www.idsirtii.or.id

8 Juni 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 100

OVERVIEW

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

General News

Google Memperbaiki Kerentanan Android Kritis Melalui Pembaruan di Bulan Juni 2022

Google minggu ini mengumumkan bahwa *patch* Android terbaru memperbaiki total 40 kerentanan, termasuk beberapa yang dinilai kritis. Kerentanan paling parah yang diatasi dengan pembaruan keamanan Juni 2022, berdampak pada komponen sistem dan dapat menyebabkan *Remote Code Execution* (RCE). Dilacak sebagai CVE-2022-127, kerentanan berdampak pada Android versi 10, 11, 12, dan 12L. Dua kerentanan tingkat kritis lainnya diselesaikan di sistem dengan rangkaian pembaruan Android bulan ini, yang keduanya dapat menyebabkan peningkatan hak istimewa. Kerentanan tersebut dilacak sebagai CVE-2022-20140, yang pertama berdampak pada Android 12 dan 12L. Bug kedua yaitu CVE-2022-145, berdampak pada Android 11. Kerentanan tingkat kritis lainnya yang ditambal di Android bulan ini ditemukan di Kerangka Media. Dilacak sebagai CVE-2022-20130, ini dapat menyebabkan RCE pada perangkat yang menjalankan Android 10 dan yang lebih baru.

Prioritas: ***2. Urgent***

<https://www.securityweek.com/google-patches-critical-android-vulnerabilities-june-2022-updates?&web_view=true>

Ancaman Siber di Tengah Pertumbuhan Ekonomi Digital

Pandemi telah menjadi pendorong percepatan digitalisasi di seluruh dunia, termasuk Indonesia sebagai salah satu pusat ekonomi terbesar di Asia Tenggara. Indonesia saat ini memiliki 202 juta pengguna internet yang berkontribusi sekitar USD 70 miliar terhadap ekonomi digital nasional pada 2021. Namun, pertumbuhan digital yang pesat diikuti oleh peningkatan ancaman siber yang signifikan. Laporan terbaru oleh National Cyber Security Index (NCSI) menunjukkan bahwa keamanan siber Indonesia berada di peringkat ke-6 di antara negara ASEAN lainnya dan ke-83 dari 160 negara secara global. Sebuah laporan Interpol juga menegaskan hal ini dengan menyebutkan bahwa sekitar 2,7 juta *ransomware* terdeteksi di negara-negara ASEAN sepanjang tahun 2021 dan Indonesia memimpin dengan 1,3 juta kasus. Ancaman-ancaman siber pada umumnya menyasar perusahaan besar dan institusi pemerintahan. Salah satu alasan utamanya adalah jaringan lama (*legacy network*) dan infrastruktur keamanan jaringan tidak lagi mampu mengakomodir cara bekerja pada lanskap modern saat ini, termasuk dalam mencegah Highly Evasive Adaptive Threats (HEAT) yang dapat mengakibatkan *ransomware*.

Prioritas: ***3. Important***

< https://www.liputan6.com/bisnis/read/4980943/awas-ancaman-siber-di-tengah-pertumbuhan-ekonomi-digital >

Breachs/Hacks/Leaks

Peretasan Toko Senjata Online di Amerika Serikat Mengakibatkan Pencurian Kartu Kredit

Dua toko senjata Amerika, Rainier Arms dan Numrich Gun Parts, yang mengoperasikan situs *e-commerce* telah mengungkapkan pelanggaran data akibat infeksi *skimmer* kartu pada situs mereka. Skimmer kartu kredit merupakan kode JavaScript berbahaya yang disematkan di situs atau diambil dari sumber daya jarak jauh oleh elemen yang tampaknya tidak berbahaya, seperti favicon. Tujuan mereka adalah untuk mencuri informasi pembayaran yang dimasukkan pada halaman *checkout* pesanan. Operator *skimmer* ini dapat mencuri nomor kartu kredit, tanggal kedaluwarsa, kode CVV, nama pelanggan, nomor telepon, dan alamat, yang mereka butuhkan untuk melakukan pembelian online yang tidak sah. Kepemilikan senjata adalah topik yang sensitif, jadi mengidentifikasi pembelian senjata api dalam jumlah besar dapat mengakibatkann pelanggan menjadi sasaran penjahat yang mencari keuntungan.

