RENATA Jurnal Pengabdian Masyarakat Kita Semua
Vol. 1 No. 1 April 2023 [Hal. 7-10]
DOI: https://doi.org/10.61124/1.renata.4

AKTIVITAS SNIFFING PADA MALWARE PENCURI UANG DI SMARTPHONE ANDROID

Mulki Indana Zulfa*[1], Silvester Tena[2], Sampurna Dadi Rizkiono[3]
[1]Teknik Elektro, Fakultas Teknik, Universitas Jenderal Soedirman, Purbalingga
[2]Teknik Elektro, Fakultas Sains dan Teknik, Universitas Nusa Cendana [3]Teknik Informatika, Fakultas Teknik, Universitas Teknokrat
*e-mail: mulki_indanazulfa@unsoed.ac.id

Abstrak
Sniffing termasuk dalam *cyber-crime* yang dilakukan oleh program jahat atau berbahaya (*malware*) yang sangat merugikan korbannya dengan tujuan untuk mencuri data dan informasi penting lewat jaringan internet. Data yang dicuri umumnya adalah *username* atau akun login aplikasi ibanking, *password m-banking*, *email*, informasi kartu kredit, atau data penting digital lainnya. Tindak kejahatan ini biasanya dengan mengirimkan format berkas yang digunakan untuk memasang aplikasi android yang biasa dikenal dengan file .apk. File berekstensi .apk adalah aplikasi yang dapat dipasang pada perangkat android. Banyak yang menyalahgunakan file .apk ini, salah satunya berisi *ransomware* atau *malware* lainnya. Salah satu contoh malware terbaru adalah Sharkbot yang pertama kali ditemukan oleh Cleafy pada Oktober 2021. Keberadaannya di Play Store dideteksi oleh peneliti dari NCC Group yang baru saja membagikan analisis rinci tentang aksi *malware* tersebut. Salah satu fitur utama *malware* ini adalah *Automatic Transfer System* (ATS) yang memungkinkan *hacker* mentransfer uang korban tanpa sepengetahuan mereka. Ada beberapa cara pencegahan atau preventif untuk menghindari diri dari serangan *malware.* Jika memiliki *server*, dapat memasang *firewall*, *Interusion Prevention System* (IPS), *Deep Packet Inspection* (DPI), *Unified Thread Management System*, antivirus, hingga konten *filtering*.
Kata kunci: sniffing, malware, android, pencuri uang

Abstract
Sniffing is included in cyber-crimes that are carried out by malicious or malicious programs (malware) which are very detrimental to victims with the aim of stealing important data and information via the internet network. The data stolen is generally an ibanking application username or login account, m-banking password, email, credit card information, or other important digital data. This crime is usually by sending the file format used to install android applications, commonly known as .apk files. Files with the .apk extension are applications that can be installed on Android devices. Many misuse this .apk file, one of which contains ransomware or other malware. One of the newest examples of malware is Sharkbot which was first spotted by Cleafy in October 2021. Its presence on the Play Store was detected by researchers from the NCC Group who have just shared a detailed analysis of the malware's actions. One of the main features of this malware is the Automatic Transfer System (ATS) which allows hackers to transfer victims' money without their knowledge. There are several preventive or preventive ways to avoid malware attacks. If you have a server, you can install a firewall, Interruption Prevention System (IPS), Deep Packet Inspection (DPI), Unified Thread Management System, antivirus, and content filtering.
Keywords: sniffing, malware, android, money thief.

1. PENDAHULUAN

Baru-baru ini berita media sosial dihebohkan adanya kasus "kurir palsu" yang mengirimkan file .apk yang dinarasikan sebagai nomor resi pengiriman paket. Pelaku memperdaya korban agar mau menginstall aplikasi dari file .apk tersebut untuk mencuri data SMS (short message service) OTP (one time password) dari perangkat atau smartphone korban. Jika file .apk tersebut terpasang pada smartphone korban maka pelaku dapat login pada aplikasi ibanking dan mampu menguras sejumlah uang direkening rekening korban. Kejahatan yang dilakukan saat ini menargetkan smartphone dari pengguna android (1). Penjahat melakukan penipuan salah satunya dengan cara sniffing. Penipuan melalui snifing ini banyak dikhawatirkan oleh pengguna teknologi digital di era sekarang karena mampu melakukan kejahatan penyadapan data melalui jaringan internet (2).

