www.idsirtii.or.id

7 Juni 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 099

OVERVIEW

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

General News

QBot Mendorong *Ransomware* Black Basta Dalam Serangan berbasis Bot

Geng *ransomware* Black Basta telah bermitra dengan operasi *malware* QBot untuk mendapatkan akses awal ke lingkungan perusahaan. QBot (QuakBot) adalah *malware* Windows yang mencuri kredensial bank, kredensial domain Windows, dan mengirimkan muatan *malware* lebih lanjut pada perangkat yang terinfeksi. Korban biasanya terinfeksi Qbot melalui serangan *phishing* dengan lampiran berbahaya. Meskipun dimulai sebagai trojan perbankan, *malware* ini memiliki banyak kolaborasi dengan geng *ransomware* lain, termasuk MegaCortex, ProLock, DoppelPaymer, dan Egregor. Black Basta merupakan operasi *ransomware* yang relatif baru yang dimulai dengan melanggar banyak perusahaan dalam waktu yang singkat sambil menuntut pembayaran uang tebusan yang besar. *Malware* ini dari jarak jauh membuat layanan sementara pada *host* target dan mengonfigurasinya untuk menjalankan file DLL menggunakan regsvr32.exe.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/qbot-now-pushes-black-basta-ransomware-in-bot-powered-attacks/ >

Menkominfo Minta Penyelenggara Sistem Elektronik Cegah Kebocoran Data

Menteri Komunikasi dan Informatika (Menkominfo), Johnny G Plate memaparkan langkah pemerintah untuk mencegah kebocoran data. Ia menyebut langkah pencegahan jangka panjang melalui literasi digital, sementara dalam jangka pendek dengan penerapan regulasi. Johnny menjelaskan, upaya pencegahan kebocoran data dilakukan dengan memastikan keamanan teknologi, enkripsi, serta penyiapan talenta digital yang kompeten di bidang enkripsi. Johnny menegaskan, Penyelenggara Sistem Elektronik (PSE) sebagai perpanjangan tangan dari masyarakat yang memiliki posisi sebagai wali data atau pengelola data harus memiliki tanggung jawab mencegah kebocoran data. Karena itu, pemerintah rutin melakukan pendampingan teknis. Johnny mengingatkan PSE sebagai penanggung jawab data pribadi masyarakat harus meningkatkan teknologi enkripsi yang digunakan. Kementerian Kominfo sebagai regulator akan terus melakukan audit teknologi dan memeriksa di mana letak kebocoran data. Jika ditemukan kesalahan, maka ada sanksi terhadap PSE baik lingkup privat maupun publik.

Prioritas: ***2. Urgent***

< https://www.republika.co.id/berita/rcsgwf485/menkominfo-minta-penyelenggara-sistem-elektronik-cegah-kebocoran-data >

Breachs/Hacks/Leaks

Informasi Pribadi Lebih dari 30.000 Siswa Terekspos di *Database* Tidak Terproteksi

Informasi pribadi lebih dari 30.000 siswa ditemukan di server Elasticsearch yang tidak diamankan dengan baik, hal tersebut merujuk pada laporan peneliti keamanan SafetyDetectives. Peneliti melaporkan bahwa server dibiarkan terhubung ke internet dan tidak memerlukan kata sandi untuk memungkinkan akses ke data di dalamnya. Dengan demikian, hal tersebut dapat mengekspos lebih dari satu juta catatan yang mewakili informasi pengenal pribadi atau *Personally Identifiable Information* (PII) dari 30.000 hingga 40.000 siswa. Informasi yang terungkap termasuk nama lengkap, alamat *email*, dan nomor telepon, informasi kartu kredit, rincian transaksi dan makanan yang dibeli serta informasi login yang disimpan dalam teks biasa. SafetyDetectives mencatat bahwa server yang tidak diamankan sedang diperbarui pada saat insiden, juga menemukan bukti *log server* yang menunjukkan data siswa terekspos. Para peneliti mengatakan bahwa *database* yang bocor berukuran 5GB berisi rincian siswa yang merupakan pemegang akun Transact Campus.

