CERT-MU Advisory

CERT-MU

CERT-MU AD-2016-02

Facebook Phishing Attacks: 10,000 Victims In Two Days

Original Issue Date: 04, July 2016

Severity Rating: High

Overview:

Thousands of Facebook users have been infected by a virus through their accounts after they received a message from a Facebook friend claiming they had mentioned them in a comment. After infection, these compromised devices were used to hijack Facebook accounts in order to spread the infection through the victim's own Facebook friends and thus enabling other malicious activities. Most affected countries are Brazil, Poland, Peru, Colombia, Mexico, Ecuador, Greece, Portugal, Tunisia, Venezuela, Germany and Israel.

Description:

Thousands of Facebook users have received a message from a Facebook friend saying they had mentioned them in a comment between the 24th and 27th June 2016. The said comment is in fact a two-stage attack originated by attackers.

The first stage of the attack is initiated when the user clicked on the "mention" in a Facebook comment. A Trojan is then downloaded onto the user's computer, and seized control of their browsers, terminating the user's legitimate browser session and replacing it with a malicious one that included a tab to the authentic Facebook login page, where the user re-enters his genuine username and password.

This was designed to lure the victim back into the social network site. The first stage completed leaves the floor to the second stage attack where the infected Facebook account is taken over by the attacker.

Methodology of attack

1. A legitimate Facebook user receives a notification of a Facebook "mention" that appears to come from a friend.

2. Upon clicking on the notification, the user is re-directed to an empty post containing a link to Google Docs. This link automatically downloads a JavaScript file called *comment_27734045.jse*, which is a Trojan downloader.

3. The JavaScript file executes a batch file and once executed, the malicious script contacts its command and control (C&C) servers and start downloading files with the same image extension and then replaces the downloaded extensions with the real ones.

4. When all the files have been added, a script starts executing whereby browsers are closed, Chrome shortcuts are added to the desktop, browsers are relaunched in infected mode and some registry keys are manipulated.

5. When the victim decides to access his Facebook account, a remote script is loaded from the C&C server and executes on the client-side. The file is responsible for taking over the Facebook account and spreading the malware to other Facebook users.

6. Following a successful login attempt, the JavaScript file data.js is loaded and redirects the user to a page that suggests in Spanish that *"Before logging back into your account it is recommended to clear your cookies. It can be done via the Settings menu in Google Chrome, watch this tutorial if don't know how."* The attackers make this request to get new user-session identifiers.

7. After logging in, the attack is executed and the user's entire Facebook list is notified by the victim about a new URL. Upon clicking on this URL, the user's friends will also become malware hosts and the infection process will loop again, through their friends.

Impact of the attack

1. Successful exploitation can allow the attacker to impersonate the user, change privacy settings, extract date and allowing it to spread the infection through the victim's Facebook friends or undertake other malicious activity such as spam, identity theft and generating fraudulent 'likes' and 'shares'.

2. The malware tried to protect itself by black-listing access to certain websites, such as those belonging to security software vendors.

3. The malware acts as a Man-In-The-Middle and can capture the entire traffic between the victim and the servers he request data from. This allows the actor to

steal data and redirect it to his command and control servers or wrap the data in a log file and send it over a different channel.

Affected System:

- Windows-based computers with access to Facebook

Solution

Facebook has already mitigated this threat and is blocking techniques used to spread malware from infected computers. According to Facebook, no further infection attempts have been observed. Google has also removed at least one of the culprit extensions from the Chrome Web Store.

In case of infections, the following is recommended:

- Logout from your Facebook account.
- Close the browser and disconnect the network cable from your computer.
- Have your computer checked and clean out any remaining malware.
- Install an updated anti-virus program.

Best Practices

As part of normal best practices, the following is strongly recommended:

- Install an antimalware solution on all devices and keep OS software up-to-date.
- Avoid clicking on links in messages from people you do not know, or in unexpected messages from friends.
- Exercise caution at all times when online and on social media networks: if something looks even slightly suspicious, it probably is.
- Apply appropriate privacy settings.

References:

Securelist

https://securelist.com/blog/incidents/75237/facebook-malware-tag-me-if-you-can/

Kaspersky

http://www.kaspersky.com/about/news/virus/2016/10000-Victims-in-Two-Days

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Please note that the members who do not want to receive the security alert, can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu