CENTAURI
TECHONOLOGIES CORPORATION

VULNERABILIDADES QUE DAN DE QUE HABLAR

JUNIO 2022

CVE-2022-24706: Apache CouchDB: Remote Code Execution Vulnerability in Packaging

En Apache CouchDB con versiones anteriores a 3.2.2, un atacante puede acceder a una instalación predeterminada incorrectamente protegida sin autenticarse y obtener privilegios de administrador.

Es recomendable la implementación de controles en todas las instalaciones de CouchDB. La API de CouchDB está disponible en el puerto registrado '5984' y este es el único puerto que debe exponerse para una instalación de un solo nodo.

MITIGACIÓN: CouchDB 3.2.2 en adelante se negará a comenzar con el valor predeterminado anterior de la cookie Erlang de 'monstruo'. Instalaciones que se actualizan a estas versiones se ven obligadas a elegir un valor diferente.

Fuente: https://www.openwall.com/lists/oss-security/2022/04/26/1
https://nvd.nist.gov/vuln/detail/CVE-2022-24706

CVE-2022-26775: Security Update 2022-004 Catalina: libresolv

Un atacante puede provocar el cierre inesperado de la aplicación o la ejecución de código arbitrario.

MITIGACIÓN: Mitigación: Este problema se corrigió en la actualización de seguridad 2022-004 Catalina, macOS Monterey 12.4. Se solucionó el desbordamiento de enteros con una validación de entrada mejorada.

Fuente: https://nvd.nist.gov/vuln/detail/CVE-2022-26775
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26775

CVSS:3.1 8.3 / 7.2

CVE-2022-22021: Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability

Un atacante podría hospedar un sitio web diseñado para aprovechar la vulnerabilidad por MS Edge y convencer a un usuario para que vea el sitio web. Sin embargo, en todos los casos, el atacante no podría obligar al usuario a ver el contenido. En su lugar, tendría que convencer al usuario para que tome medidas, generalmente mediante una invitación en un e-mail o mensaje instantáneo, o haciendo que el usuario abra un archivo adjunto enviado por e-mail.

Versión afectada: 102.0.1245.39, lanzada el 9 de junio de 2022, basada en Chromium 102.0.5005.61

Fuente: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22021

CVSS:3.1 7.8 / 7.0

CVE-2022-30190: Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability

Esta vulnerabilidad, también conocidad como “Follina” Permite a un atacante generar un documento Word malicioso y enviarlo a su objetivo. Un atacante que aproveche esta vulnerabilidad puede ejecutar código arbitrario con los privilegios de la aplicación. El atacante podría instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas según los permisos del usuario.

MITIGACIÓN: Microsoft recomienda instalar las actualizaciones de junio lo antes posible.

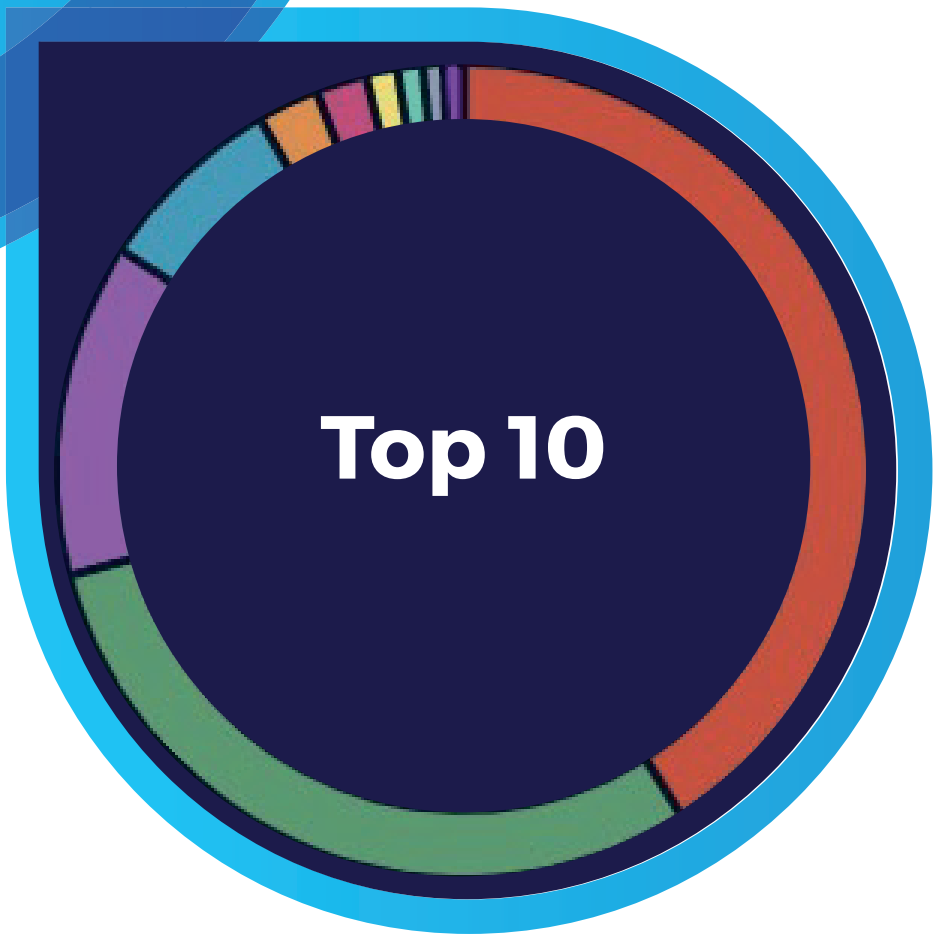
Afecta versiones de Windows 10, 8.1, 7, WS2022, WS2019, WS2016, WS2012, WS2008