Sniffing termasuk dalam cyber-crime yang dilakukan oleh program jahat atau berbahaya (malware) yang sangat merugikan korbannya dengan tujuan untuk mencuri data dan informasi penting lewat jaringan internet. Data yang dicuri umumnya adalah username atau akun login aplikasi ibanking, password m- banking, email, informasi kartu kredit, atau data penting digital lainnya. Tindak kejahatan ini biasanya dengan mengirimkan format berkas yang digunakan untuk memasang aplikasi android yang biasa dikenal dengan file .apk. File berekstensi .apk adalah aplikasi yang dapat dipasang pada perangkat android. Banyak yang menyalahgunakan file .apk ini, salah satunya berisi ransomware atau malware lainnya. Pengembang aplikasi

Vol. 1 No. 1 April 2023 [Hal. 7-10]
DOI: https://doi.org/10.61124/1.renata.4

jahat ini bertujuan negatif dengan menyamarkan aplikasi sehingga tampak 'terpercaya'. Begitu aplikasi di klik atau dipasang, file .apk tersebut justru merusak atau mencuri data dalam ponsel (2).

2. CARA KERJA MALWARE

Ada banyak jenis malware yang berbahaya diantaranya virus, trojan, worm, spyware, spam, botnet dan sebagainya. Beberapa klasifikasi serangan dan yang paling umumnya adalah untargeted attach. Untargeted attach ini tidak mentargetkan ke salah satu orang saja namun menyebarkan ke mana saja yang memiliki punya celah. Seperti menyerang website yang memiliki celah keamanan, menginfeksi media penyimpanan seperti flashdisk atau harddisk, penyerangan media sosial dan sebagainya. Selanjutnya klasifikasi serangan botnet atau dikenal dengan robot-network yang merupakan sekumpulan jaringan komputer yang telah terinfeksi oleh malware dan dikendalikan oleh pihak yang disebut sebagai bot-herder (pemilik malware). Analogi seperti kasus pencopetan, tidak satu orang saja yang terlibat namun ada banyak orang yang terlibat dan memiliki peran masing masing (komplotan) (2).

3. BEBERAPA MALWARE POPULER

Virus Joker kembali mengincar pengguna smartphone android. Hal ini diungkap oleh kepolisian Belgia dan meminta masyarakat untuk menghapus aplikasi yang disusupi virus jahat ini dari perangkat. "Program jahat ini telah terdeteksi pada 8 aplikasi di Play Store Google," ujar Kepolisian Belgia seperti dikutip dari Times of India.

A. Virus Joker

Beberapa aplikasi berikut Aplikasi ini sudah dihapus dari Play Store namun masih bisa beraksi bila terpasang di smartphone android pengguna. Berikut daftar aplikasinya: Auxiliary Message, Element Scanner, Fast Magic SMS, Free CamScanner, Go Messages, Super Message, Super SMS, dan Travel Wallpapers [2]. Virus jahat Joker mendadak terkenal pada 2017 silam karena menginfeksi dan merampok korbannya dengan bersembunyi sebagai aplikasi di Google Play Store. Google bekerja keras untuk memindai dan menghapusnya. Sekitar 1.700 aplikasi dengan malware Joker telah dihapus Google. Pada September 2020, virus Joker ditemukan pada 24 aplikasi android dengan lebih dari 500 ribu kali diunduh sebelum dihapus. Ketika itu virus ini diperkirakan sudah mempengaruhi 30 negara termasuk AS, Brasil dan Spanyol. Ponsel korban ditautkan dengan layanan berbayar secara diam-diam (3).

Virus Joker merupakan bagian dari keluarga malware bernama Bread yang tujuannya untuk menyedot uang korban melalui smartphone dengan mengotorisasi operasi tanpa persetujuan pengguna. Peneliti keamanan siber Quick Heal Security Lab menjelaskan virus ini dalam melihat pesan teks, kontak dan informasi milik smartphone yang terinfeksi. Apa yang membuat Joker Berbahaya adalah kemampuannya untuk mengaitkan ponsel android ke layanan berbayar tanpa izin dan pihak bank tidak curiga dengan tagihan dari korban yang tampak 'normal' (3).

B. Virus Sharkbot

Malware Sharkbot pertama kali ditemukan oleh Cleafy pada Oktober 2021. Keberadaannya di Play Store dideteksi oleh peneliti dari NCC Group yang baru saja membagikan analisis rinci tentang aksi malware tersebut. Salah satu fitur utama malware ini adalah Automatic Transfer System (ATS) yang memungkinkan hacker mentransfer uang korban tanpa sepengetahuan mereka. Fitur ini juga yang membedakan Sharkbot dari trojan perbankan lainnya. Menariknya, proses pemindahan uang dari rekening ini bisa dilakukan tanpa interaksi manusia. Jadi malware ini bisa mensimulasikan gerakan seperti sentuhan, klik, dan memencet tombol, layaknya pengguna aplikasi mobile banking pada umumnya (4). Menurut laporan NCC, SharkBot versi terbaru memiliki empat fungsi utama yaitu (4):

1. *Injections*: SharkBot bisa mencuri kredensial akun mobile banking pengguna dengan menampilkan halaman login palsu begitu mendeteksi aplikasi mobile banking resmi dibuka.
2. *Keylogging*: SharkBot bisa mencuri kredensial dengan mencatat accessibility events (yang terkait dengan perubahan teks dan tombol yang diklik) dan mengirimkan log ini ke server command and control (C2).
3. *SMS intercept*: SharkBot bisa mencegat atau menyembunyikan SMS yang masuk.
4. *Remote control*: SharkBot bisa mengambil alih kontrol penuh perangkat android dari jarak jauh dengan mengeksploitasi izin akses (accesibility) di smartphone.

