CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 101

9 Juni 2022

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	0
URGENT	1	1	3
IMPORTANT	0	1	0

General News

BSSN-Pemprov NTT Kolaborasi *Launching* Tim Tanggap Insiden Keamanan Siber NTTPROV-CSIRT

Sebagai bentuk kesiapsiagaan terhadap insiden keamanan siber di pemerintah daerah, BSSN bersama Pemprov NTT membentuk NTTPROV-Computer Security Incident Response Team (NTTPROV-CSIRT). *Launching* NTTPROV-CSIRT dibuka secara langsung oleh Kepala BSSN Letjen TNI (Purn) Hinsa Siburian dan Wakil Gubernur NTT, Josef Nae Soi pada Rabu, 8 Juni 2022 di Aston Hotel & Convention Center, Kupang. NTTPROV-CSIRT merupakan salah satu CSIRT yang masuk dalam proyek prioritas strategis nasional (*major project*) sesuai dengan Perpres Nomor 18 Tahun 2020 tentang RPJMN 2020-2024 yang mengamanatkan pembentukan 131 CSIRT. NTTPROV-CSIRT telah teregistrasi BSSN dengan nomor registrasi 067/CSIRT.01.02/BSSN/04/2022. Pada tahun 2022 ini ditargetkan terbentuk 32 CSIRT, salah satunya NTTPROV-CSIRT. NTTPROV-CSIRT nantinya memiliki tugas untuk melakukan penaggulangan insiden, melakukan mitigasi insiden, melakukan investigasi dan analisis dampak insiden, serta melakukan pemulihan pasca insiden keamanan siber pada Pemprov NTT.

Prioritas: ***2. Urgent***

<https://kupang.tribunnews.com/2022/06/08/bssn-pemprov-ntt-kolaborasi-launching-tim-tanggap-insiden-keamanan-siber-nttprov-csirt >

Breachs/Hacks/Leaks

Malware Emotet Saat Ini Dapat Mencuri Kartu Kredit Dari Pengguna Google Chrome

Botnet Emotet sekarang mencoba menginfeksi calon korban dengan modul pencuri kartu kredit yang dirancang untuk mengumpulkan informasi yang disimpan di profil pengguna Google Chrome. Setelah mencuri info kartu kredit (yaitu, nama, bulan dan tahun kedaluwarsa, nomor kartu), *malware* akan mengirimkannya ke server *command-and-control* (C2) yang berbeda dari yang digunakan modul pencuri kartu Emotet. Perubahan perilaku ini terjadi setelah peningkatan aktivitas selama bulan April dan peralihan ke modul 64-bit. Satu minggu kemudian, Emotet mulai menggunakan file pintasan Windows (.LNK) untuk menjalankan perintah PowerShell untuk menginfeksi perangkat korban. *Malware* Emotet dikembangkan dan disebarkan dalam serangan sebagai trojan perbankan pada tahun 2014. *Malware* Emotet telah berkembang menjadi botnet yang digunakan kelompok ancaman TA542 (alias Mummy Spider) untuk mengirimkan *payload* tahap kedua. Emotet dikenal karena dapat memuat *payload* trojan *malware* Qbot dan Trickbot pada komputer korban yang disusupi, yang digunakan untuk menyebarkan *malware* tambahan, termasuk Cobalt Strike dan *ransomware* seperti Ryuk dan Conti.

Prioritas: ***2. Urgent***

<https://www.bleepingcomputer.com/news/security/emotet-malware-now-steals-credit-cards-from-google-chrome-users/ >

6,5 TB Data Sensitif Hilang dalam Pelanggaran Data Cloud Maskapai

Beberapa hari yang lalu, Pegasus Airline mengalami pelanggaran data AWS yang mengorbankan 6,5 TB data. Hal tersebut mengakibatkan 23 juta file terbuka untuk umum, termasuk informasi sensitif seperti *Personal Identity Information* (PII) awak pesawat, kata sandi *plaintext*, kunci rahasia, dan bahkan kode sumber. Pelanggaran itu ditemukan oleh vendor keamanan Safety Detectives. Tidak diketahui berapa lama kesalahan konfigurasi tersebut berlangsung, namun berpotensi dapat berdampak pada maskapai lain. Pegasus dikabarkan mengambil tindakan cepat untuk mengamankan data tersebut. Meskipun hal ini merupakan kesalahan besar, namun ini adalah kesalahan umum yang menyebabkan banyak pelanggaran data AWS profil tinggi. Bucket AWS S3 adalah penyimpanan data yang sering kali menjadi rumah bagi informasi penting bisnis. *Bucket* ini rentan terhadap kesalahan konfigurasi, seperti membiarkannya dapat diakses publik, atau tidak memerlukan autentikasi yang tepat untuk mengaksesnya.

