Media Title : Harian Metro
Headline : Empat langkah utama jerat mangsa
Selepas ‘page error’ wang RM20k lesap
Suspek dapat kawalan penuh fungsi di SMS
Date : 31 July 2023
Section : Lokal
Page : 3

Empat langkah utama jerat mangsa

Kuala Lumpur: Sindiket penipuan fail APK biasanya menggunakan empat ‘langkah’ umum untuk memanipulasinya sebelum memperdayakan mangsanya.

Presiden Persatuan Pengguna Siber Malaysia (MCCA) Siraj Jalil berkata, empat langkah terbabit adalah perisian hasad atau malware, phishing (memancing data), langganan ke perkhidmatan premium tanpa keizinan dan penipuan iklan.

Menurutnya, *malware* memberi keupayaan kepada penipu untuk mengakses data peranti pengguna.

“*Phishing* memberi keupayaan scammer mendapatkan maklumat sulit seperti data pengguna atau ID dan kata kunci e-mel, akaun perbankan dan lain-lain.

“Langganan ke perkhidmatan premium tanpa keizinan pula adalah taktik scammer untuk menjerat mangsa dengan langganan bulanan tanpa mangsa sedar hingg pada waktu membayar bil,” katanya.

Siraj berkata, penipuan iklan ini seperti *spam* di mana setiap kali menggunakan aplikasi itu boleh menyebabkan prestasi peranti mangsa merosot.

Selepas 'page error' wang RM20k lesap

Kuala Lumpur: "Pada mulanya saya melihat satu iklan mengenai pakej perkhidmatan saluran televisyen yang murah di Facebook (FB) dan tertarik dengannya, tanpa berfikir panjang saya terus menghubungi pengiklan terbabit," kata mangsa penipuan fail APK yang ingin dikenali sebagai Ramli, 35.

Menurutnya, selepas menghubungi individu terbabit melalui WhatsApp, dia diberi tawaran pakej murah dan jika bersetuju perlu memuat naik satu aplikasi yang diberikan bagi memulakan proses pembeliannya.

"Saya yang tidak mengesyaki apa-apa memuat naik aplikasi diberi di telefon pintar dan terus mengikut arahan diberikan.

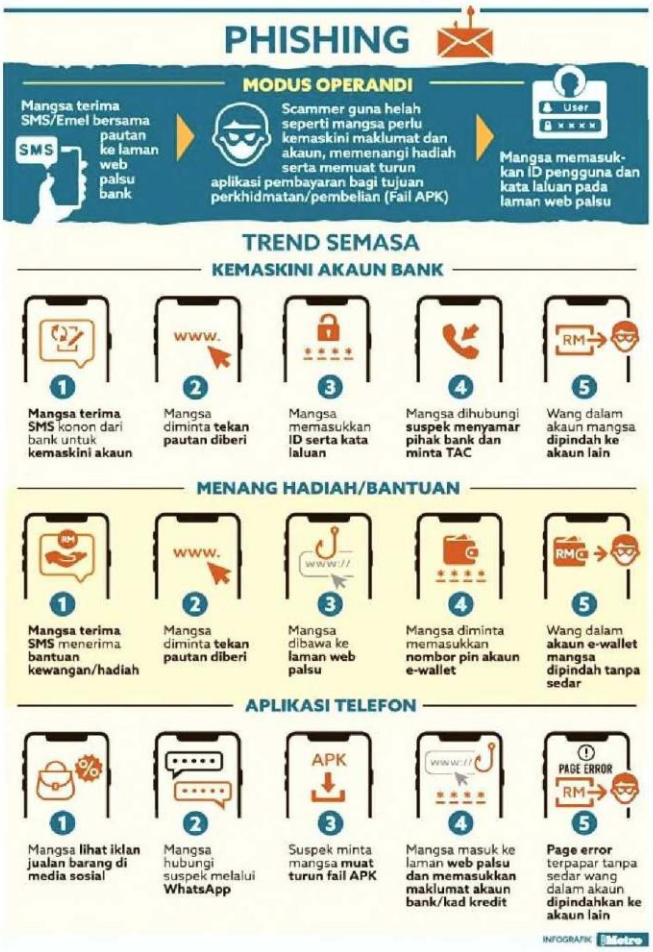
"Saya kemudian menerima mesej menerusi sistem pesanan ringkas (SMS) sebelum diarah mendaftar bagi mendapatkan akses," katanya.

Ramli berkata, dia diminta memasukkan nama, nombor kad pengenalan, e-mel, butiran kad kredit dan butiran perbankan dalam talian.

"Selepas mengisi semua maklumat itu, saya diminta menekan butang hantar namun selepas itu tiba-tiba ia menjadi *page error*.

"Saya mula berasa pelik dan cuba buka sekali lagi namun tetap tidak berjaya...malah lebih mengejutkan apabila saya menyemak baki wang di bank dan mendapati simpanan sebanyak RM20,000 lesap," katanya.

Menurutnya, dia cuba menghubungi semula individu terbabit namun gagal dan akhirnya mula menyedari dirinya ditipu.



> *Saya kemudian menerima mesej menerusi sistem pesanan ringkas (SMS) sebelum diarah mendaftar bagi mendapatkan akses"*
>
> ***Ramli***

Suspek dapat kawalan penuh fungsi di SMS

Kuala Lumpur: Pengaruhi mangsa untuk membeli dan tertarik dengan tawaran murah menjadi taktik sindiket penipuan fail APK memerangkap mangsa yang menyebabkan kerugian ratusan ribu ringgit.

Pengarah Jabatan Siasatan Jenayah Komersial (JSJK) Datuk Seri Ramli Mohamed Yoosuf berkata, mangsa terpedaya akan menghubungi suspek sebelum sindiket meyakinkan mangsa memuat turun aplikasi dari sumber tidak diketahui melalui daripada *link* atau pelokasi sumber seragam (URL) yang diberikan.

Menurutnya, selepas aplikasi mula 'masuk' dalam telefon pintar mangsa, mereka biasanya membenarkan segala permohonan kebenaran daripadanya.

"Selepas mangsa memberi kebenaran kepada aplikasi terbabit, suspek akan dapat kawalan penuh fungsi penerimaan sistem pesanan ringkas (SMS) dalam telefon pintar mangsa.

"Apabila mangsa buat pembelian di dalam aplikasi terbabit dan selepas barang dimasukkan ke *add to cart*, mangsa akan buat daftar keluar dan membuat bayaran menggunakan perbankan dalam talian atau kad kredit," katanya secara eksklusif kepada Harian Metro.

Ramli berkata, apabila kata kunci *(password)* dan segala maklumat mangsa dimasukkan, kegiatan *phishing* dilaksana untuk mendapatkan butiran seperti nama pengguna, kata kunci, nombor kad kredit dan kod pengesahan kad (CVC) atau nilai pengesahan kad (CVV).

"Dengan kawalan penuh SMS dan maklumat perbankan mangsa, suspek boleh pindah duit mangsa melalui perbankan dalam talian dan menggunakan akaun bank mangsa sebagai akaun *mule* untuk membuat *layering*.

"Orang ramai dinasihat nyah pasang *(uninstall)* aplikasi terbabit secepat mungkin dan membuat laporan polis bagi pihak berkuasa mengambil tindakan," katanya.