Meet Babar, a New Malware Almost Certainly Created by France

motherboard.vice.com/read/meet-babar-a-new-malware-almost-certainly-created-by-france

The NSA, GCHQ, and their allies in the Five Eyes are not the only government agencies using malware for surveillance. French intelligence is almost certainly hacking its targets too—and now security researchers believe they have proof.

On Wednesday, the researchers will reveal new details about a powerful piece of malware known as "Babar," which is capable of eavesdropping on online conversations held via Skype, MSN and Yahoo messenger, as well as logging keystrokes and monitoring which websites an infected user has visited.

Babar is "a fully blown espionage tool, built to excessively spy" on its victims, according to the research, which Motherboard reviewed in advance. The researchers are publishing two separate but complementary reports that analyze samples of the malware, and all but confirm that France's spying agency the General Directorate for External Security (DGSE) was responsible for its creation.

France's Defense Ministry did not respond to a request for comment by the time of publication.

"European nations are just as capable as the US and Russia to take their espionage efforts to cyberspace," Marion Marschalek, an Austrian researcher at Cyphort and author of one of the reports, told Motherboard. "France is just as active as the other big players."

"Babar is a popular French children's television show." Photo via Der Spiegel

Marschalek analyzed the malware samples with Paul Rascagneres, a malware analyst at security firm G DATA, and Joan Calvet, a researcher from anti-virus maker ESET.

Initial hints at Babar's existence were first revealed last March, when a document leaked by Edward Snowden described a 2009 spying operation dubbed SNOWGLOBE. According to Canadian intelligence agency Communications Security Establishment (CSE), which discovered the operation, SNOWGLOBE mainly targeted Iran's nuclear program, but also hit victims in European countries such as Greece and Spain.

The operation used malware the attackers named "Babar," and CSE concluded with "moderate certainty" that SNOWGLOBE was a hacking operation carried out by "a French intelligence agency." (The researchers believe this was a previous version of the Babar malware they have analyzed. The precise capabilities of that old version are unclear.)

After Le Monde published the CSE document describing SNOWGLOBE and Babar, the researchers said they obtained a series of malware samples, or binaries, that belonged to the same attackers, and are from the same "family" as the malware described in the document. Marschalek said that another researcher who preferred not to be named suggested that copies of the malware had been uploaded to VirusTotal, an online malware detection service.

Though their analysis didn't uncover any new evidence implicating France, the two reports confirm many of the details contained within CSE's document, according to the researchers.

"I'm sure [it was France], but proving this publicly is close to impossible," Marschalek told Motherboard via instant message. "With binary attribution you generally have the problem, unlike in real crime scenes, you do not have actual evidence. There are indicators, from which conclusions can be drawn, but anything that serves as something like a digital fingerprint can be faked in the end."

The first clue is the malware's name. The CSE document identified the malware's "internal name" as Babar—which happens to be the name of an elephant from a popular series of French children's books. The sample analyzed by Marschalek and Rascagneres was named Babar64. Babar also communicated with the same servers as two other hacking tools, EvilBunny and TFC—which the researchers believe were also created by the French—and those servers hosted French language websites.

Yet another clue is a simple typo.

According to the CSE document, the author of the Babar malware misspelled a string in the code. Instead of writing MSIE, the author wrote MSI. That same mistake is contained in the code of Babar64 and EvilBunny.

Photo via Der Spiegel

Photo via Marion Marschalek/Cyphort

All these breadcrumbs are "unique properties" that show that the malware analyzed by Marschalek, Rascagneres and Calvet is likely associated with the one described in the CSE document, according to Morgan Marquis-Boire, a former Google security researcher who's now director of security for First Look Media.

These reports represent "an important step" in understanding the hacking capabilities of Western nations that are not members of the Five Eyes. While Babar might not be as sophisticated as the GCHQ malware campaign REGIN, or the newly-revealed NSA campaign, it's still "high-quality," Marquis-Boire told Motherboard.

"There's different strata of players in the nation-state cyber espionage arena," said Marquis-Boire, who has reviewed the report. "There's a lot of really, really badly written malware. Here there's the quality you could expect from a nation that has a large military industrial complex."

According to Marschalek, Babar is not "very sophisticated," but is highly targeted and a "very good software, above the level of what kind of 'products' a malware analyst gets to see on a daily basis."

In other words, it seems we have evidence that France is in the hacking business now, too.