Everyone sees not what they want to see

securelist.com/everyone-sees-not-what-they-want-to-see/74997/

Authors

Anton Kivva

In early March, Kaspersky Lab detected the modular Trojan Backdoor.AndroidOS.Triada which granted superuser privileges to downloaded Trojans (i.e. the payload), as well as the chance to get embedded into system processes. Soon after that, on March 15, we found one of the modules enabling a dangerous attack – spoofing URLs loaded in the browser.

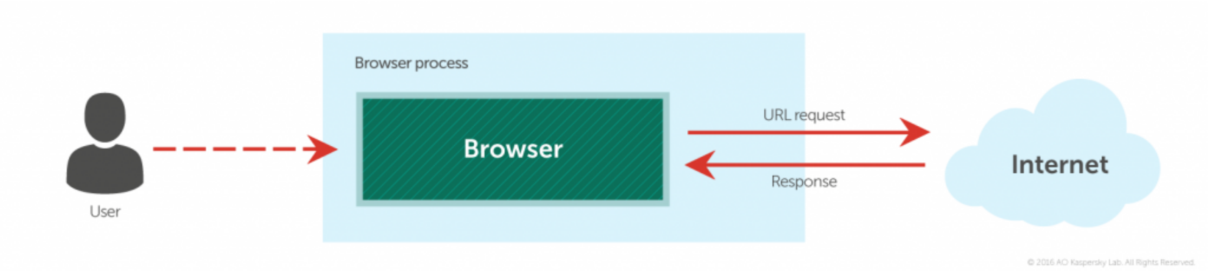
The malicious module consists of several parts and is detected by Kaspersky Lab products as Backdoor.AndroidOS.Triada.p/o/q. When it gains superuser privileges, it uses regular Linux debugging tools to embed its DLL (Triada.q, which then loads Triada.o) into the processes of the following browsers:

- **com.android.browser** (the standard Android browser)
- **com.qihoo.browser** (360 Secure Browser)
- **com.ijinshan.browser_fast** (Cheetah browser)
- **com.oupeng.browser** (Oupeng browser)

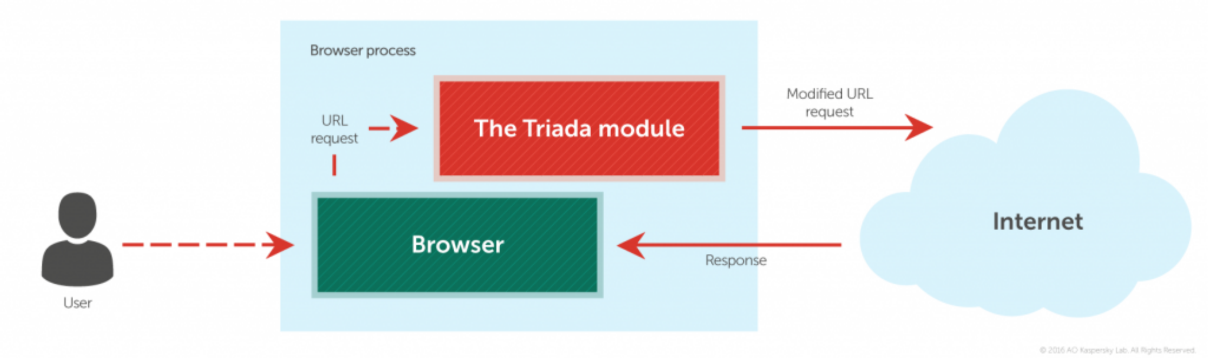
The DLL intercepts the URL the user is opening, analyzes it and, if necessary, changes it to another URL. The rules for changing the URL are downloaded from the C&C server while the module is running.

Attack sequence

In an uninfected system, the browser sends a request with a URL address to the web server via the Internet, and receives a page in response.



After infection by Triada, a DLL intercepting URLs is added to the browser's process. The URL address request finds its way into this DLL, where it is modified and sent to another web server.

