OSX/Keydnap IoCs

github.com/eset/malware-ioc/tree/master/keydnap

eset

eset/malware-ioc

Indicators of Compromises (IOC) of our various investigations

14 Contributors | 0 Issues | 1k Stars | 218 Forks

For a description of Keydnap, please see the article about Keydnap on WeLiveSecurity.

Samples

Downloader

SHA-1	Filename	First seen on VirusTotal	Backdoor download URL	Decoy descri
07cd177f5baf8c1bdbbae22f1e8f03f22dfdb148	info_list.txt	2016-05-09	hxxp://dev.aneros.com/media/icloudsyncd	"Most Commo Questions"
78ba1152ef3883e63f10c3a85cbf00f2bb305a6a	screenshot_2016-06-28-01.jpg	2016-06-28	hxxp://freesafesoft.com/icloudsyncd	BlackHat-TDS screenshot
773a82343367b3d09965f6f09cc9887e7f8f01bf	screenshot.jpg	2016-05-07	hxxp://dev.aneros.com/media/icloudsyncd	Firefox 20 abo
dfdb38f1e3ca88cfc8e9a2828599a8ce94eb958c	CVdetails.doc	2016-05-03	hxxp://lovefromscratch.ca/wp-admin/css/icloudsyncd	hxxp://lovefror admin/CVdeta
2739170ed195ff1b9f00c44502a21b5613d08a58	CVdetails.doc	2016-05-03	hxxp://lovefromscratch.ca/wp-admin/css/icloudsyncd	hxxp://lovefror admin/CVdeta
e9d4523d9116b3190f2068b1be10229e96f21729	logo.jpg	2016-06-02	hxxp://dev.aneros.com/media/icloudsyncd	sanelite logo
7472102922f91a78268430510eced1059eef1770	screenshot_93242.jpg	2016-06-28	hxxp://freesafesoft.com/icloudsyncd	Some C&C pa

Backdoor

SHA-1	C&C	Version
`a4bc56f5ddbe006c9a68422a7132ad782c1aeb7b`	hxxps://g5wcesdfjzne7255.onion.to	1.3.1
`abf99129e0682d2fa40c30a1a1ad9e0c701e14a4`	hxxps://r2elajikcosf7zee.onion.to	1.3.5

A patch for UPX to unpack the samples is provided here: https://github.com/eset/malware-research/blob/master/keydnap/keydnap_upx.patch

Backdoor C&C servers

- `hxxps://g5wcesdfjzne7255.onion.to/`
- `hxxps://r2elajikcosf7zee.onion.to/`