PWS:HTML/Phishbank.A

Article URL
malware.php?mal_id=19882524724fe40c00e49fe9.77284331

Author
SecurityHome.eu

Published: 22 June 2012

Aliases :

PWS:HTML/Phishbank.A

is also known as *Mal/ObfJS-B (Sophos)*

.

Explanation :

PWS:HTML/Phishbank.A is a personal-information stealing malware, that may be presented in a variety of ways, including:

* As a webpage that you may receive as a link in an email
* As an attachment sent in spam email
* In a pop-up advertisement
* As embedded or inline advertising within legitimate webpages

The HTML page contains obfuscated JavaScript, and may arrive as a file using the name "Application.htm".

If you open this file in a browser, the malware displays a web-form similar to the following:

The web-form invites you to enter your personal information to become a paid 'mystery shopper'.

The personal information you enter may then be used to involve you in more elaborate phishing scams.

When you click the "Register" button, any information you have filled in is sent to a remote host at:

pkmytung.com/<snip>/m.php

The PHP script than redirects the page to google.com.

Analysis by Oleg Petrovsky

Last update 22 June 2012