Prioritas: ***3. Important***

<https://www.bleepingcomputer.com/news/security/online-gun-shops-in-the-us-hacked-to-steal-credit-cards/?&web_view=true >

Pelanggaran Data Shields Health Care Group Memengaruhi 2 Juta Pasien

Shields Health Care Group (Shields) mengalami pelanggaran data yang mengekspos data sekitar 2.000.000 orang di Amerika Serikat setelah peretas menerobos jaringan mereka dan mencuri data. Shields merupakan penyedia layanan medis berbasis di Massachusetts yang berspesialisasi dalam pencitraan diagnostik MRI dan PET/CT, onkologi radiasi, dan layanan bedah rawat jalan. Pemeriksaan *file log* menunjukkan bahwa peretas memiliki akses ke sistem Shields dari 7 Maret 2022 hingga 21 Maret 2022, yang memungkinkan mereka untuk berpotensi mengakses data yang berisi informasi pasien berikut: nama lengkap, nomor KTP, tanggal lahir, alamat rumah, informasi penyedia, diagnosa, nomor dan informasi asuransi, nomor rekam medis, identitas pasien, informasi medis dan banyak lainnya. Shields mengatakan tidak menemukan bukti bahwa informasi yang dicuri telah disalahgunakan atau disebarluaskan di situs ilegal. Umumnya, informasi curian semacam ini ditukar secara pribadi dan digunakan dalam serangan bertarget skala kecil sebelum dijual kembali kepada pelaku ancaman tingkat rendah yang terlibat dalam eksploitasi massal.

Prioritas: ***3. Important***

<https://www.bleepingcomputer.com/news/security/shields-health-care-group-data-breach-affects-2-million-patients/?&web_view=true >

Vulnerabilities

QBot Mendistribusikan Ransomware Black Basta

Grup *ransomware* Black Basta telah bergabung dengan QBot untuk mendapatkan akses awal ke lingkungan perusahaan. QBot dikenal karena mencuri domain Windows dan kredensial bank serta mengirimkan *payload* tambahan. Para peneliti dari NCC Group telah melaporkan tentang kemitraan yang sedang berlangsung antara Qbot dan operator Black Basta dalam tanggapan insiden baru-baru ini. Peneliti telah mengidentifikasi beberapa TTP baru yang digunakan untuk serangan ini. QBot biasanya digunakan untuk akses awal, namun Black Basta telah menggunakannya untuk menyebar secara lateral di dalam jaringan korban. *Malware* tersebut dari jarak jauh membuat layanan sementara pada *host* dan mengonfigurasinya untuk menjalankan DLL menggunakan regsvr32[.]exe. Setelah dikonfigurasi, QBot dapat menginfeksi berbagi jaringan dan *drive*, memaksa akun *Active Directory*, atau menggunakan SMB untuk membuat salinannya sendiri atau menyebar melalui pembagian admin *default* menggunakan kredensial pengguna saat ini.

Prioritas: ***2. Urgent***

< https://cyware.com/news/qbot-delivers-black-basta-ransomware-176ed81a >

Peneliti Peringatkan Kampanye Spam yang Menargetkan Korban Menggunakan *Malware* SVCReady

Gelombang baru kampanye *phishing* telah diamati menyebarkan *malware* yang didokumentasikan sebelumnya yang disebut SVCReady. *Malware* ini terkenal karena cara yang tidak biasa dikirimkan ke PC target menggunakan *shellcode* yang tersembunyi di properti dokumen Microsoft Office. SVCReady dikatakan dalam tahap awal pengembangan, dengan penulis berulang kali memperbarui malware beberapa kali bulan lalu. Tanda-tanda pertama aktivitas dimulai pada 22 April 2022. Rantai infeksi melibatkan pengiriman lampiran dokumen Microsoft Word ke target melalui *email* yang berisi makro VBA untuk mengaktifkan penyebaran muatan berbahaya. *Malware* ini hadir dengan kemampuan untuk mengumpulkan informasi sistem, menangkap tangkapan layar, menjalankan perintah *shell*, serta mengunduh dan mengeksekusi file arbitrer.

Prioritas: ***2. Urgent***

< https://thehackernews.com/2022/06/researchers-warn-of-spam-campaign.html >