Prioritas: ***3. Important***

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

Vulnerabilities

Varian Baru Cuba *Ransomware* Group Ditemukan Menggunakan Teknik Infeksi yang Dioptimalkan

Cuba *ransomware* adalah keluarga *malware* yang telah terdeteksi secara musiman sejak pertama kali diamati pada Februari 2020. Ini muncul kembali pada November 2021 berdasarkan pemberitahuan resmi FBI, dan dilaporkan telah menyerang 49 organisasi di lima sektor infrastruktur kritis, *ransomware* ini meraup setidaknya US$ 43,9 juta dalam pembayaran tebusan. Pembuat *malware* tampaknya mendorong beberapa pembaruan saat ini dari varian baru. Sampel yang diperiksa pada bulan Maret dan April menggunakan BUGHATCH, pengunduh khusus yang tidak digunakan oleh pelaku kejahatan dalam varian sebelumnya khusus untuk fase *staging* dari rutinitas infeksi. Analisis lebih lanjut tentang varian baru mengungkapkan bahwa aktor jahat menambahkan beberapa proses dan layanan untuk menghentikan daftar layanan berikut: MySQL, MySQL80, SQLSERVERAGENT, sqlagent.exe, sqlservr.exe, sqlwriter.exe, vmwp.exe, vmsp.exe, outlook.exe, MSExchangeUMCR, MSExchangeUM, MSExchangePOP3BE, dan banyak lainnya.

Prioritas: ***2. Urgent***

< https://www.trendmicro.com/en_us/research/22/f/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html?&web_view=true >

Owl Labs Menambal Kerentanan Kritis pada Perangkat Konferensi Video

Perusahaan konferensi video Owl Labs telah merilis patch untuk kerentanan parah yang memengaruhi perangkat Meeting Owl Pro dan Whiteboard Owl. Owl Labs Meeting Owl Pro memiliki kamera lensa 360° untuk menawarkan pemandangan panorama ruang konferensi. Fitur ini menawarkan dukungan untuk berbagai solusi konferensi video, termasuk Zoom, Skype, dan Google Meet. Peneliti keamanan dengan Modzero telah mengidentifikasi beberapa kerentanan di perangkat Owl, memperingatkan bahwa mereka dapat dieksploitasi untuk menemukan perangkat terdaftar di seluruh dunia dan mengakses data sensitif, atau bahkan mendapatkan akses ke jaringan pemilik. Para peneliti menemukan lima kerentanan di Meeting Owl Pro: CVE-2022-31459, CVE-2022-31460, CVE-2022-31461 (skor CVSS 7,4), CVE-2022-31463 (skor CVSS 8,2), dan CVE-2022-31462 (skor CVSS 9,3). Semua masalah tersebut terkait dengan kredensial *hardcode* – Meeting Owl Pro membuat titik akses Wi-Fi sendiri dengan kode sandi "hoothoot" dan memengaruhi komunikasi antara perangkat Meeting Owl Pro dan aplikasi pendamping serta *backend*-nya.

Prioritas: ***2. Urgent***

< https://www.securityweek.com/owl-labs-patches-severe-vulnerability-video-conferencing-devices?&web_view=true >

Hasil Pencarian pada CCleaner Bajakan Menyebarkan *Malware* Pencuri Informasi

Malware yang mencuri kata sandi, kartu kredit, dan dompet kripto dapat disebarkan melalui hasil pencarian untuk salinan bajakan program pengoptimalan CCleaner Pro Windows. Kampanye distribusi malware baru ini dijuluki "FakeCrack," dan ditemukan oleh analis di Avast, yang melaporkan mendeteksi rata-rata 10.000 upaya infeksi setiap hari dari data telemetri pelanggannya. Sebagian besar korban ini berbasis di Prancis, Brasil, Indonesia, dan India. *Malware* yang didistribusikan dalam kampanye ini adalah pencuri informasi yang kuat yang dapat memanen data pribadi dan aset *cryptocurrency* dan mengarahkan lalu lintas internet melalui *proxy* penyadap data.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/poisoned-ccleaner-search-results-spread-information-stealing-malware/ >