Fuente: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

MALWARES MÁS ACTIVOS

período del 13 de mayo a 13 de junio de 2022

De acuerdo a lo reportado por **MANDIANT** en el último mes, los malware con mayor actividad se muestran a continuación



- AgentTesla
- LokiBot
- Dridex
- Formbook
- Qakbot
- Nanocore
- Remcos
- AZORult
- MAKOP
- Ursnif

MALWARES MÁS ACTIVOS

EMOTET

Un troyano que se propaga principalmente a través de correos electrónicos de spam (malspam). La infección puede llegar a través de archivos de órdenes maliciosos, archivos de documentos habilitados para macros o enlaces maliciosos. Los correos electrónicos de Emotet pueden contener imágenes de marcas conocidas diseñadas para que parezcan un correo electrónico legítimo.

FORMBOOK

Es un infostealer que recopila las credenciales de varios navegadores web, reúne capturas de pantalla, monitoriza y registra las pulsaciones de las teclas, y es capaz de descargar y ejecutar archivos de acuerdo con sus órdenes de comando y control (C&C).

LOKIBOT

Es un malware perteneciente a la familia de troyanos, utilizado en campañas a nivel global. Fue diseñado con el objetivo de robar credenciales de navegadores, clientes FTP/ SSH, sistemas de mensajería, y hasta incluso de billeteras de criptomonedas.

AGENTTESLA

Un malware del tipo remote access trojan (RAT), distribuido como un Malware-as-a-Service (MaaS) en campañas a nivel global. Es usado para espiar y robar información de los equipos comprometidos, es capaz de extraer credenciales de distintos softwares, obtener cookies de navegadores de Internet, registrar las pulsaciones del teclado de la máquina (Keylogging), realizar capturas de pantalla y del clipboard (portapapeles).

MALWARES MÁS ACTIVOS

NANOCORE

Tiene una variedad de funciones como keylogger, un ladrón de contraseñas que puede pasar datos de forma remota al operador de malware. También tiene la capacidad de manipular y ver imágenes de cámaras web, bloqueo de pantalla, descarga y robo de archivos, y más.

REMCOS

Remcos (acrónimo de Remote Control & Surveillance Software) es un software de acceso remoto utilizado para controlar computadoras de forma remota. Una vez instalado, abre una puerta trasera en la computadora, otorgando acceso completo al usuario remoto. Se puede utilizar para fines de vigilancia y pruebas de penetración, y en algunos casos se ha utilizado en campañas de piratería.

URSNIF

Es uno de los troyanos bancarios más extendidos. El código fuente del malware se filtró en 2015 y se puso a disposición del público en Github, lo que permitió a otros autores de malware agregar nuevas características y realizar un mayor desarrollo del código por parte de diferentes actores de amenazas. Puede recopilar la actividad del sistema de las víctimas, registrar las pulsaciones de teclas y realizar un seguimiento de la actividad de la red / navegador. Archiva los datos recopilados antes de enviarlos al servidor de C&C.

NETWIRE

Es un troyano de acceso remoto. Se sabe que los ciberdelincuentes usan NetWire para registrar las pulsaciones de teclas en dispositivos periféricos y lectores de tarjetas USB. También, registra las claves pulsadas para robar credenciales de cuentas en internet y varias aplicaciones como correo electrónico, navegadores web, etc.

