On January 17 2015, Spiegel.de published an extensive article based on documents obtained from Edward Snowden. At the same time, they provided a copy of a malicious program codenamed "QWERTY" (http://www.spiegel.de/media/media-35668.pdf), supposedly used by several governments in their CNE operations.

We've obtained a copy of the malicious files published by Der Spiegel and when we analyzed them, they immediately reminded us of Regin. Looking at the code closely, we conclude that the "QWERTY" malware is identical in functionality to the Regin 50251 plugin.

**Analysis**

The Qwerty module pack consists of three binaries and accompanying configuration files. One file from the package—20123.sys—is particularly interesting.

The "20123.sys" is a kernel mode part of the keylogger.
As it turns out, it was built from source code that can also be found one Regin module, the "50251" plugin.

Using a binary diff it is easy to spot a significant part of code that is shared between both files:
Most of the shared code belongs to the function that accesses the system keyboard driver:

Most of the "Qwerty" components call plugins from the same pack (with plugin numbers 20121 – 20123), however there is also one piece of code that references plugins from the Regin platform. One particular part of code is used in both the "Qwerty" 20123 module and the Regin's 50251 counterpart, and it addresses the plugin 50225 that can be found in the virtual filesystems of Regin. The Regin's plugin 50225 is responsible for kernel-mode hooking.

50251.dll (Regin module) 20123.sys ("qwerty")
This is a **solid proof** that the Qwerty plugin can only **operate as part of the Regin platform**, leveraging the kernel hooking functions from plugin 50225.

As an **additional proof** that both modules use the **same software platform**, we can take a look at functions exported by ordinal 1 of both modules. They contain the startup code that can be found in any other plugin of Regin, and include the actual plugin number that is registered within the platform to allow further addressing of the module. This only makes sense if the modules are used with the Regin platform orchestrator.

The reason why the two modules have different plugin IDs is unknown. This is perhaps because they are leveraged by different actors, each one with its own allocated plugin.
Conclusions

Our analysis of the QWERTY malware published by Der Spiegel indicates it is a plugin designed to work part of the Regin platform. The QWERTY keylogger doesn't function as a stand-alone module, it relies on kernel hooking functions which are provided by the Regin module 50225. Considering the extreme complexity of the Regin platform and little chance that it can be duplicated by somebody without having access to its sourcecodes, we conclude the QWERTY malware developers and the Regin developers are the same or working together.

Another important observation is that Regin plugins are stored inside an encrypted and compressed VFS, meaning they don't exist directly on the victim's machine in "native" format. The platform dispatcher loads and executes there plugins at startup. The only way to catch the keylogger is by scanning the system memory or decoding the VFSes.

Appendix (MD5 hashes):

QWERTY 20123.sys:

1. 0ed11a73694999bc45d18b4189f41ac2

Regin 50251 plugins:

1. c0de81512a08bdf2ec18cb93b43bdc2d
2. e9a43ea2882ac63b7bc036d954c79aa1

Related Posts

- AN ANALYSIS
- WINDOWS 10
- KASPERSKY
THERE ARE 2 COMMENTS

If you would like to comment on this article you must first login

Hausverwaltung Essen
Posted on January 27, 2015. 2:24 pm

Is it just as siple, as it seems???

Reply

Lecaf@geocities.com
Posted on January 27, 2015. 2:38 pm

Any similarity with bugbear keylogger? Just curious.

Reply