Related news

cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

May 26, 2020

government

German intelligence agencies warn of Russian hacking threats to critical infrastructure

(Getty Images)
Written by Sean Lyngaas
May 26, 2020 | CYBERSCOOP
A Kremlin-linked hacking group has continued its long-running efforts to target German companies in the energy, water and power sectors, according to a confidential German government advisory obtained by CyberScoop.

Investigators earlier this year uncovered evidence of the hackers' "longstanding compromises" at unnamed German companies, according to the memo that German intelligence and security agencies sent last week to operators of critical infrastructure.

The hacking group — dubbed Berserk Bear and suspected by some industry analysts of operating on behalf of Russia's FSB intelligence agency — has been using the supply chain to access the German companies' IT systems, said the alert from the BSI, BND, and BfV federal agencies.

“The attackers’ goal is to use publicly available but also specially written malware to permanently anchor themselves in the IT network…steal information or even gain access to productive systems [OT networks],” the advisory said. There was no evidence of a disruptive attack on any company’s industrial networks, German authorities said. The agencies did not respond to a request for comment.

Berserk Bear is best known in the U.S. for a years-long campaign to collect data on U.S. energy companies, which the Trump administration blamed on the Russian government in 2018. It is one of a handful of hacking teams that Moscow can call on to spy on industrial computer networks, analysts say. Another group — known as Sandworm and believed to be operating on behalf of Russia’s GRU military intelligence agency — gained notoriety for cutting off power in Ukraine in 2015 and 2016.

Berserk Bear is less conspicuous. They have used “waterholing,” or infecting websites and then picking off high-value login credentials, to compromise the IT networks of critical infrastructure companies in Europe and North America. In 2018, the hacking group “conducted extensive, worldwide reconnaissance across multiple sectors, including energy, maritime and manufacturing,” and also targeted U.S. government organizations, according to a report from cybersecurity company CrowdStrike.

This is far from German firms’ first encounter with Berserk Bear. In 2018, the BSI — one of Germany’s main cybersecurity agencies — also accused the hacking group of trying to breach the IT networks of German energy and power companies.

Robert M. Lee, CEO of industrial cybersecurity company Dragos, said his analysts were aware of the group’s history — and that of a related set of hackers his company calls “Allanite” — of targeting German and U.S. electric utilities.

“They have been aggressive and targeted numerous utilities, including those in the U.S., over the last couple years,” Lee said. “To date, they haven’t shown the capability or intent to disrupt [utilities’] operations. Given their focus on industrial control systems and wide targeting, though, we continue to track them and report on them to the community.”

Sven Herpig, a cybersecurity expert with the German think tank SNV, welcomed the advisory and urged German companies to heed the warning. The memo has “concrete recommendations of how to spot and protect against an intrusion” from Berserk Bear, he said.

The Russian Embassy in Washington, D.C., did not respond to a request for comment on the German agencies’ report.