IMBAUAN KEAMANAN TERHADAP APLIKASI BERBAHAYA PADA GOOGLE *PLAY STORE*

Rabu, 24 Agustus 2022

Ringkasan Eksekutif

1. Pada Rabu, 17 Agustus 2022, Bitdefender telah mengidentifikasi 35 aplikasi yang terdapat *malware* dan terunggah ke Google Play Store, dengan total lebih dari dua juta unduhan.
2. Mengingat dampak yang mungkin muncul dari eksploitasi kerentanan ini, diharapkan pengguna dari produk terdampak ataupun pengguna pemerintah dan publik lainnya untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada imbauan keamanan ini.

Pendahuluan

Pada Rabu, 17 Agustus 2022, Bitdefender telah mengidentifikasi 35 aplikasi yang terdapat *malware* dan terunggah ke Google Play Store, dengan total lebih dari dua juta unduhan. Peristiwa ini termasuk jenis serangan *malware* terbaru yang ada di Google Play Store. Meskipun pemeriksaan keamanan pada Google Play Store sudah ditingkatkan, namun Bifdefender masih dapat menemukan aplikasi berbahaya yang telah menerapkan beragam cara untuk melewati pemeriksaan keamanan. Pada kasus ini, di mana aplikasi-aplikasi berbahaya ini melakukan pengalihan untuk memikat pengguna agar meng-*install* aplikasi tersebut dengan cara mengubah nama dan ikon aplikasi tersebut menjadi nama dan ikon aplikasi yang biasanya ada di perangkat Android, serta mengubah nama dan ikon aplikasi asli milik Android menjadi nama dan ikon aplikasi yang lain. Setelah itu, aplikasi tersebut akan menayangkan iklan yang agresif. Tujuan dari kejahatannya adalah untuk membingungkan pengguna dan menyembunyikan lokasi keberadaan aplikasi tersebut.

Produk Terdampak

Produk yang terdampak oleh aplikasi berbahaya ini adalah perangkat lunak android sebanyak 35 aplikasi dengan rincian sebagai berikut:

1. *Walls light - Wallpapers Pack*
2. *Big Emoji – Keyboard*
3. *Grad Wallpapers - 3D Backdrops*
4. *Engine Wallpapers - Live & 3D*

5. *Stock Wallpapers - 4K & HD*
6. *EffectMania - Photo Editor*
7. *Art Filter - Deep Photoeffect*
8. *Fast Emoji Keyboard*
9. *Create Sticker for Whatsapp*
10. *Math Solver - Camera Helper*
11. *Photopix Effects - Art Filter*
12. *Led Theme - Colorful Keyboard*
13. *Keyboard - Fun Emoji, Sticker*
14. *Smart Wifi*
15. *My GPS Location*
16. *Image Warp Camera*
17. *Art Girls Wallpaper HD*
18. *Cat Simulator*
19. *Smart QR Creator*
20. *Colorize Old Photo*
21. *GPS Location Finder*
22. *Girls Art Wallpaper*
23. *Smart QR Scanner*
24. *GPS Location Maps*
25. *Volume Control*
26. *Secret Horoscope*
27. *Smart GPS Location*
28. *Animated Sticker Master*
29. *Personality Charging Show*
30. *Sleep Sounds*
31. *QR Creator*
32. *Media Volume Slider*
33. *Secret Astrology*
34. *Colorize Photos*
35. *Phi 4K Wallpaper - Anime HD*

Detail dan Dampak Kerentanan

Pada kasus ini, aplikasi-aplikasi berbahaya ini melakukan pengalihan untuk memikat pengguna agar meng-*install* aplikasi tersebut dengan cara mengubah nama dan ikon aplikasi tersebut menjadi nama dan ikon aplikasi yang biasanya ada di perangkat Android, serta mengubah nama dan ikon aplikasi asli milik Android menjadi nama dan ikon aplikasi yang lain. Setelah itu, aplikasi tersebut akan menayangkan iklan yang agresif. Banyak aplikasi yang sah menawarkan iklan kepada penggunanya, tetapi aplikasi ini menampilkan iklan melalui kerangka kerja mereka sendiri, yang berarti aplikasi ini juga dapat menayangkan jenis *malware* yang lainnya kepada pengguna tersebut. Iklan yang ditayangkan pada aplikasi ini juga dapat mengganggu pengguna ketika menggunakan aplikasi tersebut dan dapat menautkan langsung ke *malware.* Pengguna dapat memilih untuk menghapus aplikasi ini jika mereka tidak menyukainya. Namun, *developer* membuatnya lebih sulit untuk ditemukan pada perangkat yang terpengaruh. Bitdefender telah mengembangkan teknologi *real-time behavioral* terbaru yang dirancang untuk mendeteksi aplikasi berbahaya ini.

