CERT-EU

Cookiethief allows for social media account takeover

Threat Memo - Date: 16/03/2020 - Version: 1.0

TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cybercrime	Session hijacking Spam botnet	World	Technology	A1

Key Points

- A newly discovered malware steals cookies from social network apps such as Facebook.
- The attacker can then completely take over the victim's social network account.
- The malware abuses the trusted relationship between the victim's device and the social network.
- This attack is particularly difficult for the social network to detect.

Summary

Kaspersky has issued an analysis[1] of a new malware, Cookiethief, infecting Android phones. After stealing[2] cookies[3] from the victim's device, these are likely used to distribute spam. Cookies are an important part of today's digital applications as they allow for websites and services (such as Facebook) to identify users. The person presenting the cookie can execute tasks in the name of the user. Stealing cookies is thus an efficient way to impersonate someone. In the Facebook example, the attacker holding the cookie could post to the wall of the user, send messages in their name or conduct any user activity.

The malware bundle consists of two components aimed at stealing user cookies and a third module effectively turning the infected device into a proxy server[4] for spam posts. The initial infection vector is unknown, although Cookiethief was likely installed by other malware or pre-packed in the device firmware before purchase. See CERT-EU's Threat Memo 20-008 for an example of malware being pre-installed on mobile devices.

Cookiethief runs in the user-side[5] of the device, disguised as com.lob.roblox (this package name is shared with an innocent gaming client unrelated to this malware). It contains the paths to cookie folders for the default Android browser, Chrome browser, the Facebook app and the Facebook messenger app.

Cookiethief will then instruct Bood, a malicious network service running as root on the infected smartphone (on IP 127.0.01, port 5210) to steal the respective cookies. Bood returns these cookies to Cookiethief, who will collect them in a zip file and upload them to the Command and Control (C2) server.

The third piece of malware of this kit is Youzicheng. This is a proxy server that runs on the infected smartphone. The C2 server can send instructions to this proxy server that will forward them to its final destination in a way that is indistinguishable from legitimate requests. Platforms such as Facebook have taken measures against cookie theft, making them take into account other parameters (like IP address, device type etc.) besides cookies to further verify that a request is legitimate. Using a proxy on the infected phone effectively bypasses this protection mechanism, as the attacker's traffic will in fact come from the victim's phone.

Comments

Session hijacking through cookie stealing is not a new phenomenon. Previous appearances often included cookies being sent over clear-text (often HTTP) and thus exposed through simple data interception, Man-in-the-Middle[6] (MitM) attacks often requiring physical closeness or Cross-Site Scripting (XSS)[7], a web application vulnerability. One such example is the Firesheep technique described[8] in 2010, which involved clear-text cookies that an attacker could reuse for (albeit limited) account actions. Social networks' detection of this attack was not at today's level.

This current appearance of malware that will continuously steal a smartphone user's cookies is a new way of leveraging the trust relationship between a user's device and the social network or website. The proxy service on the victim device makes this attack particularly difficult to detect by the social network or website.

[1] https://securelist.com/cookiethief/96332/

[2] Cookie Stealing is a form of Session Hijacking, where an attacker can take abuse of an established session between a client and a server. Although the two concepts are not completely identical, for the purpose of this memo they can be considered the same.

[3] Cookies are not unlike access cards: they identify users and allow access. Cookies are used so that a user must not enter their username and password for every request to a site.

[4] Bypass station, which will make the attacker network traffic look like it is originating from the victim.

[5] Although a simplification, an application can have two sorts of rights on an Android device. Regular apps run under user-rights, important system apps run under the root-rights (much like in Linux systems), giving them much wider access to data on the system.

