禪

[illegible]

[illegible] SpyDleaer [illegible] 40 [illegible]

[illegible] SpyDealer [illegible].
[illegible] 40 [illegible]
[illegible].

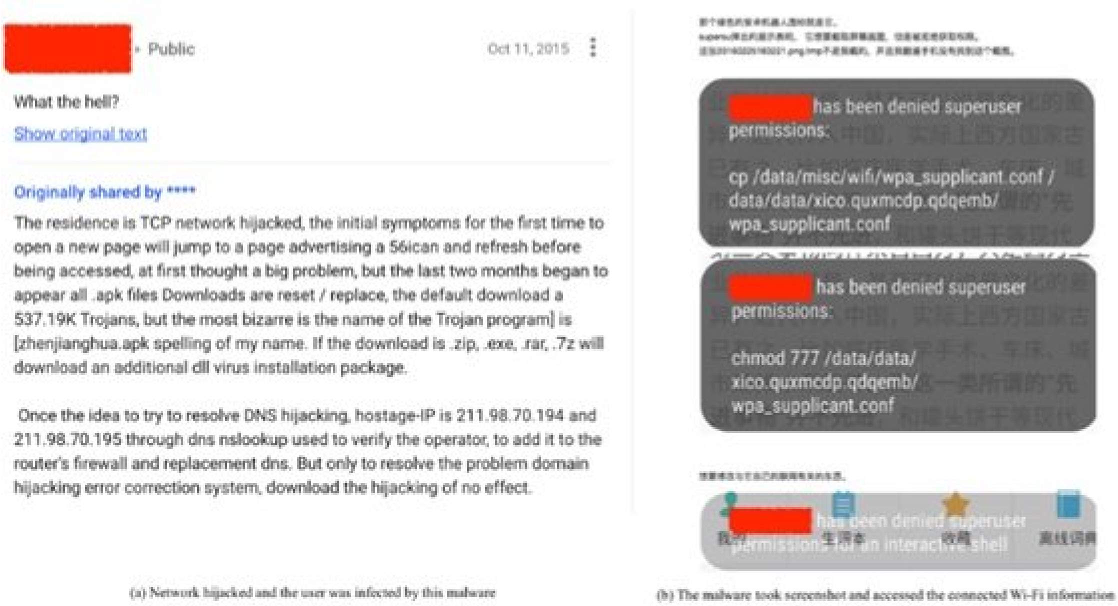
[illegible]
[illegible] Baidu Easy Root [illegible]
[illegible]
[illegible].

[illegible]

[illegible] DDoS

□□ DDoS □□□□□ □□□□□□ □□ □□□□□ □□□□□□□□ □□□□□ 18 □□□□□□□□□□ □□

□□□□□□□□□ 4.4 □□ 2.2 □□□□□□□□ □□□□ □□□□□ □□□□ □□□□□□□□ □□ □□□□□□□□□ □□□□□□ □□□□□□□ □□□□□ □□□□ □□□□□□□□□□□
□□ □□ □□□□□□□□□ □□□□□□□□□□ □□ □□□□□ 25 □□□□ □□□□□ □□□□□□ □□ □□ □□□□□□□. □□□□ □□□□□ □□□□□□□□□□ □□ □□□□ □□□□□
□□□□□□ □□ □□□□□□ □□□□ □□□□□□□□□□ □□□□□□ □□□□□□□□□□□ □□□□ □□□□□□□□□ □□□□ □□ □□□□□□. □□□□ □□□□□ □□□□□□ □□□□□
□□□□ □□□□□ □□□□□□ □□ □□□□□□□□□ □□□□ □□ □□□□□ □□□□ □□□□□□□ □□□□ □□ (broadcast) □□□□□□□□□ □□□□□□□□ □□ □□□□□□
.□□□□ □□□□□ □□□□ □□□□□□□□ □□□□□ □□ □□□□□□□□ □□□□□□□ □□□□□□□□ □□□□□□□□□□□ □□□□□□ □ □□□□□□□□□


[redacted] • Public Oct 11, 2015

What the hell?

Show original text

Originally shared by ****

The residence is TCP network hijacked, the initial symptoms for the first time to open a new page will jump to a page advertising a 56ican and refresh before being accessed, at first thought a big problem, but the last two months began to appear all .apk files Downloads are reset / replace, the default download a 537.19K Trojans, but the most bizarre is the name of the Trojan program] is [zhenjianghua.apk spelling of my name. If the download is .zip, .exe, .rar, .7z will download an additional dll virus installation package.

Once the idea to try to resolve DNS hijacking, hostage-IP is 211.98.70.194 and 211.98.70.195 through dns nslookup used to verify the operator, to add it to the router's firewall and replacement dns. But only to resolve the problem domain hijacking error correction system, download the hijacking of no effect.