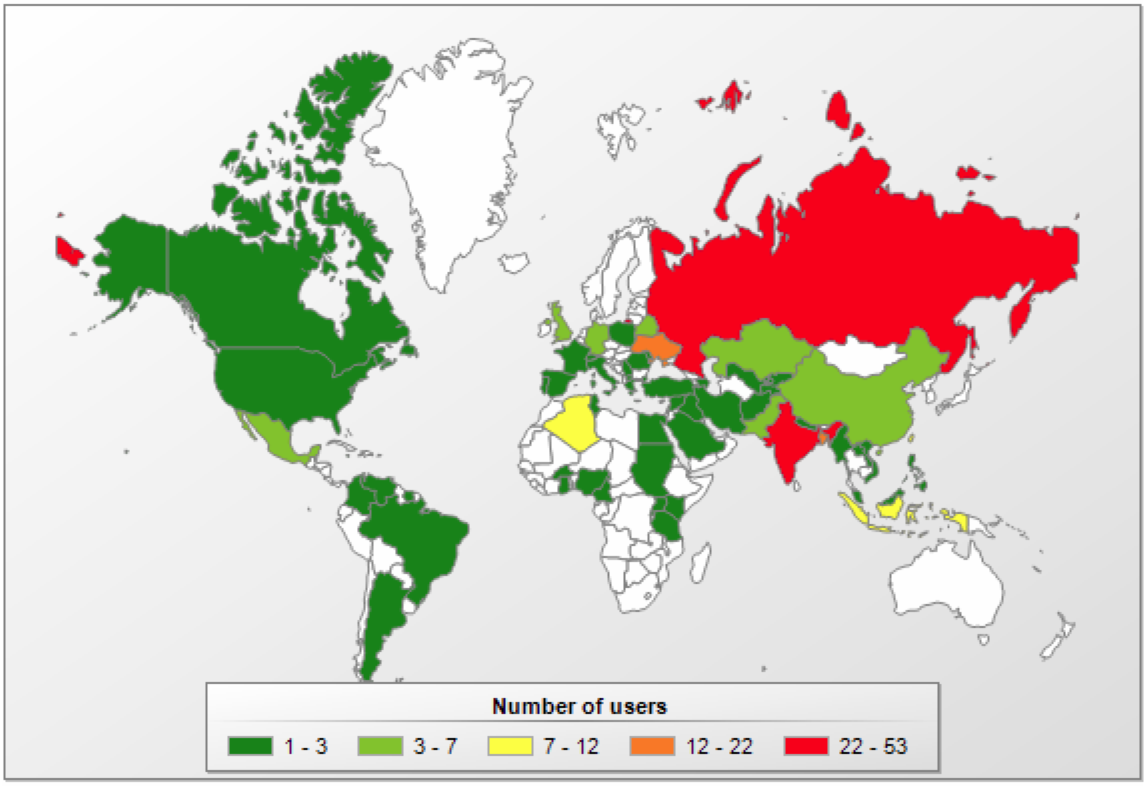


As a result, the browser receives data that's different from that requested, meaning the user ends up viewing a different page.

Now, this sequence of actions is being used by malware creators to change the standard search engine selected in the user's browser, and to replace the home page. Essentially, these actions are identical to those carried out by numerous adware programs for Windows. However, there is nothing to stop similar attacks intercepting any URL, including banking URLs, and redirecting users to phishing pages, etc. All it takes is for the cybercriminals to send the appropriate command.

During our observation period, this module attacked 247 users, and there have been no signs of a decrease in the intensity of attacks. The number of module versions is small; it appears the creators of this backdoor have decided to focus their efforts elsewhere, in spite of all the ‘promise’ shown by this technology.

The geography distribution is very similar to that of root-access malware, as this module can only function together with Triada, and is downloaded by Triada.



Number of users attacked by Backdoor.AndroidOS.Triada.p in different countries

In conclusion, we would like to note that cybercriminals specializing in Android are pretty lazy – it’s easier for them to steal money directly, for instance, with the help of Trojans that send text messages to premium-rate numbers, or spoof banking app windows. However, we have recently observed that some cybercriminals have begun to actively study the structure of the operating system, expand their repertoire of technical skills, and launch sophisticated attacks like the one we examined above.

- Google Android
- Mobile browser
- Rooting Trojan
- spoofing
- Trojan

Authors

Anton Kivva

Everyone sees not what they want to see
