www.idsirtii.or.id

11 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 211

OVERVIEW

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

General News

Worok Sembunyikan *Malware* Baru Dalam *File* PNG Menggunakan Steganografi

Kelompok peretas yang dikenal dengan nama Worok menyembunyikan *malware* dalam *file* gambar ".PNG" untuk menginfeksi perangkat korban. Worok adalah kelompok spionase siber yang tertarik pada eksfiltrasi data, gerakan lateral, dan mata-mata pada perangkat yang terinfeksi. Tujuan utamanya adalah menanamkan *malware* pencuri informasi tanpa menimbulkan adanya peringatan pada perangkat korban. ESET menyebutkan bahwa target utama Worok adalah entitas pemerintah di Asia Tengah, Asia Tenggara, dan Afrika Selatan. Avast menduga bahwa Worok menggunakan DLL untuk mengeksekusi CLRLoader *malware loader* ke dalam memori. Hal ini didasarkan dengan adanya temuan empat DLL yang mengandung CLRLoader pada perangkat yang terkompromi. Worok menggunakan teknik *least significant bit* (LSB) *encoding* yang menyematkan potongan kecil kode berbahaya di piksel gambar.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/worok-hackers-hide-new-malware-in-pngs-using-steganography/ >

Malware IceXLoader pada Ribuan Perangkat Rumah dan Perusahaan melalui *Phising*

Kampanye *phising* yang sedang berlangsung telah menginfeksi ribuan pengguna rumahan dan perusahaan dengan versi baru *malware* "IceXLoader". *Malware loader* ini ditemukan telah meningkatkan fungsionalitasnya dan memperkenalkan adanya *multi0-stage delivery chain*. Infeksi dimulai dengan penyebaran *malware* melalui *email phising* dengan *file* ZIP yang berisi ekstraktor tahap pertama. Ekstraktor membuat *hidden folder* baru (.tmp) dan menjatuhkan *executable* tahap berikutnya. Sistem yang terinfeksi dapat di-*boot* ulang dan *registry key* baru akan ditambahkan untuk menghapus *hidden folder* tersebut saat perangkata dinyalakan kembali. *Executable* yang jatuhkan merupakan *loader* yang mengambil *file* PNG dari URL *hardcoded* dan mengubahnya menjadi *file* DLL yang diobfuskasi. Saat peluncuran pertama, IceXLoader menyalin dirinya sendiri ke dalam dua direktori dan kemudian mengumpulkan informasi berupa alamat IP, UUID, nama pengguna dan nama perangkat, versi OS Windows, produk keamanan terpasang, kehadiran .NET Framework, informasi pernagkat keras, dan *timestamp*.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/phishing-drops-icexloader-malware-on-thousands-of-home-corporate-devices/ >

Breachs/Hacks/Leaks

Bjorka Klaim Miliki 44 Juta Data MyPertamina

Bjorka kembali mengklaim telah memiliki data yang diduga merupakan data pelanggan MyPertamina. Data tersebut dijual seharga Rp392 Juta dalam bentuk Bitcoin. Hal tersebut disampaikannya melalui BreachForums pada Kamis, 10 November 2022 dengan judul "MYPERTAMINA INDONESIA 44 MILION". Dalam informasi tersebut, Bjorka mengungkapkan bahwa kebocoran data tersebut terdiri dari *file* terkompresi 6GB, tidak terkompresi 30 GB, dengan total 44.237.264 data. Pembocoran data dengan format CSV ini memuat informasi pelanggan berupa nama, *email,* alamat, DOB, *gender,* pendapatan, dan lain-lain.

Prioritas: ***1. Critical***

< https://cyberthreat.id/read/14773/Bjorka-Beraksi-Lagi-Kini-Klaim-Miliki-44-Juta-Data-MyPertamina >

Vulnerabilities

Cisco Terbitkan Imbauan Keamanan Terkait Kerentanan SSL/TLS *Client* pada Adaptive Security Appliance (ASA) dan Cisco Firepower Threat Defense (FTD)

Kerentanan pada SSL/TLS *Client* dari perangkat lunak Adaptive Security Appliance (ASA) dan Cisco Firepower Threat Defense (FTD) dapat memungkinkan penyerang jarak jauh yang terautentikasi menyebabkan terjadinya denial of service (DoS) pada perangkat terpengaruh. Kerentanan ini disebabkan oleh manajemen memori yang tidak tepat saat pernagkat memulai koneksi SSL/TLS. Pernyerang dapat mengekspolitasi kerentanan ini dengan memastikan bahwa perangkat akan terhbung ke server SSL/TLS yang menggunakan parameter enkripsi tertentu. Kerentanan ini memengaruhi produk Cisco yang menjalankan rilis ASA dan FTD Seri 5500-X, Seri Firepower 4100, dan Seri Firepower 9300. Cisco telah merilis pembaruan perangkat lunak untuk mengatasi kerentanan ini.

Prioritas: ***2. Urgent***

< https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssl-client-dos-cCrQPkA >

Kerentanan *Firmware* UEFI Baru Dilaporkan pada Beberapa Model Notebook Lenovo

Lenovo telah mengatasi tiga kerentanan dalam *firmware* Unified Extensible Firmware Interface (UEFI) yang memengaruhi beberapa perangkat Lenovo, yaitu Yoga, IdeaPad, dan ThinkBook. Kerentanan yang dilacak sebagai CVE-2022-3430, CVE-2022-3431, dan CVE-2022-3432 dapat disalahgunakan untuk menonaktifkan UEFI *Secure Boot*, mekanisme keamanan yang dirancang untuk mencegah program jahat dari *loading* selama proses *boot*. Kerentanan ini memungkinkan penyerang untuk mengeksekusi *boot loader* jahat, memberikan penyerang akses istimewa kepada *host* yang disusupi dengan memodifikasi variabel NVRAM. CVE-2022-3430 diketahui berdampak pada WMI Setup *driver* pada beberapa produk Notebook Lenovo, CVE-2022-3431 diketahui berdampak pada *driver* yang digunakan selama proses pembuatan pada beberapa perangkat Notebook Lenovo konsumen yang secara keliru tidak dinonaktifkan, sedangkan CVE-2022-3432 berdampak pada *driver* yang digunakan pada IdeaPad Y700-14ISK yang secara keliru tidak dinonaktifkan.

Prioritas: ***1. Critical***

< https://thehackernews.com/2022/11/new-uefi-firmware-flaws-reported-in.html >

Peretas Dihadiahi $70.000 Karena Menemukan Cara untuk Melewati Layar Kunci Ponsel Google Pixel

Kerentanan pada layar kunci ponsel Google Pixel, yang dilacak sebagai CVE-2022-20465, telah diperbaiki sebagai bagian dari pembaruan Android bulanan untuk November 2022. Kerentanan ini memungkinkan penyerang dengan akses fisik untuk melewati layar kunci (sidik jari, PIN, dan lain-lain) dan mendapatkan akses penuh ke perangkat pengguna. Schütz, yang berhasil melakukan *bypass* pada layar kunci tersebut dihadiahi $70.000. Menurut peneliti, akar masalah terletak pada adanya kenyataan bahwa perlindungan layar kunci sepenuhnya dikalahkan saat mengikuti aturan tertentu, seperti *swap* SIM dan kode PUK. Schütz menjelaskan bahwa penyerang bisa saja menukar SIM di perangkat korban, dan melakukan eksploitasi dengan kartu SIM yang memiliki kunci PIN dan penyerang mengetahui kode PUK yang benar.

Prioritas: ***2. Urgent***

< https://thehackernews.com/2022/11/hacker-rewarded-70000-for-finding-way.html >