(a) Network hijacked and the user was infected by this malware

[redacted] has been denied superuser permissions:

cp /data/misc/wifi/wpa_supplicant.conf /data/data/xico.quxmcdp.qdqemb/wpa_supplicant.conf

[redacted] has been denied superuser permissions:

chmod 777 /data/data/xico.quxmcdp.qdqemb/wpa_supplicant.conf

[redacted] has been denied superuser permissions for an interactive shell

(b) The malware took screenshot and accessed the connected Wi-Fi information

□□ □□□□□□ □□□□ □□ □□□□□ □□ □□□□□□□□□ □□□□ □□□□□□ □□□□□ □□□□ □□ □□□□□□ □□□□□□□□ □□□□□ □□□□□ □□□□□□□□□ □□□□ □□□□
□ UDP □□□□□□□□□□ □□ □□□□□□□□□ □□ □ □□□□ □□□□ □□ □□□□□□ □□□□□ □□□□□□□□ □□□□□□. □□□□□ □□□□□ □□ □□ □□□□□□□□□
□□□□□□ □□□□□□ □□□□□□□□□ □□□□□ □□□□ □□□□ □□□□□□□□□. □□□□□ □□□□□□ □□□□□□ □□□□□□□□ □□□□□□ □□□□□□□□□ □ TCP
□□□□□□ □□□□□□□□□ □□ □□□□□□ □□□□□□□□□ □ □□□□□□ □□□□□□ □□□□□□□□ □□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□ □□□□□□□□□
□□□□□□□□ □□□□□ □□□□□ □□□□□□□□□□ □□ □□ □□□□□□ □□□□□□□□□□ □□ □□ □□□□□□ □□ □□□□□□□□□ □□□□ □□□□□□□□ □□□□□ □□ □□
.□□□□□□□□□ □□□□ □□□□□□ □□ □□□□□□□□ □□□□□□ □□ □□□□□□□□ □□□□□ □ □□□□□ □□□□ □□ □□□□□ □□□□□□□□□ □□□□□□ □□□□□

□□□□□□□□□□ □□□□□

□□□□□□□ □□□□□□□□□□□ □□□

□□ □□□□ Humax □□□□□□□□ □□ □□□□□ □□□□ □□□□□□□□□□□

□□□□ □□ □□□□□□□□□□□□□□□ □□□□□□□ □ □□□□□□ □□□□□□□ □□□□□□□ □□□□□□□ □□ □□□□□□□□ □□□□ □□□□□□□□ □□□□□ □□□□□
□□ □□ □□□□□ □□□□□□ □ □□ □□□□□□□□□ □□□□□□□ 2015 □□□□ □□□□□□ □□ □□□□□□□□□ □□□□ □□ □□□□□ □□□□□□. □□□□ □□□□□
.□□□□ □□□□□ □□□□□ □□ □□□□ □□□□ 18 □□ □□□□□□ □□□□ □□□□□□□□□ □□ □□□□□□ □□□□□ □□□□□□ □□□□. □□ □□□□□□□□□ 2017
□□ □□□□□□□ □□□□□□□□□□ □□□□□□□. □□□□□ □□□□□ □□□□□□ □□□□□□ □□ □□□□□□□□□ □□□□» :□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□□
□□□□□□ □□□□□□□ □ □□□□□□□□□□ □□□□□□□□□ □□□□□□□ □□□□□□□□□□□ □□□□ □□□□□□ □□ □□ □□□□□□□ □□□□□□□□ □□□□□□□□ □□□□
□□□□ □□□□□□□□□ □□□□ □□ □□□□□□. □□□□□□□ □□□□□□□□□□ □ □□□□□□□□ □□□□□□□□ □□□□ □□□□ □□ □□□□□□□□ □□□□□ □□□□□□□□□
□ □□□□□□ □□□□□ □□ □□ IP □□□□□ □□□□□□ □□□□□□□□□□ □□□□□□□□ □□□□ □□□□□□ □□ □□□□□□ □□□□ □□□□□□□ □□□□□□□

[illegible] readme.txt [illegible]. [illegible] [illegible] 50 [illegible] [illegible].»

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
23:13 - 20/04/1396
[illegible]:
[illegible] - [illegible] - [illegible] - SpyDleaer - [illegible] - [illegible] - [illegible] - [illegible] - [illegible] - [illegible] - Baidu - Easy Root

---

[illegible]
[illegible]: https://www.shabakeh-mag.com/security/8642/%D8%AA%D8%B1%D9%88%D8%AC%D8%A7%D9%86-spydleaer-%D9%85%DB%8C%E2%80%8C%D8%AA%D9%88%D8%A7%D9%86%D8%AF-%D8%A7%D8%B2-40-%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C-%D8%AC%D8%A7%D8%B3%D9%88%D8%B3%DB%8C-%DA%A9%D9%86%D8%AF