."

Is Microsoft culpable for negligence in all this? At this point, there's no way to know. But one thing we do know: because of the hacks, it's open season on Microsoft in Congress. The company better double-down on its security practices, or billions of dollars could go up in smoke.

Preston Gralla is a contributing editor for Computerworld and the author of more than 45 books, including Windows 8 Hacks (O'Reilly, 2012) and How the Internet Works (Que, 2006).

Follow

It's time to break the ChatGPT habit

UNITED STATES ▾