BANK PERTANIAN MALAYSIA BERHAD 200801010522 (811810-U)

AGRO BANK

NOTICE

ALERT
SMSSpy MALWARE CAMPAIGN

SMSSpy is a malicious software (malware) masquerading as a legitimate application. This malware is developed to steal personal information of Internet Banking users, particularly those with Android mobile.

SMSSpy TARGETING ANDROID USERS IN MALAYSIA, THROUGH TWO (2) CAMPAIGNS

CAMPAIGN ONE

PRETENDING TO BE LAW ENFORCECERS

An imposter (that pretending to be law enforcecers) call the victim, informing them that they were involved in a crime, or their financial amount is overdue.

The victim will be directed to pay a sum a of money to cancel the action by downloading malicious Android applications to complete the payment process.

THE EFFECT

The perpetrator **steals the victims' bank credentials, money, and their sensitive personal information.**

PREVENTIVE STEPS

1. **Do not click on adware or suspicious** URLs sent via SMS and message services.
2. **Avoid downloading and installing application from unofficial sources.** If you need to install Android application from other than trusted sources, do ensure it comes from a reputable and reliable source.
3. **Verify the owner** or **the publisher of the application** before installing the same on your mobile device and **its access permission request.**
4. **Always use reputable antivirus software on your smartphone/ mobile device and keep it up to date.**
5. **Always update** the operating system and applications on **smartphones/ mobile devices**, including **web browser software,** to **avoid any exploitation of vulnerabilities found in older versions of software.**

BANK PERTANIAN MALAYSIA BERHAD 200801010522 (811810-U)

AGRO BANK

NOTICE

ALERT
SMSSpy MALWARE CAMPAIGN

SMSSpy TARGETING ANDROID USERS IN MALAYSIA, THROUGH TWO (2) CAMPAIGNS

CAMPAIGN TWO

FAKE WEBSITE

Perpetrators pretend to be a legitimate service provider by using **ads on Facebook** to influence potential victims into downloading malicious Android software (malware) from fake websites.

EXAMPLE

Eight (8) websites masquerading as valid service providers are **Grabmaid, Maria's Cleaning, Maid4u, YourMaid, Maideasy, MaidACall, MyMaidKL** and **PetsMore.**

WHAT TO DO IF YOUR DEVICE HAS BEEN INFECTED?

Two (2) signs the device has been infected by the malicious software;

- **You tap an app, and it doesn't open**
- **You try to uninstall the app and instead shown an error message**

If you think an application may be malware, reset the phone to factory settings.

SUPPORT & INQUIRY

Email:

- cyber999@cybersecurity. my

Contact Us:

- Agrobank Contact Centre: 1-300-88-2476

12 September 2022

BANK PERTANIAN MALAYSIA BERHAD 200801010522 (811810-U)

AGRO BANK

PERBANKAN ISLAM

NOTIS

AWAS
KEMPEN PERISIAN HASAD (MALWARE) SMSSpy

SMSSpy adalah perisian berniat jahat (malware) yang menyamar sebagai aplikasi yang sah. Perisian hasad ini dibangunkan untuk mencuri maklumat peribadi pengguna perbankan internet, terutamanya mereka yang menggunakan telefon bimbit/ peranti mudah alih dengan perisian Android.

PERISIAN HASAD (MALWARE) SMSSpy MENYASARKAN PENGGUNA TELEFON ANDROID DI MALAYSIA MELALUI DUA (2) KEMPEN

KEMPEN PERTAMA

MENYAMAR SEBAGAI PENGUATKUASA UNDANG-UNDANG

Pelaku (yang berpura-pura menjadi Penguatkuasa Undang-undang) membuat panggilan kepada mangsa, memaklumkan bahawa mereka terlibat dalam sesuatu jenayah atau mempunyai bayaran kewangan yang tertunggak.

Mangsa akan diarahkan untuk membayar sejumlah wang bagi membatalkan tindakan tersebut dengan memuat turun aplikasi Android berniat jahat (malware) untuk menyelesaikan proses pembayaran.

IMPAK

Pelaku
mencuri maklumat peribadi, maklumat perbankan, wang dan maklumat peribadi yang sensitif daripada mangsa.

LANGKAH-LANGKAH PENCEGAHAN

1. **Jangan klik pada perisian iklan (adware)** atau URL yang mencurigakan yang dihantar melalui perkhidmatan SMS dan aplikasi mesej.
2. **Elakkan memuat turun dan memasang aplikasi daripada sumber tidak rasmi.** Jika anda perlu memuat turun perisian Android selain daripada sumber yang sah, pastikan ia datang daripada sumber yang mempunyai reputasi yang baik dan boleh dipercayai.
3. **Sahkan pemilik** atau **penerbit aplikasi tersebut** dan juga **kebenaran capaian aplikasi** sebelum memuat turun pada telefon bimbit anda.
4. **Sentiasa menggunakan perisian anti-virus yang bereputasi baik di dalam telefon pintar/ peranti mudah alih anda dan pastikan ia sentiasa dikemas kini.**
5. **Sentiasa kemas kini** sistem pengendalian dan aplikasi pada **telefon pintar/ peranti mudah alih anda** termasuk **perisian pelayar laman sesawang (browser)**, untuk **mengelakkan sebarang eksploitasi ke atas kelemahan yang terdapat dalam perisian versi lama.**

BANK PERTANIAN MALAYSIA BERHAD 200801010522 (811810-U)

AGRO BANK

NOTIS

AWAS
KEMPEN PERISIAN HASAD (MALWARE) SMSSpy

PERISIAN HASAD (MALWARE) SMSSpy MENYASARKAN PENGGUNA TELEFON ANDROID DI MALAYSIA MELALUI DUA (2) KEMPEN

KEMPEN KEDUA

LAMAN SESAWANG PALSU

Pelaku cuba untuk mencuri maklumat peribadi perbankan mangsa melalui laman sesawang palsu yang berselindung di sebalik laman penyedia perkhidmatan yang sah. Selain itu, pelaku juga menggunakan **iklan di Facebook** untuk mempengaruhi bakal mangsa agar memuat turun perisian hasad (malware) Android daripada laman sesawang palsu.

CONTOH

Terdapat **lapan (8) laman sesawang** yang menyamar sebagai penyedia perkhidmatan dalam bidang perkhidmatan pembersihan (hanya di Malaysia) seperti **Grabmaid, Maria's Cleaning, Maid4u, YourMaid, Maideasy, MaidACall** dan **MyMaidKL** serta **PetsMore** (kedai haiwan peliharaan).

APA YANG PERLU DILAKUKAN JIKA PERANTI ANDA TELAH DIJANGKITI?

Terdapat **dua (2) tanda peranti** telah dijangkiti oleh perisian hasad (malware);

- **Anda mengetik aplikasi dan ia tidak dibuka.**
- **Anda cuba menyahpasang aplikasi dan sebaliknya menunjukkan mesej ralat**

Jika anda fikir sesuatu aplikasi boleh menjadi perisian hasad (malware), tetapkan semula telefon anda kepada tetapan semula kilang (factory reset setting)

SOKONGAN DAN PERTANYAAN

E-mel:

- cyber999@cybersecurity. my

Hubungi Kami:

- Pusat Panggilan Agrobank: 1-300-88-2476

12 September 2022