1 December 2015

ABS ISSUES CONSUMER ADVISORY ON MALWARE TARGETING MOBILE BANKING

Singapore – The Association of Banks in Singapore (ABS) alerts consumers of incidences of malware infection on Android smartphones used by mobile banking customers that have been reported over the past couple of months. Until recently, the malware attacks were on internet banking via desktop computers or laptops. Consumers are asked to be vigilant when using their smartphones for mobile banking.

Mobile phones or smartphones are more than a communications device these days. Banks and financial institutions have also made banking services accessible to their customers on their smartphones via mobile applications. The major retail banks in Singapore have seen an increase of mobile banking customers from 1.5 million in 2013 to 2.4 million in 2015. At the same time, cybercriminals are turning towards mobile malware to exploit consumers' smartphones to commit fraud.

Malware or "malicious software" is any software that is used to disrupt operations, gather sensitive information or gain access to the smartphone. Smartphones are infected by malware when customers install applications from unauthorised/illegitimate applications laced with malware. Once the malware infects a customer's smartphone, it resides in the smartphone. The malware can then masquerade as the smartphone user to snoop and steal data, and transact mobile banking as if the owner was doing it.

According to the Motive Security Labs H2 2014 Malware Report[1], mobile malware infections continued to accelerate, with an increase of 25% in 2014, compared with 20% for 2013 globally. The report estimated that about 16 million mobile devices worldwide were infected by malware. The infections were split 50-50 between Android devices and Windows computers, with less than 1% coming from other devices such as the iPhone and Blackberry. The Symantec Intelligence Report[2] also shared that the Finance, Insurance, & Real Estate sector was the most targeted sector in October 2015, comprising 69% of all malware attacks. The Microsoft Security Intelligence Report[3] advises that Singapore's malware infection rate overall has been consistently lower than the worldwide average.

[1] https://www.alcatel-lucent.com/solutions/malware-reports

[2] http://www.symantec.com/security_response/publications/monthlythreatreport.jsp

[3] http://www.microsoft.com/security/sir/archive/default.aspx

Customers should be careful to not let their smartphones be infected by malware. They should

(1) install an anti-virus/anti-malware software on the smartphone
(2) only install applications from trusted sources such as “Google Play”, or other reputable app stores, and avoid downloading pirated applications from unauthorised/illegitimate app stores, or random download locations on the internet as the latter could be laced with malware.
(3) only click on hyperlinks from messages and emails if they are from a trusted source.
(4) not “root” or “jailbreak” the smartphone, as this could compromise smartphone security.

Said Mrs Ong-Ang Ai Boon, Director of ABS: “ABS would like to remind mobile banking customers that smartphones are as susceptible to malware as desktop computers or laptops. Consumers are reminded to download applications only from trusted sources. As cybercriminals’ mode of operations and the malware are constantly evolving, visit your bank’s website for more information, latest updates and malware signs to watch out for.”

ABS would also like to draw attention to a specific malware that disguises itself as a software update for Android smartphones, or as a service for updating WhatsApp. In the latter, a pop-up advertisement encourages consumers to tap it and download a “new” version of the program or risk losing access to the service. After downloading the “update”, the application will prompt the customer to input confidential information, such as credit card details, which could then be used to commit fraud.

More details on this malware that has infected mobile banking users here, and a list of general tips on securing smartphones against malware attacks can be found in the Appendix.

ENDS

Contact details:

Ong-Ang Ai Boon, Mrs
Director
The Association of Banks in Singapore
Tel: (65) 6224 4300
E-mail: *banks@abs.org.sg*

John Lim, CEO
Reputation Management Associates
Tel: (65) 6298 2520
Mobile: (65) 9756 3582
E-mail: *jlim@reputation.com.sg*

About The Association of Banks in Singapore:

The Association of Banks in Singapore (ABS) plays an active role in promoting and representing the interests of the banking community in Singapore. In doing so, ABS works closely with the relevant government authorities towards the development of a sound financial system in Singapore. Since its establishment in 1973, ABS has promoted common understanding among its members and projected

a unifying voice on banking issues. It has brought its members closer together through various guidelines and banking practices as well as the support of projects of mutual benefit to face the challenges of the financial and banking community in Singapore. Today, ABS has a membership of 158 local and foreign banks. Further information on ABS is available on the website: www.abs.org.sg.