Bitdefender telah mengidentifikasi 35 aplikasi yang telah menyelinap ke Google Play Store, dengan total lebih dari dua juta unduhan. Ini adalah kasus *malware* baru di Google Play Store di mana banyak aplikasi menggunakan dalih palsu untuk memikat korban agar menginstalnya, hanya untuk mengubah nama mereka dan secara agresif menayangkan iklan setelahnya. Salah satu cara penjahat dunia maya memonetisasi kehadiran mereka di Google Play adalah dengan menayangkan iklan kepada korbannya. Meskipun ini mungkin terdengar kecil, iklan yang ditayangkan kepada korban ini mengganggu pengalaman penggunaan dan dapat menautkan langsung ke *malware*. Bitdefender mengidentifikasi aplikasi berbahaya menggunakan teknologi perilaku *real-time* baru yang dirancang untuk mendeteksi secara tepat praktik berbahaya ini, di antara banyak lainnya. Teknologi baru ini sudah membuahkan hasil karena deteksi baru langsung dibagikan dengan semua pengguna Bitdefender *Mobile Security*.

Aplikasi ‘GPS Location Maps' sebagai contoh pertama yang memiliki lebih dari 100 ribu unduhan, namun tidak memiliki ulasan apapun. Setelah dilakukan instalasi pada perangkat Android, aplikasi tersebut mengubah nama yang awalnya “GPS Location Maps'” menjadi “Settings”. Kemudian, menampilkan situs web tambahan di WebViews dan iklan. WebViews merupakan bagian dari sistem operasi Android yang memungkinkan aplikasi memuat konten, seperti halaman web, iklan, dan yang lainnya.

Aplikasi ‘GPS Location Maps' mempersulit pengguna untuk menemukan dan melepeas pemasangannya dengan mengubah ikon aplikasi tersebut. Selain itu, beberapa aplikasi meminta izin untuk melewati fitur pengoptimalan baterai dan memulai pemberitahuan layanan agar tetap jalan pada *foreground* dan tidak terbunuh oleh sistem. Aplikasi-aplikasi ini juga ada yang terdeteksi meminta izin untuk ditampilkan di atas aplikasi lain.

Panduan Mitigasi

Untuk melakukan mitigasi terhadap aplikasi berbahaya pada Google *Play Store*, disarankan kepada pemilik aset untuk melakukan langkah pencegahan sebagai berikut:

1. Jangan menginstal aplikasi yang tidak dibutuhkan
2. Menghapus aplikasi yang tidak lagi digunakan
3. Hati-hati terhadap aplikasi yang memiliki jumlah unduhan yang banyak maupun sedikit atau tanpa ulasan.
4. Hati-hati terhadap aplikasi yang meminta izin khusus, seperti berjalan di atas aplikasi atau akses ke *Accessibility*.
5. Hati-hati terhadap aplikasi yang meminta akses izin yang tidak ada hubungannya dengan fungsi aplikasi tersebut
6. Menjalankan keamanan di latar belakang yang dapat mendeteksi perilaku *malicious*. Aplikasi yang diunduh dari *official store*, bukan berarti aplikasi tersebut aman.
7. Melakukan *scanning* setiap *file* yang diterima melalui aplikasi *file scanning*.

Riwayat Dokumen

Versi Dokumen	Tanggal Rilis
1.0	Rabu, 24 Agustus 2022

Ketentuan Penggunaan Dokumen

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal Website ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

Referensi

[1] “Real-Time Behavior-Based Detection on Android Reveals Dozens of Malicious Apps on Google Play Store” https://www.bitdefender.com/blog/labs/real-time-behavior-based-detection-on-android-reveal-dozens-of-malicious-apps-on-google-play-store/ (accessed August. 24, 2022)

[2] “Alert! These 35 sneaky apps on Android are ad bombs, delete now” https://www.timesnownews.com/technology-science/alert-these-35-sneaky-apps-on-android-are-ad-bombs-delete-now-article-93658411/amp (accessed August. 24, 2022)

[3] “Android reveal dozens of malicious apps” https://ciotechasia.com/android-reveal-dozens-of-malicious-apps/ (accessed August. 24, 2022)