VideoLAN
ORGANIZATION

Internets, March 9th, 2017

On Tuesday, the 7th of March 2017, the Wikileaks organization released a new series of documents code-named “Vault 7” that are allegedly acquired through a leak from the U.S. Central Intelligence Agency. These documents reveal the existence of a malware arsenal, including “zero days” exploits, against a wide range of products (some of them being mainstream devices and software).

One revelation[1] concerns a tool that exploits a modified old version of VLC media player. The described tool gathers documents from a computer or network and, in order to hide its activity, runs inside VLC Portable 2.1.5 on Microsoft Windows platforms. Such modified software provides a legitimate appearance (plays media files) while scanning the computer or the network for its intelligence purpose.

VideoLAN is taking these revelations very seriously but it is important to note that the leaked document does **not** describe a vulnerability that is remotely exploitable, nor is present in a normal VLC installation.

The technique used is a modification of the software’s manifest in order to force the loading of a fake dynamic library “psapi.dll”, instead of using the official Windows version. This DLL contains the malware's executable code. The attack described in the leaked document requires:

- physical access to the targeted computer,
- Microsoft Windows XP or later host system,
- and execution of the tool allegedly developed by the CIA (provided on "thumbdrive", but not exclusively).

We would like to bring to your attention that this exploit is nothing different than installing a trojaned software from an untrusted source. **The only safe source for getting VLC media player is the official VideoLAN website**[2].

Security of our users data is of prime importance. As a consequence, we have taken counter-measures to prevent malware from hiding their activity behind VLC media player. The used attack vector modification will not be possible starting from the next minor release, 2.2.5. We are also working on hardening the VLC security for the next major releases (3.x.x).

VLC media player is a free and open-source multimedia player that is being used by millions of people worldwide. It is made by the VideoLAN non-profit organization which is run by volunteers. All its members strongly believe in open source and standards.

The VideoLAN team

1 https://wikileaks.org/ciav7p1/cms/page_15729066.html
2 https://www.videolan.org