www.idsirtii.or.id

07 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 207

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	1	0	0
URGENT	2	0	1
IMPORTANT	0	2	0

General News

Microsoft Menggugat Pembajakan Melalui GitHub Copilot

Programmer dan pengacara Matthew Butterick telah menggugat Microsoft, GitHub, dan OpenAI dengan tuduhan bahwa Copilot GitHub melanggar persyaratan lisensi sumber terbuka dan melanggar hak-hak programmer. GitHub Copilot yang dirilis pada Juni 2022 merupakan bantuan pemrograman berbasis AI yang menggunakan OpenAI Codex untuk menghasilkan kode sumber secara *real-time* dan rekomendasi fungsi di Visual Studio. *Tool* ini dilatih dengan pembelajaran mesin menggunakan miliaran baris kode dari repositori publik dan dapat mengubah bahasa alami menjadi cuplikan kode di lusinan bahasa pemrograman. Selain pelanggaran lisensi, Butterick juga menuduh bahwa fitur pengembangan melanggar persyaratan layanan dan kebijakan privasi GitHub, DMCA 1202 yang melarang penghapusan informasi manajemen hak cipta, undang-undang Privasi Konsumen California, dan undang-undang lain yang menimbulkan tuntutan hukum terkait.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/microsoft-sued-for-open-source-piracy-through-github-copilot/ >

Peneliti Mengungkap 29 Paket PyPI Berbahaya yang Ditargetkan Pengembang dengan W4SP *Stealer*

Peneliti keamanan siber menemukan 29 paket dalam Python Package Index (PyPI), repositori perangkat lunak pihak ketiga resmi untuk bahasa pemrograman Python, yang bertujuan untuk menginfeksi mesin pengembang dengan *malware* yang disebut W4SP Stealer. Daftar paket yang dimaksud yaitu: typesutil, typestring, sutiltype, duonet, fatnoob, strinfer, pydprotect, incrivelsim, twyne, pyptext, installpy, faq, colorwin, requests-httpx, colorsama, shaasigma, stringe, felpesviadinho, cypress, pystyte, pyslyte, pystyle, pyurllib, algorithmic, oiu, iao, curlapi, type-color, dan pyhints. Modul palsu menggunakan kembali *library* sah yang ada dengan menyisipkan pernyataan impor berbahaya dalam skrip "setup.py" untuk meluncurkan kode Python yang mengambil *malware*. W4SP *Stealer, open-source trojan* berbasis Python memungkinkan terjadinya pencurian *file,* kata sandi, *cookie browser,* metadata sistem, token Discord, dan data dari beberapa *crypto wallet*. Temuan ini menggambarkan adanya penyalahgunaan berkelanjutan ekosistem *open-source* untuk menyebarkan paket berbahaya yang dirancang untuk mengumpulkan informasi sensitif dan membuka jalan bagi serangan rantai pasokan.

Prioritas: ***1. Critical***

< https://thehackernews.com/2022/11/researchers-uncover-29-malicious-pypi.html >

Empat Aplikasi Android Berbahaya yang DItemukan di Google Play

Terdapat empat aplikasi Android yang ditemukan di Google Play telah terinfeksi *ads trojan* dan diunduh lebih dari 1 juta pengguna. Pengembang aplikasi ini diketahui telah menyebarkan *malware* pada Google Play sebelumnya. Adapun aplikasi yang dimaksud, yaitu Bluetooth Auto Connect, Bluetooth App Sender, Driver: Bluetooth, Wi-Fi, USB, dan Mobile transfer: smart switch. Berdasarkan analisis yang dilakukan, aplikasi tidak menunjukkan adanya perilaku berbahaya dalam 72 jam pertama sejak diunduh. Aplikasi mulai melakukan aktivitas dengan membuka situs *phising* di Chrome ketika pengguna membuka kunci perangkat seluler. Beberapa situs diantaranya relatif tidak berbahaya, dan beberapa lainnya relatif lebih berbahaya dan mencoba untuk mengelabui pengguna bahwa meraka telah terinfeksi atau perlu memperbarui perangkat mereka. Hal ini juga membuat riwayat penggunaan *browser* dipenuhi dengan situs-situs *phising*.

