MA-416.092014 : MyCERT Alert - Banker Malware Targeting Malaysian Internet Banking User

Date Published: 23 September 2014
1st Revision: 25 September 2014

1.0 Introduction

MyCERT had received several reports regarding a malware that targets Malaysian Internet banking customers. Based on our initial analysis, we found this campaign uses the Zeus banking malware family as its Modus Operandi in this campaign.

Attacker will infect victim's computers with Zeus banker malware which will inject modified fake contents or page while a user is browsing a legitimate online banking website.

2.0 Affected Systems

Based on our initial analysis of a sample incident, we found the below is the affected system:

2.1 Smartphone running on Android
2.2 Vulnerable and unpatched Windows Operating System

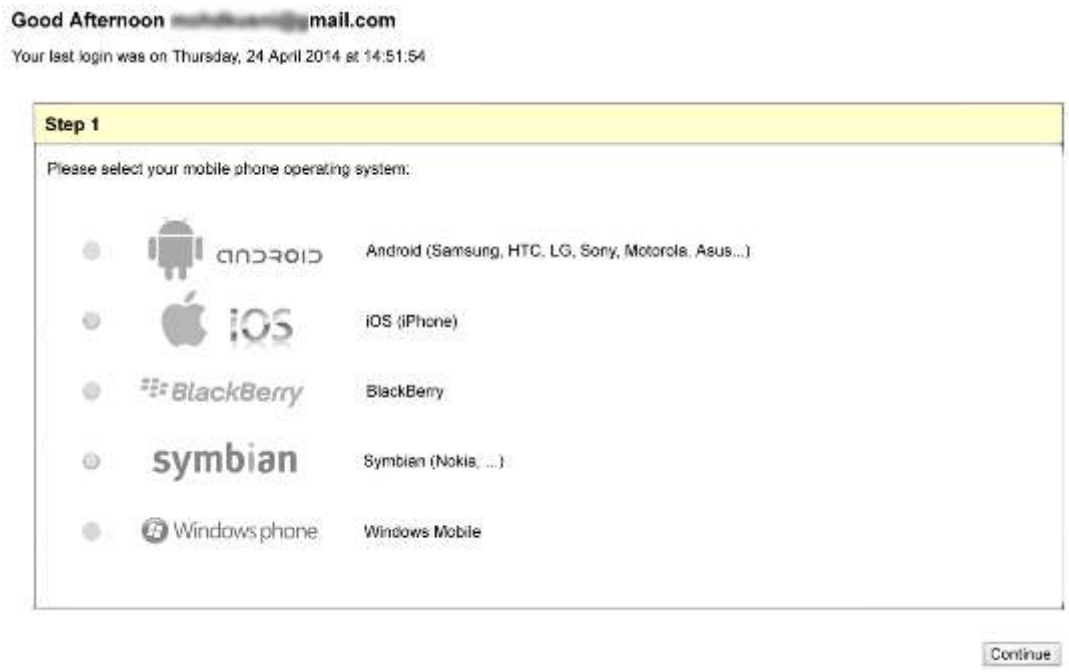
3.0 Impact

3.1 The malware will inject a modified fake contents that looks like a real online banking website when user is browsing a legitimate online banking website, in which the content will request victim's smartphone operating system and mobile number.

3.2 The malware will SMS to the smartphone a malicious APK and infect the smart phone in order to establish callback with the attackers for further instructions.

4.0 Technical Details

Attacker will infect victim's computers with Zeus banker malware which will inject modified contents when users is browsing a legitimate online banking website, as shown in the below sample image of the injected page.



The modified content will prompt user to choose their smartphone Operating System and provide their phone number as well. With the phone number information, attacker will send SMS containing link to a malicious APK known as Zitmo malware to the victim's smartphone, purportedly to be a an online banking verification certificate.

Once the APK is installed in the smartphone, a popup message will appear and the Zitmo malware will attempt to make callback to attacker through SMS and wait for further instruction.

Few days later, attacker will login to victim's online banking account using the stolen credentials and perform online transaction successfully by using intercepted TAC number.

The mobile malware has been discovered since late September 2010 but first time being used in malware campaign targeting Malaysian Online Banking users.

5.0 Recommendation

5.1 For laptop/PC User:

1) Install robust anti-virus, anti-spyware and firewall software on your computer and other devices and configure it to update regularly.

2) Perform regular scans of your systems for malware and other risks.

3) Operating system providers such as Microsoft, periodically releases updates and patches that improve the security of your operating system. You should periodically check for these updates and keep your system current or configure it to do so automatically.

4) When accessing to online banking, make sure there is no pop-up/window that requires personal info such as credit card number, smartphone platform(Android/iOS) etc. Do not enter those information if required.

5) Use only a dedicated computer or laptop to do online banking

6) If you suspect your bank account has been compromised or spot any activity you have not authorized, please notify your banking provider immediately.

7) Please ensure you logout properly at the end of each session by clicking log-out button. Do not exit by simply closing the browser window.

8) If you come across anything suspicious when you do banking online such as unusual web pages asking for banking information, notify your bank provider immediately.

9) Never respond to any email/advertisements requesting you to provide your login details or log in via a link sent in an email/applications. The bank will never send you a mail or provide links in any applications like that, and such a request is likely to be a phishing attempt.

5.2) For Smartphone Users:

1) Verify an app's permission and the app's author or publisher before installing it.

2) Do not click on adware or suspicious URL sent through SMS/messaging services. Malicious program could be attached to collect user's information.

3) Since URL on mobile site appears differently from desktop browser, make sure to verify it first.

4) Always run a reputable anti-virus on your smartphone/mobile devices, and keep it up to date regularly.

5) Don't use public Wi-Fi networks for bank transactions and turn off Bluetooth connection when not in use. These can be open windows for eavesdroppers intercepting the transaction or installing spyware and other malware on user's smartphone/tablet.

6) Update the operating system and applications on smartphone/tablet, including the browser, in order to avoid any malicious exploits of security holes in out-dates versions.

7) Do not root or otherwise 'Jailbreak' your phone; avoid side loading (installing from non-official sources) when you can. If you do install Android software from a source other than the Market, be sure that it is coming from a reputable source.

6.0 References

6.1. Kapersky report on Zitmo malware

6.2. ATSEngine