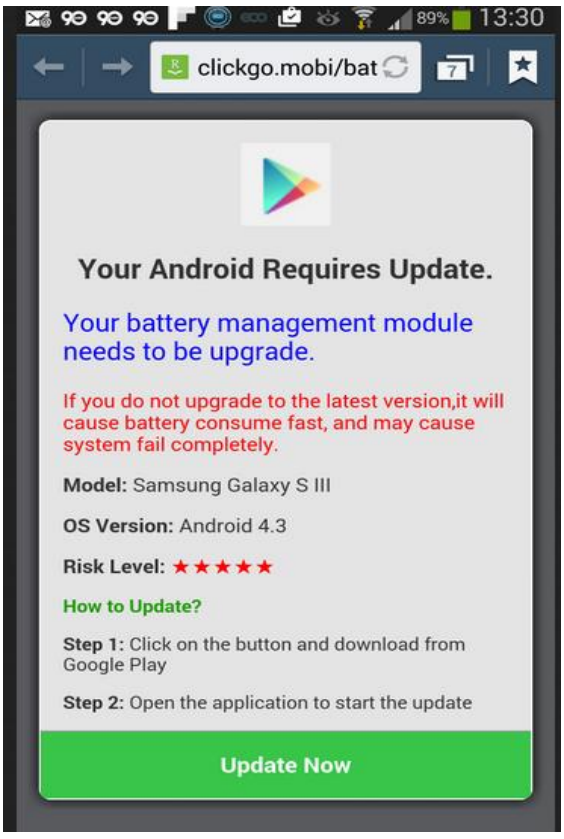
Appendix: Consumer Advisory on Malware Targeting Mobile Banking Customers

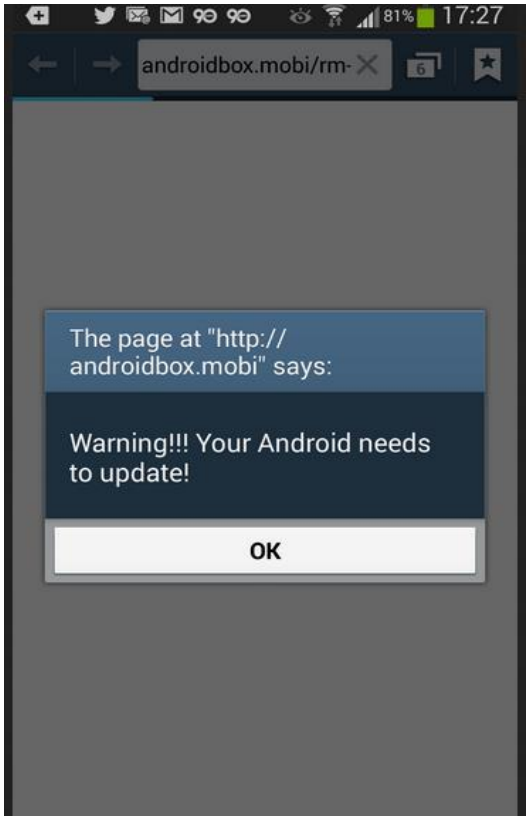
How does a smartphone get infected by this malware?

The malware infects a smartphone when an application laced with malware is downloaded onto the smartphone. Consumers would typically be prompted to install unfamiliar apps, grant permission to certain apps or update existing apps. Those consumers who go on to do so could end up having the malware infect their smartphones.

Once loaded onto the smartphone, the malware can access critical information such as credit card details and SMS One-Time-Password (OTP) that are required for online purchases.

