US, Iran dig in for long cyber war

June 2 2012, by Rob Lever

The United States and Iran are locked in a long-running cyber war that appears to be escalating amid a stalemate over Tehran's disputed nuclear program.

The Flame virus that surfaced recently may be part of the face-off, but Washington probably has more sophisticated tools at its disposal, security specialists say.

"Large nations with large spy agencies have been using these kinds of techniques for more than a decade," said James Lewis, a senior fellow who monitors technology at the Center for Strategic and International Studies in Washington.

Lewis said cyber espionage is "not a weapon" but can be "very effective" as an intelligence tool and can avoid some of the problems with traditional surveillance such as spy planes.

"If you have to choose between this and a pilot being paraded through the streets of Tehran, this is much preferable," he said.

But Lewis noted that the Flame virus is more primitive than one would expect from US intelligence services.

"I hope it wasn't the US that developed it because it isn't very sophisticated," he told AFP.

He said Israel has quite advanced capabilities as well, and that this probably means Flame was developed in a "second-tier country."

Some analysts, however, consider Flame to be highly sophisticated. The International Telecommunications Union said the virus is "a lot more complex than any other cyber-threat ever seen before."

Johannes Ullrich, a computer security specialist with the SANS Technology Institute, said Flame is a rather "clumsy" tool compared to other types of malware, but that it may be a rough version or prototype which can be wrapped into a "more polished" version.

"The technical part isn't that great, and I think it has been a bit hyped in some of the reports," Ullrich said.

Exactly where the malware came from is impossible to know from the code, Ullrich said.

"It doesn't look like one single individual," he said. "Whether it is a government or some criminal group, it's hard to tell."

Marcus Sachs, former director of the SANS Institute's Internet Storm Center, said Flame "could be written by virtually anybody but it looks similar to targeted espionage from a country."

Sachs said Flame is not a sabotage tool like the Stuxnet virus that targeted control systems in Iran, but instead resembles spyware seeking "to gain intellectual property, but it could be surveillance by a foreign government."

Neither the US nor the Israeli government has openly acknowledged authoring Flame, though a top Israeli minister said use of the software to counter Iran's nuclear plans would be "reasonable."

The US military has acknowledged working on both defensive and offensive cyber war systems.

The Pentagon's Defense Advanced Research Projects Agency has revealed few details about its "Plan X," which it calls a "foundational cyber warfare program" that draws on expertise in academia, industry and the gaming community.

But a DARPA statement said the program is "about building the platform needed for an effective cyber offensive capability. It is not developing cyber offensive effects."

Sachs said the US has been open about developing its cyber capabilities and that DARPA, which created the Internet, is looking at longer-term projects that may involve technologies not yet deployed.

On the surface, it might be harder for the US to maintain superiority in cyberspace as it does in the skies, for example, because the costs for computer programming is far less than for fighter planes.

But experts say the US is investing in cyberspace through DARPA and other projects.

Still, Sachs said measuring the capabilities of another country are not as easy as counting missile silos. "There's no way to measure what a country has," he said.

The New York Times reported that President Barack Obama secretly ordered cyber warfare against Iran to be ramped up in 2010 after details leaked out about Stuxnet, which some say came from the US, Israel or both.

Ilan Berman, an analyst at of the American Foreign Policy Council who follows Iran, said that with cyber war simmering, Tehran is boosting its defensive and offensive capabilities.

"They feel like there is a campaign against them and they are mobilizing in response," he said.

And the US should therefore be prepared for cyber retaliation from Iran.

"I think a cyber attack by Iran may not be as robust (as one from China or Russia) but politically it's more likely," he said.

Lewis said the US and Iran have been engaged in struggles for the past decade, due to the nuclear issue and suspected Iran involvement with certain forces in Iraq while US forces were deployed there.

But he said Flame and other cyber weapons are "not really warfare, it's primarily intelligence collection."

Lewis said he was not surprised that the discovery of the virus came from a Russian security firm, Kaspersky, which worked with the ITU.

"Flame is a way to drive Russia's diplomatic agenda," which includes bringing the Internet under UN control, Lewis said.

Citation: US, Iran dig in for long cyber war (2012, June 2) retrieved 26 April 2024 from https://phys.org/news/2012-06-iran-cyber-war.html