Cybersecurity

Swiss Firm Says It Has Accessed Servers of a SolarWinds Hacker

PRODAFT report details nicknames hackers used, hours they worked

By Daniele Lepido
2021年3月20日GMT+8 下午1:00

A Swiss cybersecurity firm says it has accessed servers used by a hacking group tied to the SolarWinds breach, revealing details about who the attackers targeted and how they carried out their operation. The firm, PRODAFT, also said the hackers have continued with their campaign through this month.

PRODAFT researchers said they were able to break into the hackers' computer infrastructure and review evidence of a massive campaign between August and March, which targeted thousands of companies and government organizations across Europe and the U.S. The aim of the hacking group, dubbed SilverFish by the researchers, was to spy on victims and steal data, according to PRODAFT's report.

SilverFish carried out an "extremely sophisticated" cyber-attack on at least 4,720 targets, including government institutions, global IT providers, dozens of banking institutions in the U.S. and EU, major auditing/consulting firms, one of the world's leading Covid-19 test kit manufacturers and aviation and defense companies, according to the report.

The hackers used other methods to attack their victims besides the vulnerability in SolarWinds's software, according to the researchers.

The researchers don't attribute the attacks to a known hacking organization or a country, though they describe SilverFish as an "APT group." APT stands for advanced persistent threat, and APT groups are often associated with state-backed hacking organizations. PRODAFT researchers said in an interview that the hackers bore some hallmarks of a state-sponsored group, including not being motivated by money and targeting critical infrastructure. But they said more analysis was required to make a definitive determination.

As a result, it isn't clear from the report if SilverFish is a hacking organization linked the Russian government, who the U.S. government and other cybersecurity firms have said is likely behind the SolarWinds attack, or if some other organization also participated. That cyber-attack, which was disclosed in December, involved hackers inserting malicious code in updates for popular software from Texas-based SolarWinds Corp.

As many as 18,000 SolarWinds customers received the malicious update, but far fewer were targeted by the hackers for further infiltration. About 100 private-sector companies and nine U.S. government agencies have been identified, according to the White House.

Swiss cybersecurity officials said they are in contact with PRODAFT, but declined to comment on the information exchanged "for security reasons." The FBI declined to comment about the report, while SolarWinds didn't respond to a request for comment.

The report was received with some skepticism among cybersecurity researchers in the U.S. who have little doubt that the attack was purely an espionage operation by the Russian Federation, though they declined to criticize the report publicly. Microsoft indicated in December that a second attacker might have played a role in exploiting SolarWinds.

Researchers at the cyber research firm Malwarebytes described PRODAFT's findings as "sound."

"We expected to discover more breaches in the aftermath of the SolarWinds disclosure late last year and knew that quite likely multiple different threat groups took advantage of this unprecedented supply-chain attack," said Marcin Kleczynski, chief executive officer and co-

founder of Malwarebytes. He said the discovery of SilverFish reinforces the idea that more than one group exploited SolarWinds.

It's not known if the 4,720 organizations that PRODAFT says were "compromised" by SilverFish simply received the malicious update from SolarWinds or were targeted for further attacks by the hackers. The researchers said they weren't able to gain that level of visibility into the attacker's actions.

Nonetheless, the report offers insights into how the hacking organization operated.

SilverFish's hackers maintained regular working hours and were most active Monday to Friday between the hours of 8 a.m. and 8 p.m., the report said. The hackers operated servers in Russia and Ukraine, and shared some of the same servers as a notorious Russian criminal hacking group known as Evil Corp., the report said.

PRODAFT said the hackers were an "extremely well-organized cyber-espionage group," with four teams named 301, 302, 303 and 304 responsible for breaching their victims' computers. The hackers placed emphasis on targeting governments and large corporations, such as Fortune 500 enterprise companies, according to the report.

The SilverFish group chose not to pursue attacks against victims originating from countries including Russia, Ukraine, Georgia and Uzbekistan, the report said. The U.S. was by far the region most frequently targeted by hackers, with 2,465 attacks recorded, followed by European states with 1,466 victims originating from Italy, the Netherlands, Denmark, Austria, France and the U.K.

The hackers wrote comments "in Russian slang and vernacular," while English was the other main language used. Source code also contained ID numbers and nicknames -- including "new hacker," "cyberbro netsupport" and "walter," for 14 people who likely workede under the supervision of four teams, the report says.

”What is perhaps the most striking from this report is the highly organized professionalism of the threat actor,” said Rik Ferguson, vice president of security research at the cybersecurity company Trend Micro Inc. and special adviser for Europol, the EU’s law enforcement agency, who reviewed the report. He said it was clear that the hackers were highly-skilled, well-funded and is operating with a clearly defined mission brief.

PRODAFT’s involvement began in December, after a client was compromised as part of the SolarWinds breach. The researchers searched the internet for other servers using the same unique digital fingerprint used in the attack and found about a dozen machines used by the attackers.

Among these, PRODAFT found what is known as “command and control” servers, platforms set up and used by the attackers to monitor and send commands to the infected victims. PRODAFT identified security weaknesses in the configuration of the two servers and gained access to them.

The researchers found lists of compromised organizations, along with evidence indicating that the hacking group had been actively targeting its victims since August last year. SilverFish went quiet in late November, according to PRODAFT’s report, but returned in January to resume its operations.

In what the researchers described as one of the more shocking discoveries, the attackers created a web panel for testing their malicious payloads on victims’ devices, testing to see if antivirus or threat-hunting products would flag their activities.

PRODAFT, which stands for Proactive Defense Against Future Threats, was founded in 2012 and is based in Yverdon-les-Bains, Switzerland.

– With assistance by Ryan Gallagher, and Kartikay Mehrotra

In this article

SWI
SOLARWINDS CORP
16.99 USD ▼ -0.41 -2.36%

MSFT
MICROSOFT CORP
237.58 USD ▲ +1.59 +0.67%

1066455D
TREND MICRO INC
Private Company