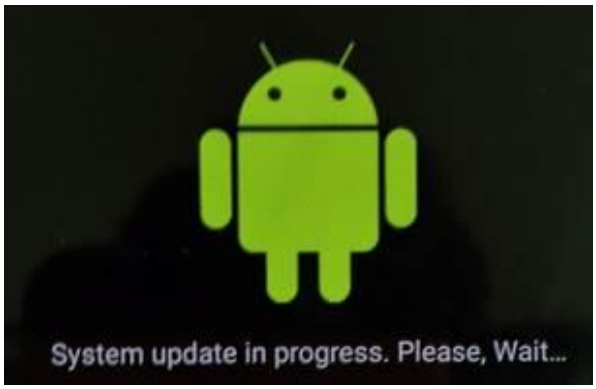
The screenshots below are samples of how consumers were prompted to perform "application updates", which had resulted in their smartphones being infected by the malware.





Once the consumer clicked on the link/button within the message, he was directed to enter his credit card information for payment to upgrade WhatsApp.

Soon after the credit card information was entered, a "System Update" icon (see screenshot below) appeared. This was when the malware "took over" the smartphone to use the credit card information and intercept the SMS OTP sent to the smartphone to make fraudulent online purchases.



What should I do if my smartphone is infected by malware?

1. Do not use your smartphone to perform any banking transactions.
2. Install an anti-malware application on your smartphone. Anti-malware apps would normally be able to detect and remove malware. Depending on the extent of the damage you may need to reset your smartphone using “factory reset” your smartphone to remove the malware.

How can I prevent my smartphone from being infected by malware?

1. Do not download pirated applications from unauthorised or illegitimate app stores, or random download locations on the internet. Do not click on hyperlinks from messages, emails if you are unsure of the source.
2. Be alert especially if a screen on your mobile device suddenly pops up and asks for your confidential information, even if you did not open your applications or initiate any activity;
3. If there is an update for your device make sure you download and install it. This is because manufacturers, carriers, and Google are constantly pushing out updates with bug fixes, enhancements, and new features that can make your device more secure.
4. Avoid using public/unsecured WiFi when transacting with sensitive information or mobile internet banking. Cybercriminals can use these WiFi networks to snoop and pry on your smartphone.
5. Secure your smartphone with a password, pin or a relevant mechanism to prevent unauthorised use.
6. As the fraudsters’ mode of operations and the malware could constantly be evolving, do visit your bank’s websites for more information and latest updates on other signs to watch out for.

How do I know if my phone is infected with malware?

1. **Bad Battery Life**: Whether malware is hiding in plain sight, pretending to be a regular application, or trying to stay hidden from the user, abnormal battery drainage can often give away the presence of an infection. This could be due to malware utilising the system resources to perform its actions (e.g., communicating with a command and control server) in the background.

2. **Dropped Calls and Disruptions**: Mobile malware can affect outgoing and incoming calls. Dropped calls or strange disruptions during a conversation could be the interference of mobile malware. Call your service provider to determine if the dropped calls are its fault. If it's not, it is possible that someone or something is trying to eavesdrop on conversations or perform other suspicious activities.
3. **Unusual Phone/Data Bills**: Android malware often infects devices and starts sending SMS text messages to premium-rated numbers. Some malware may send an SMS message just once a month to avoid suspicions, or they may uninstall themselves after punching a serious hole in your budget. Malware can also smuggle data from your device to a third-party. Significant changes in your download or upload patterns could be a sign that someone or something has control over your device.
4. **Clogged Performance**: Malware infestation may cause serious performance problems as it tries to read, write or broadcast data from your smartphone. Checking RAM (Random Access Memory) use or CPU load could reveal the presence of malware that's actively running on the device.
5. **Suspicious Applications:** If you notice an unusual change in the look-and-feel of your smartphone (such as new icons or applications), malware may have infected your phone.