Babar: Suspected Nation State Spyware In The Spotlight

web.archive.org/web/20150218192803/http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/

February 18, 2015

Cyphort Labs

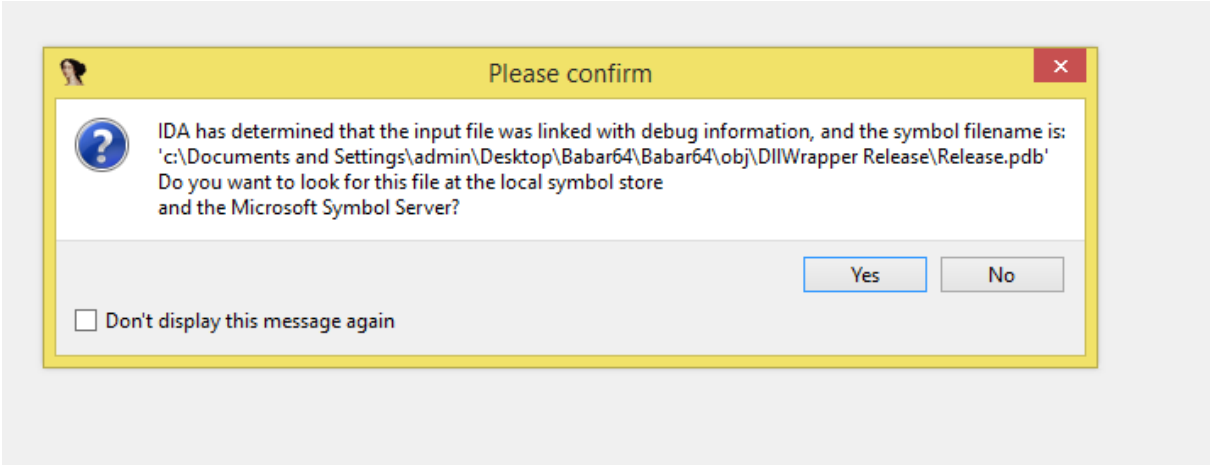
Blog

Posted on February 18th, 2015 by Marion Marschalek

Blog Home

Cyphort Labs has collected and analyzed a highly advanced piece of malware, which for all intents and purposes seems to be a full blown cyber espionage tool of the kind a nation state would be behind. This malware invades Windows desktop machines and aims at exfiltrating almost anything of value: it steals data from instant messengers, softphones, browsers and office applications.

The analyzed malware consists of two pieces: a dropper and an implant. The implant is able to hook APIs of interest in dedicated remote processes to steal data on the fly.



The internal project name of the analyzed malware is ‘Babar64’, which rings a bell when thinking back of documents leaked through Der Spiegel back in January (http://www.spiegel.de/media/media-35683.pdf). There, a slide deck originating from

Communications Security Establishment Canada (CSEC) describes an alleged nation state malware named Babar. The samples at hand fit well with what is described in the CSEC document; and, as CSEC states they are suspected to originate from French intelligence.

As it is with binary attribution, these allegations are impossible to prove without the shadow of a doubt. What we can say with certainty though is that Babar strikes the analyst with sophistication not typically seen in common malware. Furthermore, the binaries come with the same handwriting as the malware dubbed 'Bunny' which we have blogged about before (http://www.cyphort.com/evilbunny-malware-instrumented-lua/). We assume the same author is behind both families.

Note: I will be hosting a webinar on the topic of Evil Bunny malware next week. You can register here to attend.

DROPPER

MD5	9fff114f15b86896d8d4978c0ad2813d
SHA-1	27a0a98053f3eed82a51cdefbdfec7bb948e1f36
File Size	693.4 KB (710075 bytes)

IMPLANT

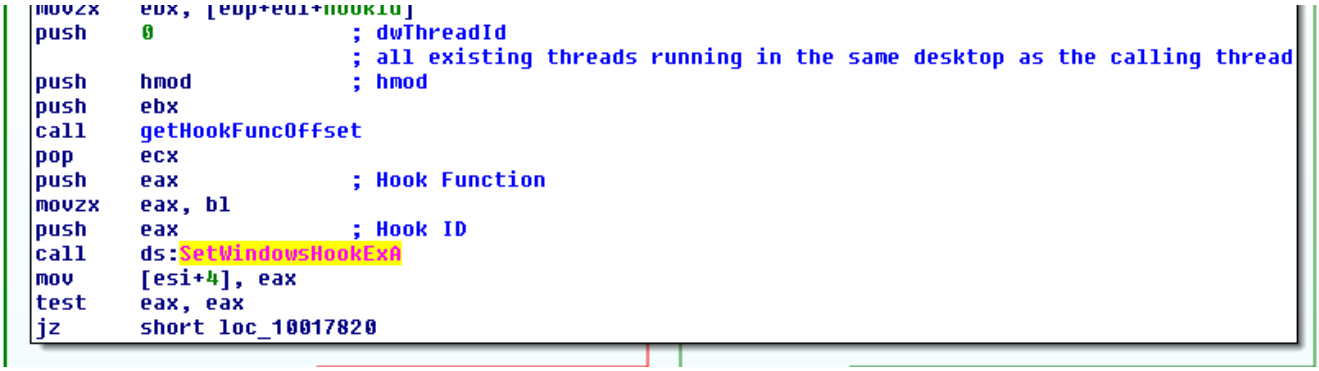
MD5	4525141d9e6e7b5a7f4e8c3db3f0c24c
SHA-1	efbe18eb8a66e4b6289a5c53f22254f76e3a29bd
File Size	585.4 KB (599438 bytes)

A BABAR(ian) BINARY

A target machine is infected possibly through a drive-by or malicious e-mail attachments. Babar is deployed through a malware dropper, which installs the malware.

