BUZZDIRECTION: BLATSTING reloaded

laanwj.github.io/2016/09/11/buzzdirection.html

Laanwj's blog

Randomness

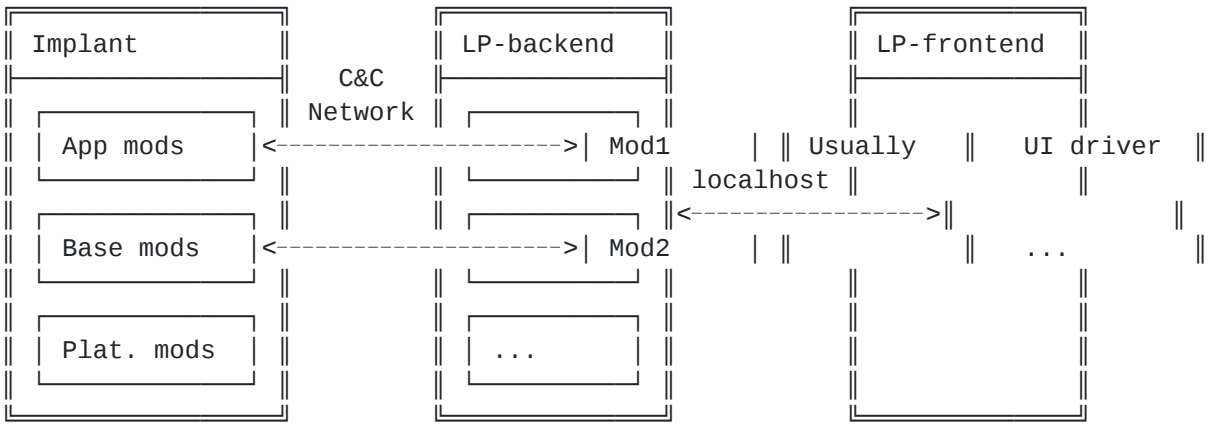
Blog About

This time I will be taking a cursory look at a different malware framework in the EQGRP free dump: BUZZDIRECTION. BUZZDIRECTION is another modular rootkit, but more extensive than BLATSTING. This list classifies it as “a firewall software implant for Fortigate firewalls”, just like BLATSTING. Maybe it is just a successor for the same purpose, but maybe it is something more.

There is clear evidence that it is a newer and improved version of the same software:

- The terms **LP** and **Implant** are used in the same way, for the controlling and victim site respectively. Both the LP side and the implant side have loadable code modules with a dependency hierarchy.
- There are approximately the same modules, and they are named similarly.
- Both use an ELF-based loading system (Executable-and-Loading Format is a standard format used for executables by many operating systems and compiler toolchain)
- Both use the same obfuscation method for strings.

However, BUZZDIRECTION adds some new features:



- Platform-dependent and -independent modules.

    Two platforms are included: BUZZTACO and BUZZFAJITA. It is not clear to me what these are exactly, but they are both based on Linux, supposedly Linux-based routers. This software seems less specifically targetted than BLATSTING which was hardcoded to specific kernels. It is also much easier to add support for new targets here.
- Multiple CPU architecture support: `i386` `ppc` `x86_64` are those included.
- Even more care has been taken to purge / obfuscate strings.
- There is a better organized directory hierarchy. Modules are split between base (Crypto, Hash, core utilities), base platform (platform functions for accessing files, processes, persistence, and so on), and application (NetworkProfiler, SecondDate, Tunnel, and so on).
- The LP has been split into two parts: an binary backend and a Python-based frontend. The frontend sends commands to the backend, which in turn sends them to the implant. This supposedly allows some more flexibility in separating functions over different networks, as well as being easier for automation.
- An XML-based description format is used to describe the modules and their parameters and dependencies on the LP side.

The smell of industrialization of these kind of operations is clear from this progression. By making it easier to configure, easier to retarget, and easier to automate, it is cheaper to do more of it. If this trend continued by now there will be a sprawling ecosystem of surveillance modules, like a NSA appstore, which are habitually used on every router in sight.

Another name that is used for supposedly this malware is BUZZLIGHTYEAR (from `Firewall/OPS/userscript.FW`).

Written on September 11, 2016

Tags: eqgrp malware

Filed under Reverse-engineering