Vol. 1 No. 1 April 2023 [Hal. 7-10]
DOI: https://doi.org/10.61124/1.renata.4

Selain empat fungsi di atas, malware SharkBot juga bisa menerima perintah dari server C2 untuk melakukan beberapa hal seperti mengirim SMS ke sebuah nomor, mengunduh file dari URL tertentu, menghapus aplikasi dari ponsel, mematikan optimalisasi baterai, dan lain- lain. Malware SharkBot ditemukan di dalam empat aplikasi antivirus yang beredar di Play Store. Malware pada aplikasi smartphone tersebut sudah dihapus oleh Google dan telah diunduh lebih dari 57.000 kali. Bagi pengguna yang memiliki aplikasi- aplikasi berikut ini di ponselnya, harap segera menghapusnya dan melakukan reset. Berikut ini daftar aplikasi yang berisi malware SharkBot (4): Super Cleaner, Atom Clean-Booster, Alpha Antivirus, dan Powerful Cleaner.

C. Virus Escobar

Sebuah laporan memperingatkan sebuah trojan atau software jahat yang dapat mencuri data pribadi pengguna, seperti data perbankan melalui serangan phising. Menurut BleepingComputer, virus baru tersebut bernama Escobar yang saat ini sedang menyebar di antara pengguna android. Trojan ini sebenarnya tidak benar-benar baru, ia hanya hadir dengan nama dan kemampuan yang jauh lebih berbahaya. Malware Escobar diketahui menargetkan nasabah dari 190 lembaga keuangan di 18 negara berbeda. Rincian spesifik terkait dengan negara dan institusi mana, masih belum terungkap. Berdasarkan laporan tersebut, malware perbankan itu dapat mencuri kode otentikasi 2 faktor (2FA) Google Authenticator, yang dikirim ke perangkat ketika seseorang mencoba masuk ke email atau layanan perbankan online (5).

Apabila perangkat korban telah terinfeksi, malware itu bisa mendapatkan akses mudah ke data pribadi dan keuangan korbannya. Semua yang dikumpulkan trojan tersebut, kemudian diunggah ke server C2, termasuk isi pesan SMS, daftar panggilan, lokasi, dan kode otentifikasi 2FA Google Authenticator. Ini bukan pertama kalinya trojan perbankan seperti Escobar beraksi. Pada tahun 2021, ada sebuah malware android, Aberebot, dengan kemampuan serupa menargetkan ratusan pengguna Android. Escobar kurang lebih mirip dengan Aberebot, tapi hadir dengan kemampuan yang lebih canggih. Trojan 'Escobar' mengambil kendali penuh atas perangkat yang terinfeksi dengan mengklik foto, merekam audio, dan juga memperluas kumpulan aplikasi yang ditargetkan untuk pencurian data digital. Tidak seperti malware android lainnya, Escobar menargetkan pengguna melalui file .apk yang diinstal di web. Kebanyakan kasus virus mirip Escobar mengambil alih rekening perbankan pengguna dan melakukan transaksi yang tidak sah (5).

4. TINDAKAN MENCEGAH MALWARE

Ada beberapa cara pencegahan atau preventif untuk menghindari diri dari serangan malware. Jika memiliki server, dapat memasang firewall, Interusion Prevention System (IPS), Deep Packet Inspection (DPI), Unified Thread Management System, antivirus, hingga konten filtering dan sebagainya. Jika komputer pribadi, cukup menggunakan antivirus yang biasanya juga sudah termasuk anti malware dan anti trojan. Antivirus dapat mencegah aktivitas malware dengan cara signature-detection maupun behaviour-detection. Teknik pertama masih dilakukan secara pendekatan yaitu melalui deteksi signature-detection. Setiap malware pasti memiliki signature. Jika terdeteksi signature-nya maka antivirus dapat langsung melakukan proses blok. Kedua, secara behaviour atau yang dievaluasi berdasarkan tingkah laku objeknya.