Babar essentially is an implant, a malicious Windows DLL. Babar's implant is a 32-bit DLL written in C++, which upon start injects itself to running processes and invades desktop applications by applying a global Windows hook. The original filename of the sample at hand is 'perf585.dll'. The implant is capable of logging keystrokes, capturing screen shots, eavesdropping on installed softphones and spying on instant messengers in addition to a list of simpler espionage tricks. Babar is a full blown espionage tool, built to excessively spy on the activity on an infected machine's user.

The DLL dropped by Babar is placed into the application data folder, along with a directory named 'MSI' where the runtime data will be stored. Babar operates through multiple instances, by injecting its DLL to a maximum of three desktop processes. This is achieved by loading the Babar DLL to remote processes through a mapped memory object.



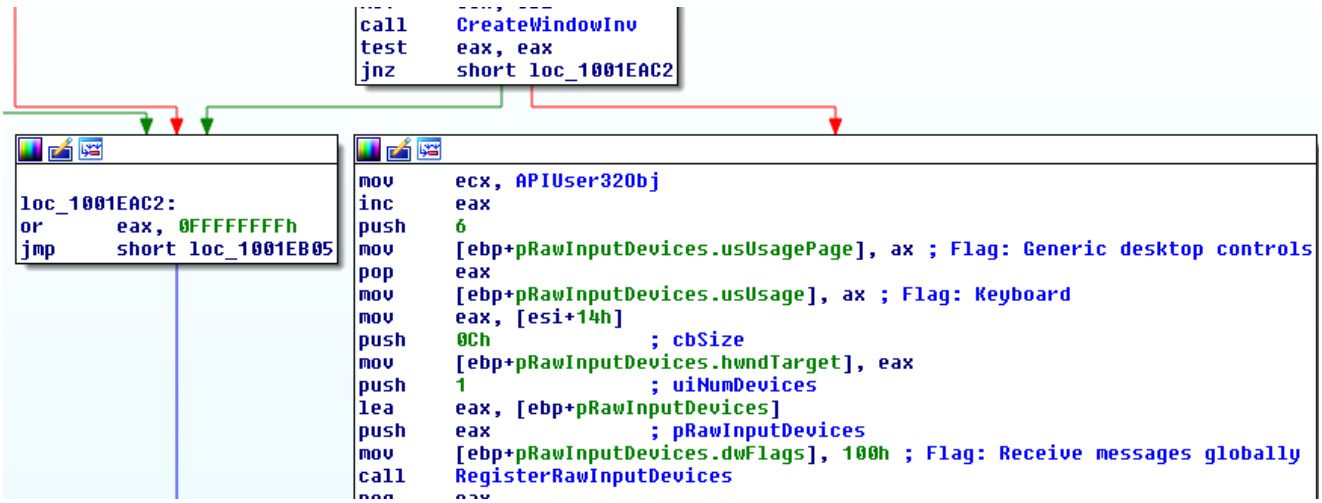
Apart from that, Babar comes with a userland rootkit component which applies global Windows hooks to invade all processes on its desktop. This way Babar can install API hooks for various APIs via Windows Detours technique to actively steal data from arbitrary processes.

The spying activities are performed either through the Babar instance locally or through processes invaded via hooking. Instance-local capabilities are basic spying on window names or snooping on the clipboard data, while the global hooks manage to steal information directly from Windows API calls.

A summary of the capabilities would be as follows:

- Logging keystrokes
- Taking screenshots
- Capture of audio streams from softphone applications
- Stealing of clipboard data
- System and user default language, keyboard layout
- Names of desktop windows

The keylogger module is based on Windows RAWINPUT. The malware creates an invisible window, with no other purpose than to receive window messages. By processing the window message queue it filters out input events and dispatches them to a raw input device object. Said object is configured to grab keyboard events through GetRawInputData.



The interest of Babar's process hooking module is focused on the following applications, parted in the categories internet communication, file processing and media:

- Internet communication
  iexplore.exe,firefox.exe,opera.exe,chrome.exe,Safari.exe,msnmsgr.exe
- File processing
  exe, winword.exe, powerpnt.exe, visio.exe, acrord32.exe, notepad.exe, wordpad.exe.txt
- Media
  skype.exe, msnmsgr.exe, oovoo.exe, nimbuzz.exe, googletalk.exe, yahoomessenger.exe, x-lite.exe

The malicious implant can steal input coming from the keyboard, information on which files are edited, it can intercept chat messages and record calls established by one of the listed softphones. The stolen information is encrypted and dumped to a file on disk, which will be located in the working directory under %APPDATA%\MSI.

COMMAND AND CONTROL SERVERS

The analyzed sample of Babar has two hard coded C&C server addresses which are included in its configuration data:

- http://www.horizons-tourisme.com/_vti_bin/_vti_msc/bb/index.php
- http://www.gezelimmi.com/wp-includes/misc/bb/index.php

The domain horizons-tourisme.com is a legitimate website, operated by an Algerian travel agency, located in Algiers, Algeria. The website is in French and still online today. Gezelimmi.com is a Turkish domain, currently responding with an HTTP error message 403, access not permitted. Both domains appear to be of legitimate use, but compromised and abused to host Babar's server side infrastructure.

« Read Previous Post