BAE report says Ukraine has faced cyberattacks

March 10 2014, by Danica Kirka

Ukraine was repeatedly attacked by sophisticated cyberspies as tensions between pro-Russian and Western-leaning factions escalated in recent months, according to a report from U.K.-based defense contractor BAE Systems.

Ukrainian computer systems have been targeted by at least 22 attacks launched by "committed and well-funded professionals" since January 2013, BAE found. While BAE didn't identify the source of the attacks, a German company said the espionage software has "Russian roots."

The spies used "Snake" malware that allowed them to gain control of the computer systems of large organizations and steal information, according to the report from BAE's Applied Intelligence unit. Snake's design "suggests that attackers possess an arsenal of infiltration tools and bears all the hallmarks of a highly sophisticated cyber operation," BAE said.

While the report released last week by BAE Systems Applied Intelligence doesn't name Russia as the source of the attacks, it suggests they originated in the time zone where Moscow is located.

G Data Software, based in Bochum, Germany, went a step further, saying that a variant of the snake software known as Uroburos has "Russian roots." There are "strong indications" that the group behind Uroburos, the Greek word for an ancient symbol that shows a serpent eating its own tale, is the same one that attacked U.S. military bases in 2008 with malware known as Agent.BTZ, G Data said.

"Notable hints include the usage of the exact same encryption key then and now, as well as the presence of Russian language in both cases," according to the G Data report.

The BAE report, which is highly technical and designed to help system operators block attacks, comes at an uneasy moment in relations between Ukraine and Russia. Pro-Russian leader Viktor Yanukovich fled his country after months of anti-government protests by Ukrainians who favored closer ties with the European Union. In response, pro-Russian forces took control of Crimea and scheduled a referendum on joining Russia.

A majority of people in Crimea identify with Russia and Moscow's Black Sea Fleet is based in Sevastopol, making it a flashpoint for tensions.

While Ukraine was the most frequently targeted by Snake malware, it is not alone. BAE identified 56 attacks that took place since 2010. Thirty-two were directed at Ukraine and 11 at Lithuania, another former Soviet republic. The U.K. was subject to four attacks, with two each directed at the U.S., Georgia and Belgium.

"Whilst this view is likely to only be the tip of the iceberg, it does give us an initial insight into the profile of targets for the Snake Operations," BAE said.

Martin Sutherland, the managing director, of BAE Systems Applied Intelligence, said the threat described in the report raises the bar in terms of what potential targets and security officials need to do to keep ahead of cyberattackers.

"What this research once more demonstrates is how organized and well-funded adversaries are using highly sophisticated tools and techniques to

target legitimate organizations on a massive scale," he said in a statement. "Although there has been some awareness of the Snake malware for some years, until now the full scale of its capabilities could not be revealed, and the threat it presents is clearly something that needs to be taken much more seriously."