# PROSES PHISHING

## Mangsa

1. Komputer atau telefon pintar mangsa akan dijangkiti virus jenis Zeus Trojan
2. Apabila mangsa mendaftar masuk ke dalam perbankan Internet dengan username dan kata laluan, virus akan aktif
3. Virus akan memaparkan pautan palsu yang mengarahkan mangsa memasukkan nombor telefon, maklumat peribadi dan sistem telefon pintar digunakan (Blackberry, Android, Apple iOS, Symbian dan Windows Phone)
4. Mangsa akan menerima pautan URL melalui SMS dan diarahkan klik pada pautan
5. Apabila mangsa klik, satu sijil palsu bersama nombor kod akan dipaparkan. Mangsa dikehendaki memasukkan nombor kod di dalam laman perbankan internet itu untuk mengesahkan mereka memasukkan nombor telefon sebenar
6. Program akan dimuat turun di dalam telefon pintar mangsa dengan ikon bank berkaitan tanpa mangsa sedari itu ia berfungsi sebagai SMS Stealer yang menghantar nombor TAC kepada suspek

## Sindiket

Mencari pemegang akaun (keldai akaun) dengan menawarkan kerja sambilan kepada lelaki atau wanita tempatan

## Keldai Akaun

1. Pemegang akaun bekerja secara sambilan
2. Menerima komisen antara lima dan 10 peratus
3. Menerima arahan dan cara kerja melalui kiriman emel
4. Akan mengeluarkan wang (disyaki milik mangsa) dari bank dan menghantar kepada sindiket melalui Western Union

# 'Virus' curi duit

Metro 29/9/14
MS 31.

## Sindiket phishing 'pindah' wang mangsa dari Malaysia ke Ukraine

**Oleh Asmah Rusman**
asmah_rusman@hmetro.com.my
**Kuala Lumpur**

Awas bagi mereka yang gemar menggunakan perbankan Internet melalui aplikasi telefon pintar berikutan sindiket 'phishing' (serangan virus) aktif 'mengirim' sejenis virus dikenali 'Zeus Trojan' bagi mencuri duit simpanan mangsa.

Lebih mengejutkan apabila wang mangsa rakyat Malaysia yang dicuri itu dipindahkan sindiket ke Ukraine.

Difahamkan virus itu aktif sebaik saja mangsa mendaftar masuk ke dalam laman perbankan Internet sebelum sindiket memintas telefon mangsa dan 'mencuri' semua maklumat peribadi yang dimasukkan mangsa.

Timbalan Pengarah Siasatan Jabatan Siasatan Jenayah Komersial (JSJK) Bukit Aman Datuk Wira Hamza Taib berkata, setakat ini pihaknya menerima lapan laporan polis berhubung jenayah itu dengan kerugian mencecah RM60,000 termasuk terbaru dilaporkan di Bukit Merah, Perak, semalam.

"Apabila mangsa mendaftar masuk di paparan utama perbankan Internet itu virus berkenaan akan mula aktif dengan memaparkan pautan palsu yang mengarahkan mangsa memasukkan maklumat peribadi dan nombor telefon selain dikehendaki memilih jenis sistem telefon contohnya Blackberry, Android, Apple iOS, Symbian atau Windows Phone.

"Mangsa menerima satu pautan (URL) melalui kiriman sistem pesanan ringkas (SMS) dari satu nombor telefon antarabangsa sebelum diarahkan untuk klik pautan berkenaan," katanya dalam sidang media di Bukit Perdana, semalam.

Hamza berkata, pautan berkenaan mengeluarkan satu sijil yang kononnya dikeluarkan bank bersama nombor kod.

"Seterusnya mangsa dikehendaki memasukkan nombor kod itu ke dalam laman perbankan internet palsu bagi tujuan pengesahan suspek mangsa memasukkan nombor telefon sebenar.

"Proses itu hanya mengambil masa satu minit, malah ia juga mewujudkan satu program baru di telefon pintar mangsa dengan ikon bank berkaitan.

> "Apabila mangsa mendaftar masuk di paparan utama perbankan Internet itu virus mula aktif dengan memaparkan pautan palsu yang mengarahkan mangsa memasukkan maklumat peribadi dan nombor telefon"
> *Hamza Taib*

"Tanpa mangsa sedari program itu berfungsi sebagai 'SMS Stealer' yang menghantar Kod Pengesahan Urus Niaga (Transaction Authorisation Code) dihantar ke telefon suspek untuk setiap pengeluaran atau perpindahan wang," katanya.

Katanya, mangsa tidak menyedari telefon mereka dimasukkan virus itu kerana paparan muka sebenar bank dipaparkan semula di skrin telefon mangsa sebaik proses berkenaan selesai.

"Mangsa beranggapan mereka sudah menggunakan aplikasi perbankan internet itu tanpa menyedari mereka turut 'mendaftar' dengan penjenayah," katanya.

Katanya, virus itu membolehkan penjenayah merompak wang di dalam akaun bank mangsa pada bila-bila masa mengikut had pengeluaran yang ditetapkan bank.

"Mangsa hanya menyedari akaun mereka 'dirompak' selepas menerima nombor TAC daripada bank sedangkan mereka tidak menggunakan perbankan Internet.

"Apabila diperiksa, akaun merekakehilangan wang tunai selalunya antara RM5,000 hingga RM10,000 bergantung kepada kadar pengeluaran yang ditetapkan bank," katanya.

Katanya, siasatan awal pihaknya mendapati nombor telefon antarabangsa itu dikesan dari Eropah manakala wang berkenaan dimasukkan ke dalam akaun tempatan milik individu yang dijadikan 'keldai akaun' sebelum dikirimkan melalui Western Union ke Ukraine.

"Pemegang akaun mengaku bekerja sebagai pekerja sambilan dengan bayaran komisen antara lima hingga 10 peratus untuk satu tugasan yang mana sindiket menghantar arahan kerja melalui kiriman emel," katanya.