Jika aktifitasnya ubnormal akan ditandai kemudian dapat diblokir jika terus mengancam dengan tindakan yang ubnormal tersebut. Sedangkan untuk melindungi smartphone anda dari ancaman malware maka dapat lakukan cara berikut ini (6):

1. Pengguna Android harus memastikan mereka tidak menginstal file .apk dari luar Google Play Store.
2. Aktifkan opsi Google Play Protect di ponsel, yang menanyakan apakah pengguna sedang dalam proses memasang malware di perangkat mereka.
3. Selalu berhati – hati dengan cookies yang diminta oleh website non-official (7).
4. Tidak mudah mengunduh dan menggunakan file aplikasi berbayar yang diunduh secara gratis pada website non-official (8).
5. Pengguna harus selalu memeriksa izin umum yang diminta oleh aplikasi tertentu. Ini akan memungkinkan mereka melihat aplikasi atau file yang menginstal malware di perangkat yang berisiko.
6. Pastikan selalu periksa detail seperti nama, deskripsi, dan lebih banyak file atau aplikasi sebelum memasangnya di ponsel.

5. KESIMPULAN

Ada beberapa ancaman kejahatan online dapat terjadi. Setiap kejahatan online mempunyai tujuannya masing-masing. Kejahatan online yang bertujuan untuk merusak file atau sistem komputer maupun smartphone umumnya dilakukan oleh malware berjenis virus atau trojan. Kejahatan lainnya tidak bertujuan untuk merusak file atau sistem komputer namun justru memiliki dampak kerugian yang lebih besar, seperti pencurian akun email hingga internet banking. Aktivitas pencurian tersebut dilakukan dengan cara sniffing. Malware atau program jahat yang umumnya digunakan untuk melakukan aktivitas sniffing adalah spyware. Beberapa aktivitas dapat dilakukan untuk mencegah dua kejahatan online tersebut. Jika yang digunakan adalah perangkat komputer pribadi atau laptop, anda cukup menginstal antivirus yang di dalamnya sudah dilengkapi dengan antitrojan maupun antispyware. Namun untuk melindungi smartphone anda dari aktivitas kejahatan online, hal utama yang harus diperhatikan setelah memang antivirus adalah memastikan semua aplikasi yang terpasang harus didapatkan dari penyedia official, seperti Google Play Store. Setelah memastikan hal tersebut, jangan mudah untuk membuka file dari pengirim yang tidak dikenal dan selalu berhati-hati terhadap permintaan akses dari aplikasi yang anda pasang.

DAFTAR PUSTAKA

1. Ali W. Hybrid Intelligent Android Malware Detection Using Evolving Support Vector Machine Based on Genetic Algorithm and Particle Swarm Optimization. Int J Comput Sci Netw Secur [Internet]. 2019;19(9):15–28. Available from: http://ijcsns.org/07_book/html/201909/201909003.html
2. Komputer T. Bahaya Keamanan Aplikasi Berbasis APK Digital Android [Internet]. UNPAB. 2023 [cited 2023 Feb 4]. Available from: https://tekom.pancabudi.ac.id/bahaya-keamanan-aplikasi-berbasis-apk-digital-android/
3. Bestari NP. Mengenal Joker, Virus yang Curi data & Uang Pengguna Android [Internet]. CNBC Indonesia. 2021 [cited 2023 Feb 4]. Available from: https://www.cnbcindonesia.com/tech/20210827094650-37-271665/mengenal-joker-virus-yang-curi-data-uang-pengguna-android
4. Putri VM. Awas! Aplikasi Android Ini Curi Uang dari Mobile Banking Anda [Internet]. Detik Inet. 2022 [cited 2023 Feb 4]. Available from: https://inet.detik.com/security/d-6021994/awas-aplikasi-android-ini-curi-uang-dari-mobile-banking-anda
5. Dewi IR. Waspada! Virus Jahat Android Ini Bisa Rampok Uangmu di Bank [Internet]. CNBC Indonesia. 2022 [cited 2023 Feb 4]. Available from: https://www.cnbcindonesia.com/tech/20220322072123-37-324735/waspada-virus-jahat-android-ini-bisa-rampok-uangmu-di-bank
6. Hanjarwadi W. Tips Menghindari Penipuan Sniffing [Internet]. Pajak.com. 2022 [cited 2023 Feb 4]. Available from: https://www.pajak.com/ekonomi/tips-menghindari-penipuan-sniffing/
7. Suma GS, Dija S, Pillai AT. Forensic Analysis of Google Chrome Cache Files. In: 2017 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2017. IEEE; 2018. p. 1–5.
8. Duy Le, Haining Wang. An Effective Memory Optimization for Virtual Machine-Based Systems. IEEE Trans Parallel Distrib Syst [Internet]. 2011 Oct;22(10):1705–13. Available from: http://ieeexplore.ieee.org/document/5703077/