Industrial infection: Hackers put chokehold on energy firms with Stuxnet-like viruses

01/07/2014

Hackers are targeting energy companies in the US and Europe in an apparent case of industrial espionage, according to several security companies, which say the perpetrators seem to be based in Eastern Europe.

The group of hackers, known as 'Energetic Bear' or 'Dragonfly', are attacking hundreds of Western oil and gas companies, as well as energy investment firms, and infecting them with malware capable of disrupting power supplies.

Additional targets have included energy grid operators, major electricity generation firms, petroleum pipeline operators, and industrial energy equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland, according to a Symantec report released on Monday.

The malware campaign is somewhat similar to Operation Olympic Games, an alleged cyberwarfare attacks mounted by the US and Israel that used a virus called Stuxnet to target the Iranian nuclear industry in July 2010. The attack was the first known major malware campaign to target industrial control system (ICS) equipment providers.

The US-Israeli operation was tailored against Iranian uranium enrichment facilities, but the Dragonfly attacks, while having signatures of a government-sponsored operation, are more ambitious, the IT security firm believes.

Espionage, potential sabotage

The hackers infect the industrial control software with a remote access-type (RAT) Trojan horse malware code – called Havex RAT – which gives them a “beachhead in the targeted organizations’ networks,” as well as the ability to sabotage infected ICS computers. The malware also allows the hackers to monitor energy consumption in real time and to potentially cripple physical systems such as wind turbines, gas pipelines and power plants through that software.

Symantec says the Dragonfly hackers have been in operation since at least 2011, and initially targeted defense and aviation companies in the US and Canada. The shift in focus to US and European energy firms occurred in early 2013.

That campaign began with phishing emails to top executives in targeted firms. Then Dragonfly began using watering hole attacks, which compromise websites likely to be visited by those working in the sector, then redirect visitors to websites hosting an exploit kit. That kit then delivers malware to the victims' computers. Finally, the hackers began 'Trojanizing' legitimate software bundles belonging to three different ICS equipment manufacturers.

"Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability. The group is able to mount attacks through multiple vectors and compromise numerous third party websites in the process," Symantec wrote in the report published on its blog.

Clever, sometimes unprofessional

Finnish security company F-Secure has also been tracking the use of the Havex malware. "The attackers behind Havex are conducting industrial espionage using a clever method. Trojanizing ICS... software installers is an effective method in gaining access to target systems, potentially even including critical infrastructure," the company said on its blog.

F-Secure noted that "the group doesn't always manage the C&C's [command and control servers] in a professional manner, revealing lack of experience in operations."

But its security analyst, Sean Sullivan, told Infosecurity that the group could well be state-sponsored.

"It fits the pattern of a nation state doing intelligence work, getting the lay of the land, in order to find exploitable systems for future 'need'," he argued.

Symantec, F-Secure and a third security company, CrowdStrike, all believe that cyber espionage is the main motive. "Dragonfly has targeted multiple organizations in the energy sector over a long period of time. Its main motive appears to be cyber espionage, with potential for sabotage a definite secondary capability," Symantec said.

Russian trail?

Symantec analyzed the compilation of timestamps on the malware used by the hackers.

"The group mostly worked between Monday and Friday, with activity mainly concentrated in a nine-hour period that corresponded to a 9am to 6pm working day in the UTC +4 time zone. Based on this information, it is likely the attackers are based in Eastern Europe," the Silicon Valley-based security company wrote.

CrowdStrike, also based in California, began tracking a group of hackers it called Energetic Bear in August 2012. Symantec believes that the group it calls Dragonfly and the group "known by other vendors as Energetic Bear" are the same.

In its 2013 Global Threat Report, CrowdStrike detailed the evidence that led it to believe Energetic Bear is a group of Russian hackers. Like Symantec, it noted the times of the attacks indicated Eastern Europe, but went further in its assessment.

"Targeted entities and countries are consistent with likely strategic interests of a Russia-based adversary. Several infected hosts were observed within the Russian Federation, but this could be the result of accidental compromise through large-scale SWC operations or deliberate efforts to conduct domestic internal monitoring," the report said.

But among victims of the hacker group identified by F-Secure, the majority of which are based in Europe, there is a Russian construction company "that appears to specialize in structural engineering."