How Purism avoids Vault 7 leaked threats "Dark Matter" – Purism

3-4 minutes ⋮ 4/25/2017

Todd Weaver

Founder and CEO
PGP Fingerprint: B8CA ACEA D949 30F1 23C4 642C 23CF 2E3D 2545 14F7

Recently, WikiLeaks unloaded another lot of Vault 7 documents, under the “Dark Matter” codename. In there, other tools and techniques used by the CIA to gain persistent remote exploits on Apple devices (including Macs and iPhones) are revealed.

Most of these attacks target Apple’s EFI/UEFI firmware, therefore such infections persist even if the operating system is re-installed. This collection of threats, including *Sonic Screwdriver, Triton, Der Starke,* and *Dark Sea Skies,* all utilize the same general principle: to attack a device at the BIOS level depth, in order to seize control of all shallower levels including the operating system, applications, networking, and web access.

In addition to the EFI/UEFI exploits mentioned, there are targeted exploits such as *Night Skies* focusing on iPhones, or the *Sea Pea* rootkit focusing on Apple’s Mac OS X kernel specifically.

Night Skies is a tool that operates in the background and does not exhibit user-alerting behavior, providing upload, download and execution capability on the device. NightSkies will attempt to use any available Internet connection to beacon. Once user activity is detected, it will monitor specific directories on the phone such as the browser history file, YouTube video cache, map files cache, or mail files metadata. Night Skies can then:

- retrieve files from the iPhone including the address book, SMSes, call logs, etc.;
- send files and binaries to the iPhone (such as additional hacking tools);
- execute arbitrary commands on the iPhone;
- grant full remote command and control;
- masquerade as the standard HTTP protocol for communications;
- use XXTEA block encryption to provide secure communications;
- provide self-upgrade capability.

Sea Pea, on the other hand, is a rootkit designed for Mac OS X’s kernel, that will remain on the system unless one of the following conditions are met: the hard drive is reformatted, an upgrade is made to the next major version of OS X (i.e. 10.6), or an error is encountered (at which point SeaPea may remove itself).

What these threats continue to showcase is that EFI/UEFI is an ideal low-level backdoor to control a user’s device without their knowledge, and the leaked documents shows how widespread these threats are against any user running a EFI/UEFI BIOS.

Purism is working hard to make its products immune against these threats by designing its devices to be able to run coreboot instead EFI/UEFI. Purism also utilizes PureOS (a GNU/Linux based distribution that does not contain any mystery binaries), so the entire source code stack can be audited.

These documents continue to reinforce the fact that security is a game of depth, and the deeper you go with releasing free software where the source code can be audited, the better.

Purism has future plans of including hardware encryption tools to verify the entire boot chain, putting the entire system under a user’s control, rather than that of a bad corporation, government, spying agency, criminals, or ISPs.