MALWARES MÁS ACTIVOS

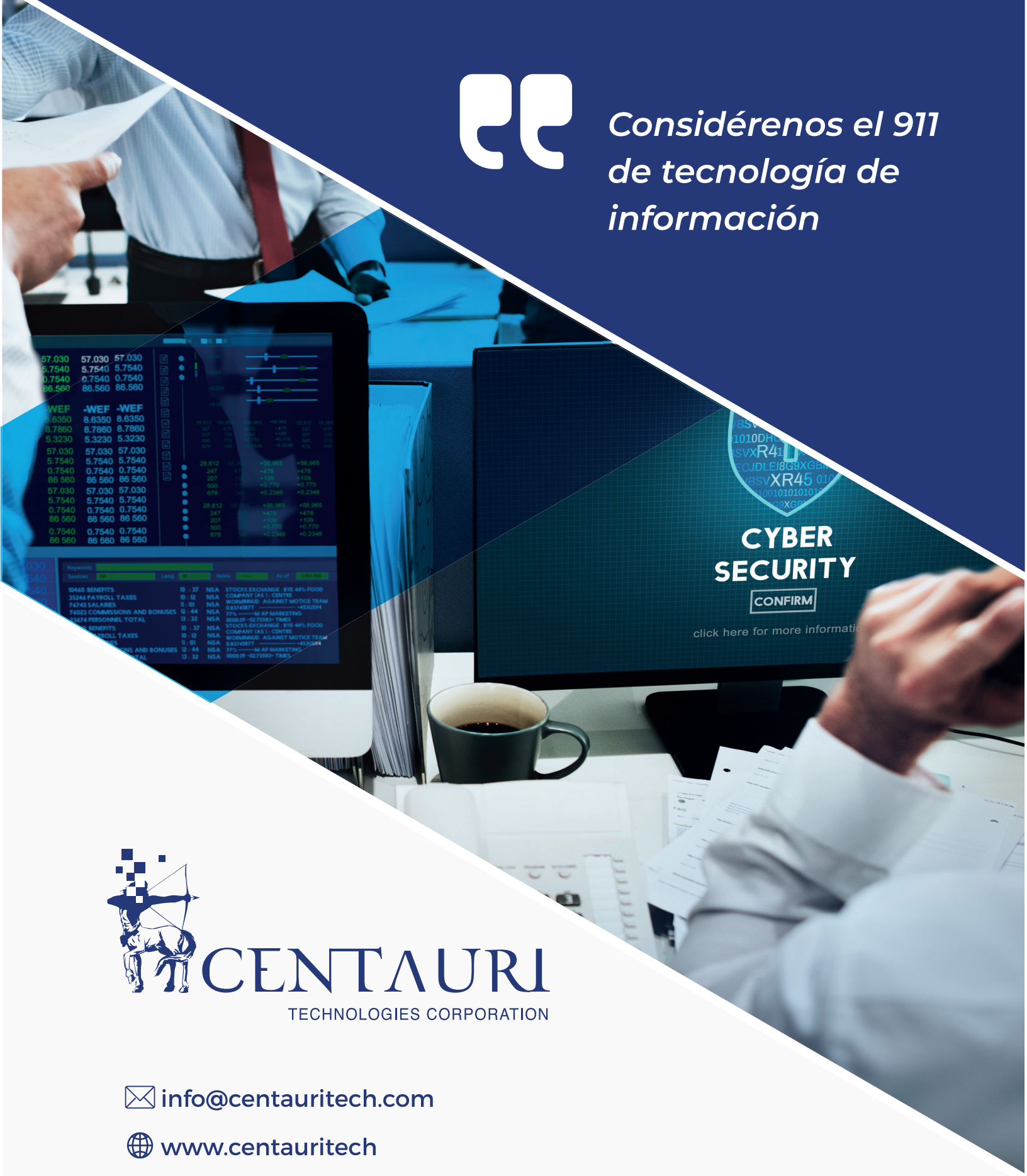
QAKBOT

Un troyano bancario diseñado para robar información personal. Se propaga usando varias campañas de correo basura. Vienen con adjuntos maliciosos (documentos de Office, normalmente Word) que se presentan como documentos importantes (facturas, recibos, etc.). Los delincuentes intentan engañar a los usuarios para que abran esos archivos, permitiendo la infiltración de Qakbot.

BEACON

También conocido como payload, es un ejecutable o programa que se comunica con un ciberatacante a través de algún canal de comunicación. Desde el punto de vista del actor de amenazas, la gestión de balizas es la base de su campaña maliciosa.

Considérenos el 911 de tecnología de información



CENTAURI
TECHNOLOGIES CORPORATION

info@centauritech.com

www.centauritech

Tel: (+507) 317-1217

Centauri Technologies Corporation