Prioritas: ***2. Urgent***

< https://www.msn.com/en-us/news/technology/4-dangerous-android-malware-apps-discovered-on-google-play/ar-AA13NSnz >

Breachs/Hacks/Leaks

Kelompok LockBit 3.0 Mengklaim Telah Mencuri Data dari Kearney & Company

Kelompok *ransomware* LockBit mengklaim telah mencuri data dari konsultan dan penyedia layanan TI Kearney & Company. Kelompok ini mengancam akan mempublikasikan data curian paling lambat 26 November 2022 jika perusahaan tidak mau membayar uang tebusan. Pelaku telah menerbitkan sampel data yang dicuri, mencakup dokumen keuangan, kontrak, laporan audit, dokumen penagihan, dan banyak lagi. Kelompok LockBit 3.0 menuntut pembayaran sebesar $2 Juta untuk menghancurkan data yang dicuri dan $10 Ribu untuk memperpanjang waktu selama 24 jam. Selain itu, kelompok ini juga mengklaim telah meretas organisasi besar lainnya, seperti Continental dan Thales.

Prioritas: ***3. Important***

< https://securityaffairs.co/wordpress/138136/cyber-crime/lockbit-ransomware-kearney-company.html >

Medibank Alami Peretasan yang Mempengaruhi 9,7 Juta Pelanggan

Peretasan yang terjadi pada Medibank mengekspos data pribadi 9,7 Juta pelanggan. Data meliputi nama pelanggan saat ini dan sebelumnya, tanggal laihr, alamat, nomor telepon, dan alamat *e-mail*. Selain itu, klaim kesehatan sekitar 160.000 pelanggan Medibank, 300.000 pelanggan ahm, dan 20.000 pelanggan internasional juga diakses dalam pelanggaran ini. Informasi yang dicuri oleh peretas tidak termasuk dokumen identitas utama, seperti surat izin mengemudi, untuk Medibank Australia atau pelanggan ahm, detail kartu kredit atau perbankan apa pun. Kepala eksekutif Medibank, David Kockzar, mengatakan bahwa hanya ada kemungkinan terbatas bahwa uang tebusan akan dibayarakan. Medibank menilai bahwa pembayaran dapat memiliki efek untuk mendorong penjahat untuk secara langsung memeras pelanggan dan membuat lebih banyak orang dalam bahaya dengan menjadikan Australia target yang lebih besar.

Prioritas: ***3. Important***

< https://www.sbs.com.au/news/article/medibank-says-it-wont-pay-a-ransom-for-cyber-hack-affecting-9-7-million-heres-what-we-know-so-far/y5rcm0t25 >

Vulnerabilities

Microsoft Memperingatkan Adanya Peningkatan Pemanfaatan Kerentanan *Zero-Day* yang Dipublikasi

Microsoft memperingatkan peningkatan di antara negara dan pelaku kriminal yang semakin memanfaatkan kerentanan *zero-day* yang diungkapkan secara publik untuk melanggar lingkungan target. Adanya peningkatan ini menjadi catatan penting bagi organisasi untuk segera melakukan penambalan kerentanan. Hal ini juga dikuatkan dengan adanya *advisory* yang diterbitkan oleh CISA, yang menemukan adanya *threat actor* yang secara agresif menargetkan *bug* perangkat lunak yang baru diungkapkan terhadap target luas secara global. Microsoft mencatat bahwa hanya butuh 14 hari untuk melakukan eksploitasi yang telah tersedia secara publik. Aktivitas ini diduga sebagai elemen yang didukung untuk melakukan kegiatan spionase. Beberapa kerentanan yang diduga menjadi alat untuk mempersenjatai tujuan ini diantaranya CVE-2021-35211 (CVSS score: 10.0), CVE-2021-40539 (CVSS score: 9.8), CVE-2021-44077 (CVSS score: 9.8), CVE-2021-42321 (CVSS score: 8.8), dan CVE-2022-26134 (CVSS score: 9.8).

Prioritas: ***2. Urgent***

< https://thehackernews.com/2022/11/microsoft-warns-of-uptick-in-hackers.html >