Prioritas: ***3. Important***

<https://www.securityweek.com/personal-information-over-30000-students-exposed-unprotected-database?&web_view=true >

Situs Web Kementerian Rusia Dilaporkan Diretas

Situs web Kementerian Konstruksi, Perumahan, dan Utilitas Rusia dilaporkan telah diretas, dengan pencarian di internet untuk situs yang mengarah ke tanda "Kemuliaan untuk Ukraina" dalam bahasa Ukraina. RIA, kantor berita negara Rusia, mengutip perwakilan kementerian pada hari Minggu, mengungkapkan bahwa situs tersebut sedang *down*, tetapi tidak berdampak pada data pribadi pengguna. RIA mengatakan bahwa peretas konon menuntut uang tebusan untuk mencegah pengungkapan data pribadi ke publik. Banyak perusahaan milik negara dan organisasi berita Rusia telah mengalami serangan dalam beberapa bulan terakhir sejak Rusia menginvasi Ukraina. Pada bulan Februari, kantor berita milik negara TASS dan surat kabar harian Kommersant diretas. Pada bulan Mei, sistem daftar televisi Rusia diretas hingga memengaruhi beberapa jaringan utama, termasuk Channel One, Rossiya-1, dan NTV-Plus. Bulan lalu juga, kelompok hacktivist Anonymous mengumumkan di media sosial bahwa mereka meluncurkan perang siber melawan kelompok pro-Rusia Killnet, yang baru-baru ini menyerang institusi Eropa.

Prioritas: ***3. Important***

< https://www.infosecurity-magazine.com/news/russian-ministry-website/?&web_view=true >

Vulnerabilities

SMSFactory Menargetkan Pengguna Android Di Delapan Negara

Para peneliti memperingatkan terhadap serangan yang sedang berlangsung oleh *malware* Android yang membuat korban berlangganan layanan premium. *Malware*, bernama SMSFactory, mencoba menginfeksi puluhan ribu pengguna di delapan negara. SMSFactory telah menargetkan lebih dari 165.000 pelanggan Avast dari Mei 2021 hingga Mei 2022. Sebagian besar korban berada di Brasil, Ukraina, Argentina, Rusia, dan Turki. Tujuan utamanya adalah untuk mengirim teks premium dan melakukan panggilan ke nomor telepon premium. Namun, *malware* dapat mencuri daftar kontak pada perangkat yang terinfeksi sebagai metode distribusi lebih lanjut untuk ancaman tersebut. Serangan ini menyebar melalui berbagai metode yang mencakup pemberitahuan *push*, *malvertising*, *pop-up* promosi di situs, video yang menawarkan peretasan untuk game, atau akses konten dewasa. Paket APK berbahaya yang berisi *malware* dihosting di toko aplikasi tidak resmi (seperti APKMods dan PaidAPKFree) yang tidak memiliki pemeriksaan dan kebijakan keamanan yang tepat untuk produk yang terdaftar.

Prioritas: ***2. Urgent***

< https://cyware.com/news/smsfactory-targets-android-users-across-eight-countries-6c2b9618 >

Bug Chain yang Belum Diperbaiki Menimbulkan Ancaman *'Mass Account Takeover'* Untuk Aplikasi Pemantauan Berat Badan Yunmai

Eksploitasi *zero-day* berantai berpotensi mengekspos semua data pengguna pada *backend* aplikasi seluler pendamping untuk timbangan pintar yang populer. Bogdan Tiron, *managing partner* di firma infosec Inggris Fortbridge, menemukan lima kerentanan di aplikasi Yunmai Smart Scale, tiga di antaranya dapat digabungkan untuk mengambil alih akun dan mengakses detail pengguna seperti nama, jenis kelamin, usia, tinggi, hubungan keluarga, dan foto profil. Pada 12 Mei, vendor produk *Internet of Things* (IoT) yang berbasis di China, Zhuhai Yunmai Technology, tampaknya telah menerapkan perbaikan hanya untuk satu kelemahan. Namun kemudian, Tiron mengatakan bahwa dia berhasil melewati *patch* tersebut. Kelemahan itu ditemukan selama uji penetrasi aplikasi Yunmai di Android dan iOS..

Prioritas: ***2. Urgent***

< https://portswigger.net/daily-swig/unpatched-bug-chain-poses-mass-account-takeover-threat-to-yunmai-weight-monitoring-app?&web_view=true >