F-SECURE LABS

<<< NEWS FROM THE LAB - Friday, March 6, 2015 >>>

ARCHIVES | **SEARCH**

Is Babar a Bunny?

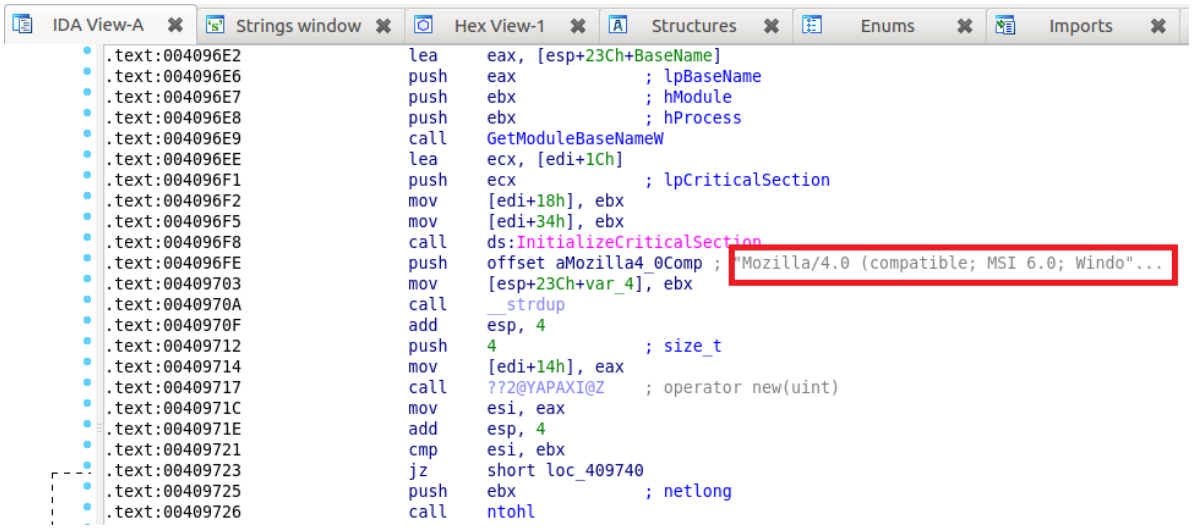
Posted by FSLabs @ 09:37 GMT

SNOWGLOBE was first brought to media attention about a year ago by French newspaper Le Monde, when they wrote about top secret SCEC slides leaked by, who else than Edward Snowden himself. In the set of slides, there are numerous claims about French-originating malware which internally calls itself Babar. It didn't take a long time for the security community to dig out samples resembling Babar [1] [2] [3].

What exactly can we say about Bunny and its connection to Babar? For Bunny and EvilBunny, we have a lot of research available, so it is already quite known to the security community. But when it comes to Babar, we only have screenshots of the mysterious top secret slides. However, there is now enough correlation to say with a high level of probability that Bunny and Babar, as described in the SCEC slides, belong to same family of espionage tools.

Fact 1. Both operations seem to be active mostly 2010-2011. This is evident from Bunny PE header timestamps, and the CSEC slides are from 2011.

Fact 2. Some Bunny samples present the same typing error in User-Agent as document in the slides (MSI instead of MSIE, see the SCEC slide SNOWBALL Beacons). Doesn't sound like a coincidence.



Fact 3. One of the samples connected to Bunny drop a file named ntrass.exe, also mentioned in the SCEC slides. Doesn't sound like a coincidence.

Fact 4. Latest findings from the Bunny family actually reveal another internal project name: Babar64 [2] [3]. Doesn't sound like a coincidence.

Fact 5. Bunnies and little elephants are both cute and fluffy little animals. Very unusual in the APT world.

Also, it can be said with a high likelihood that this malware originates from France. Some of the Bunny samples use *Accept-Language: fr* in the HTTP headers. There are also some really strange decisions in the internal namings, like for example naming task threads as "hearer" [1]. In the English-speaking software development world, this kind of task is usually named as "listener" or "monitor". "Hearer" isn't exactly one of the default terms used by an English-speaking developer. It sounds more like a non-native English speaker who used a literal translation of a language they are used to. For example, French "auditeur" translates to "auditor, listener, hearer".

But there are some things we cannot say about the connection. First off, the slides themselves do not name any specific actor, so rumors about French Intelligence are not based on sound facts at the moment. The fact that Bunny uses the Lua programming language for extending its capabilities also adds up to the mess (remember Flame?). Also, it should be noted that all the juicy pieces of attribution are in the slides, so we don't have first hand evidence about that. There is also something to think about the complexity level of Bunny. It is nowhere near the level of the high-profile APT's, such as Turla and Equation. But that doesn't of course mean that there couldn't be a high-profile actor behind SNOWGLOBE. Sometimes it just makes one wonder why these people make the tools so obvious, like a glowing Christmas tree in the dark.

Hashes:

- 2c678924a3d4307644208b199afd20940c058b62
- c923e15718926bb4a80a29017d5b35bb841bd246