

Forum:[Hack Forums](#)

Thread: [\[NEW\] OSX Malware/RAT](#)

[BLANK] - February 21, 2018, 7:57 am

If you are interested in OSX malware, have a look at this new sample of EvilOSX that just appeared on VT.

- 1)Repo: <https://github.com/Marten4n6/EvilOSX> ...
- 2)Source and decodes: <https://ghostbin.com/paste/gugbj>
- 3)Hash: 89e5b8208daf85f549d9b7df8e2a062e47f15a5b08462a4224f73c0a6223972a

A pure python, post-exploitation, RAT (Remote Administration Tool) for macOS / OSX.

Features

- Emulate a simple terminal instance
- Undetected by anti-virus (randomized hash, HTTPS communication)
- Multi-threaded
- No client dependencies (pure python)
- Persistent
- Simple extendable module system
- Retrieve Chrome passwords
- Retrieve iCloud tokens and contacts
- Download and upload files
- iTunes iOS backup enumeration
- Retrieve browser history (Chrome and Safari)
- Attempt to get root via local privilege escalation
- Auto installer, simply run EvilOSX on your target and the rest is handled automatically

CyberStrike - February 21, 2018, 11:28 am

Great find I saw it yesterday objective-see was talking about it .. but most people here seem to like "java" rats for OSX nevermind that Safari blocks Java applets, maybe they have their target java -jar their rats.. I been saying between Metasploit/pupy/Python and BASH scripts I dunno why everyone is having such a hard time with OSX, seems that they secretly have not moved on to what works currently.

general79 - December 22, 2019, 2:34 pm

(Feb 21, 2018 08:57 AM)[BLANK] Wrote: [\[CITE\]](#) If you are interested in OSX malware, have a look at this new sample of EvilOSX that just appeared on VT.

- 1)Repo: <https://github.com/Marten4n6/EvilOSX> ...
- 2)Source and decodes: <https://ghostbin.com/paste/gugbj>
- 3)Hash: 89e5b8208daf85f549d9b7df8e2a062e47f15a5b08462a4224f73c0a6223972a

A pure python, post-exploitation, RAT (Remote Administration Tool) for macOS / OSX.

Features

- Emulate a simple terminal instance

Undetected by anti-virus (randomized hash, HTTPS communication)
Multi-threaded
No client dependencies (pure python)
Persistent
Simple extendable module system
Retrieve Chrome passwords
Retrieve iCloud tokens and contacts
Download and upload files
iTunes iOS backup enumeration
Retrieve browser history (Chrome and Safari)
Attempt to get root via local privilege escalation
Auto installer, simply run EvilOSX on your target and the rest is handled automatically
Does it work perfectly?

doomfish - December 22, 2019, 6:14 pm

Been looking for a OSX rat for a while,thanks fam.

kayla_90 - December 24, 2019, 6:51 pm

Take a look at eggshell,maybe you ind it interesting.

<https://github.com/neoneggplant/EggShell/>

kayla