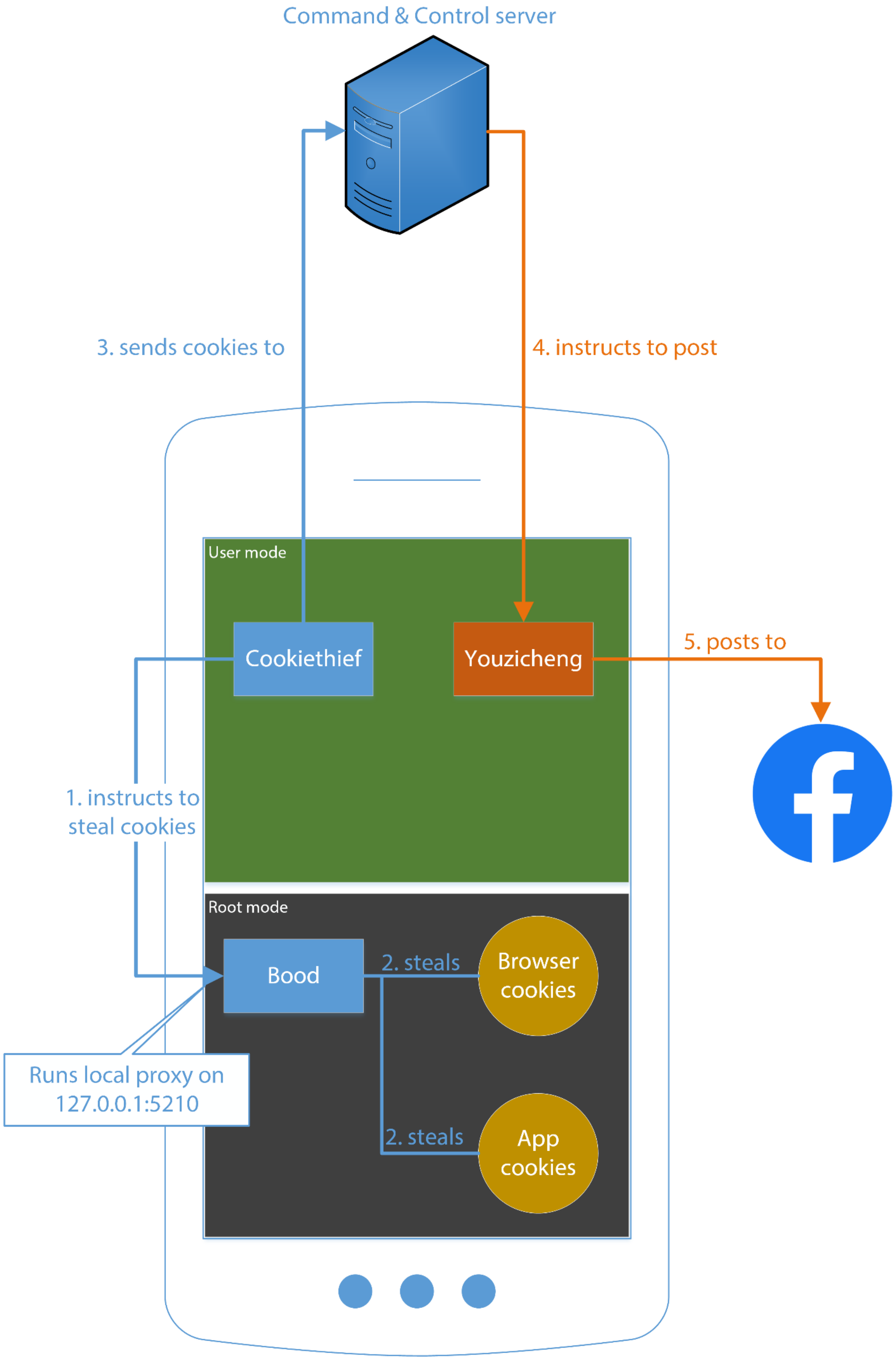
[6] An attack where the threat actor forces themself into the network traffic path of the victim.

[7] An attack where an attacker leverages the possibility to insert code into vulnerable websites that will steal the victim's cookies.

[8] https://www.pcworld.com/article/209333/how_to_hijack_facebook_using_firesheep.html

Annex I – Overview of Cookiethief components

The path in blue is the Cookiethief malware bundle. The Youzicheng malware, in orange, allows for abuse of the stolen cookies to distribute spam through the infected device.


Command & Control server
3. sends cookies to
4. instructs to post
User mode
Cookiethief
Youzicheng
5. posts to
1. instructs to steal cookies
Root mode
Bood
2. steals
Browser cookies
2. steals
App cookies
Runs local proxy on 127.0.0.1:5210