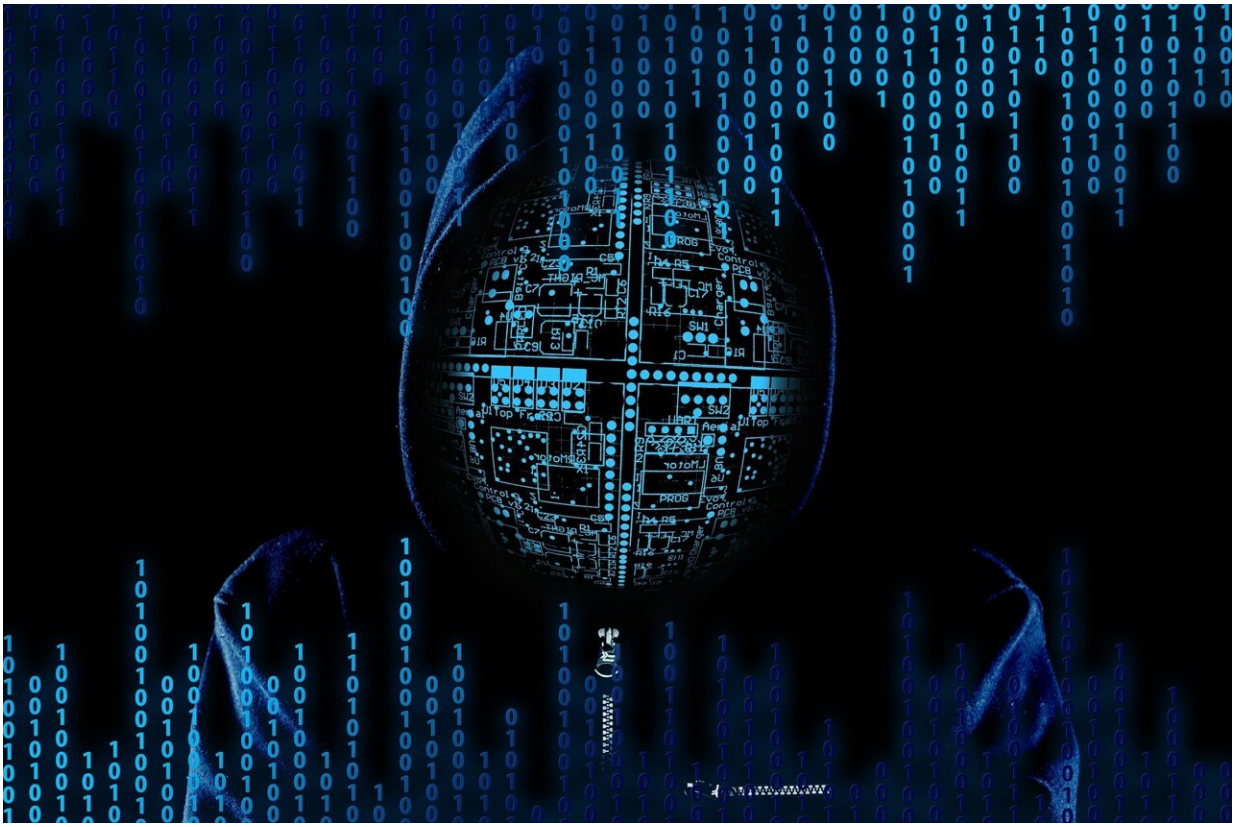
Cisco hit by cyberattack from hacker linked to Lapsus$ gang

August 11 2022, by Margi Murphy



Credit: Pixabay/CC0 Public Domain

Cisco Systems Inc. said it was the victim of a cyberattack in which a hacker repeatedly attempted to gain access to the Silicon Valley firm's corporate network.

Cisco said it became aware of a potential compromise on May 24, and disclosed it on Wednesday after the hacker leaked a list of the files it had stolen on the dark web.

An investigation determined that the hacker broke into Cisco's network by cracking into an employee's personal Google account, which synchronized their saved passwords across the web, the San Jose, California-based company said in a blog post published on Wednesday. The attacker then pretended to be trusted organizations during phone calls with the employee and successfully persuaded the employee to accept a multifactor push authentication notification to their device. That allowed the hacker to gain access to Cisco's network using the employee's credentials.

Cisco had "not identified any evidence suggesting that the attacker gained access to critical internal systems, such as those related to product development, code signing, etc.," according to the blog. "The only successful data exfiltration that occurred during the attack included the contents of a Box folder that was associated with a compromised employee's account. The data obtained by the adversary in this case was not sensitive."

Investigators said they believe that the attack was conducted by an adversary who has previously been identified as an initial access broker for several notorious cybercrime groups: UNC2447, Lapsus$ and Yanluowang ransomware operators. Initial access brokers attempt to gain privileged access to corporate computer networks and then sell it to other hackers.

UNC2447 is an "aggressive financially motivated group" that has targeted organizations with ransomware in Europe and North American, the cybersecurity firm Mandiant concluded last year. Yanluowang, named after a Chinese deity, is a ransomware variant that has been used

against US corporations since August 2021, according to Symantec. The Lapsus$ group was accused of going on a rampage of high-profile attacks against technology companies including Okta Inc., Microsoft Corp. and Nvidia Corp.

Bloomberg News reported that the suspected mastermind was a 16-year-old British teenager living at his mother's house.

Cisco said it found evidence that the hacker was preparing to encrypt files but hadn't managed to do so before they were detected and booted out. There were repeated attempts to regain access after the attack had been evicted, according to Cisco.

The hack was previously reported by Bleeping Computer.