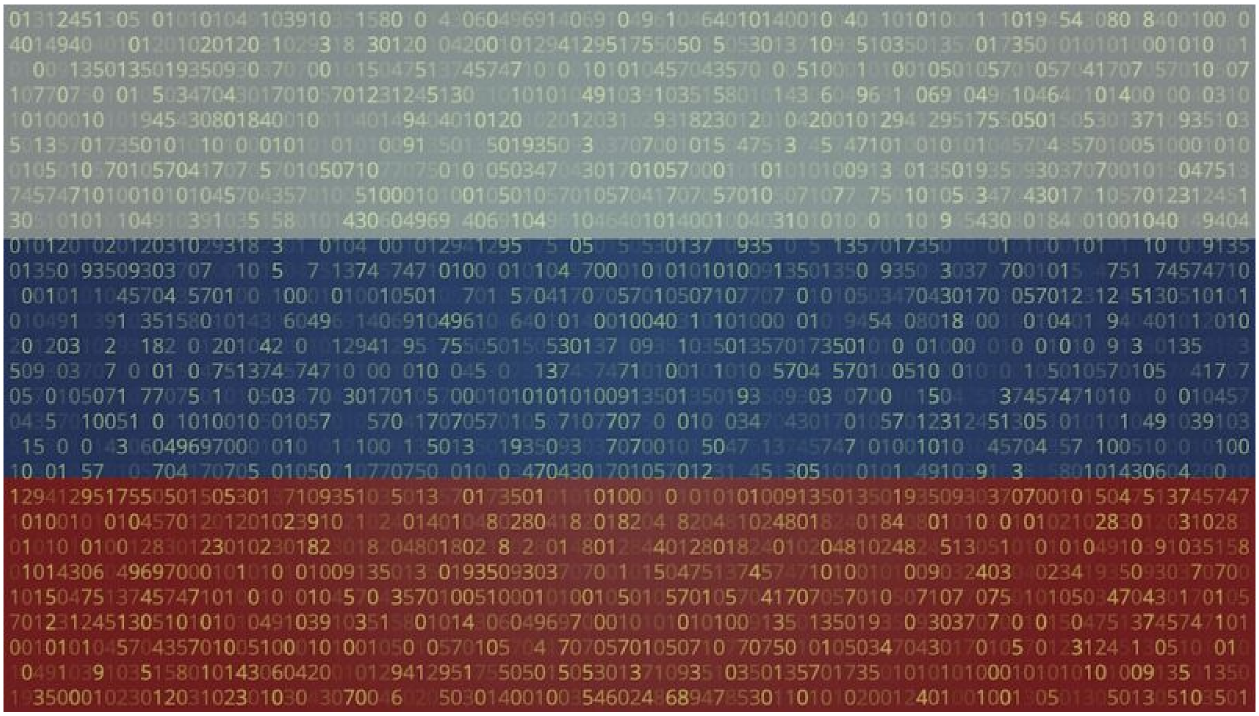
The life and times of Cozy Bear, the Russian hackers who just hit Microsoft and HPE

arstechnica.com/security/2024/01/the-life-and-times-of-cozy-bear-the-russian-hackers-who-just-hit-microsoft-and-hpe/

Dan Goodin

January 26, 2024



Enlarge

Getty Images

Hewlett Packard Enterprise (HPE) said Wednesday that Kremlin-backed actors hacked into the email accounts of its security personnel and other employees last May—and maintained surreptitious access until December. The disclosure was the second revelation of a major corporate network breach by the hacking group in five days.

Further Reading

Microsoft network breached through password-spraying by Russia-state hackers

The hacking group that hit HPE is the same one that Microsoft said Friday broke into its corporate network in November and monitored email accounts of senior executives and security team members until being driven out earlier this month. Microsoft tracks the group as Midnight Blizzard. (Under the company's recently retired threat actor naming convention, which was based on chemical elements, the group was known as Nobelium.) But it is perhaps better known by the name Cozy Bear—though researchers have also dubbed it APT29, the Dukes, Cloaked Ursa, and Dark Halo.

“On December 12, 2023, Hewlett Packard Enterprise was notified that a suspected nation-state actor, believed to be the threat actor Midnight Blizzard, the state-sponsored actor also known as Cozy Bear, had gained unauthorized access to HPE’s cloud-based email environment,” company lawyers wrote in a filing with the Securities and Exchange Commission. “The Company, with assistance from external cybersecurity experts, immediately activated our response process to investigate, contain, and remediate the incident, eradicating the activity. Based on our investigation, we now believe that the threat actor accessed and exfiltrated data beginning in May 2023 from a small percentage of HPE mailboxes belonging to individuals in our cybersecurity, go-to-market, business segments, and other functions.”

An HPE representative said in an email that Cozy Bear’s initial entry into the network was through “a compromised, internal HPE Office 365 email account [that] was leveraged to gain access.” The representative declined to elaborate. The representative also declined to say how HPE discovered the breach.

Cozy Bear hacking its way into the email systems of two of the world’s most powerful companies and monitoring top employees’ accounts for months aren’t the only similarities between the two events. Both breaches also involved compromising a single device on each corporate network, then escalating that toehold to the network itself. From there, Cozy Bear camped out undetected for months. The HPE intrusion was all the more impressive because Wednesday’s disclosure said that the hackers also gained access to Sharepoint servers in May. Even after HPE detected and contained that breach a month later, it would take HPE another six months to discover the compromised email accounts.

The pair of disclosures, coming within five days of each other, may create the impression that there has been a recent flurry of hacking activity. But Cozy Bear has actually been one of the most active nation-state groups since at least 2010. In the intervening 14 years, it has waged an almost constant series of attacks, mostly on the networks of governmental organizations and the technology companies that supply them. Multiple intelligence services and private research companies have attributed the hacking group as an arm of Russia’s Foreign Intelligence Service, also known as the SVR.

The life and times of Cozy Bear (so far)

In its earliest years, Cozy Bear operated in relative obscurity—precisely the domain it prefers—as it hacked mostly Western governmental agencies and related organizations such as political think tanks and governmental subcontractors. In 2013, researchers from security firm Kaspersky unearthed MiniDuke, a sophisticated piece of malware that had taken hold of 60 government agencies, think tanks, and other high-profile organizations in 23 countries, including the US, Hungary, Ukraine, Belgium, and Portugal.

MiniDuke was notable for its odd combination of advanced programming and the gratuitous references to literature found embedded into its code. (It contained strings that alluded to Dante Alighieri's *Divine Comedy* and to 666, the Mark of the Beast discussed in a verse from the Book of Revelation.) Written in assembly, employing multiple levels of encryption, and relying on hijacked Twitter accounts and automated Google searches to maintain stealthy communications with command-and-control servers, MiniDuke was among the most advanced pieces of malware found at the time.

It wasn't immediately clear who was behind the mysterious malware—another testament to the stealth of its creators. In 2015, however, researchers linked MiniDuke—and seven other pieces of previously unidentified malware—to Cozy Bear. After a half-decade of lurking, the shadowy group was suddenly brought into the light of day.

Cozy Bear once again came to prominence the following year when researchers discovered the group (along with Fancy Bear, a separate Russian-state hacking group) inside the servers of the Democratic National Committee, looking for intelligence such as opposition research into Donald Trump, the Republican nominee for president at the time. The hacking group resurfaced in the days following Trump's election victory that year with a major spear-phishing blitz that targeted dozens of organizations in government, military, defense contracting, media, and other industries.

One of Cozy Bear's crowning achievements came in late 2020 with the discovery of an extensive supply chain attack that targeted customers of SolarWinds, the Austin, Texas, maker of network management tools. After compromising SolarWinds' software build system, the hacking group pushed infected updates to roughly 18,000 customers. The hackers then used the updates to compromise nine federal agencies and about 100 private companies, White House officials have said.

Cozy Bear has remained active, with multiple campaigns coming to light in 2021, including one that used zero-day vulnerabilities to infect fully updated iPhones. Last year, the group devoted much of its time to hacks of Ukraine.