COTEDEM
Consultores Tecnológicos y Desarrollo Empresarial

# INFORME DE INTELIGENCIA DE AMENAZAS CIBERNETICAS

## COTEDEM S.A.

**Fecha de generación:** 19/07/2024

**Resumen Ejecutivo**

Este informe proporciona una visión detallada de las amenazas cibernéticas detectadas y analizadas entre el 01/01/2024 hasta hoy. Se destacan las amenazas más críticas, los patrones emergentes y las recomendaciones para la mitigación de los riesgos. Este análisis es fundamental para fortalecer la seguridad cibernética y progteger los activos de la organización.

Gráficos obtenidos:





## Detalle de Amenazas

**Cerberus**

Es un sofisticado troyano bancario con funcionalidad de acceso remoto al dispositivo donde se instala (Remote Acces Trojan), que además del robo de datos bancarios, permite el robo de patrones de desbloqueo del teléfono, la superposición de pantallas (por ejemplo, para suplantar las de petición de claves), y la captura de los códigos de Google Authenticator. Todo ello de forma invisible para el usuario.

**CoralRaider**
Distribuye tres infostealers conocidos: Cryptbot, LummaC2 y Rhadamanthys. Utiliza métodos sofisticados para evadir sistemas de seguridad y afecta a víctimas en múltiples países. Comienza con un archivo LNK descargado mediante un enlace engañoso, que ejecuta un comando PowerShell para descargar y ejecutar un archivo HTML malicioso (HTA). El actor de amenazas usa una red de distribución de contenido (CDN) para alojar y distribuir archivos maliciosos, evitando la detección y minimizando el tiempo de respuesta. Emplea técnicas avanzadas de evasión, como el uso del “FoDHelper” para ejecutar scripts con privilegios elevados y eludir las advertencias de Control de Acceso de Usuario (UAC) de Windows.

**LABHost**
Distribuye malware usando un archivo LNK engañoso que ejecuta un comando PowerShell para descargar un archivo HTML malicioso (HTA). Este archivo instala infostealers como Cryptbot, LummaC2 o Rhadamanthys. Los atacantes usan una CDN para distribuir el malware y técnicas avanzadas como el "FoDHelper" para evadir la detección y obtener privilegios elevados en el sistema.

**KageNoHitobito**
Cifra los datos en la computadora de la víctima, haciendo los archivos inaccesibles sin una clave de descifrado. Los atacantes exigen un rescate a cambio de la clave que permitirá recuperar los archivos. Este ransomware crea una nota de rescate llamada KageNoHitobito_ReadMe.txt en cada carpeta con archivos cifrados.

**Mallox**
Cifra los archivos de la víctima y demanda un rescate a cambio de la clave de descifrado. Este malware emplea métodos avanzados para evitar la detección y se propaga a través de técnicas como correos electrónicos de phishing y descargas maliciosas. Una vez que Mallox infecta un sistema, cifra los archivos y deja una nota de rescate con instrucciones para pagar el rescate y recuperar los archivos cifrados.

**SideCopy**
Es una campaña de ciberespionaje que se dirige principalmente a organizaciones en Asia del Sur, imitando las tácticas del grupo APT Sidewinder. Utiliza correos electrónicos de spear phishing con documentos maliciosos para infectar sistemas. El malware roba información sensible y mantiene el acceso persistente a los sistemas infectados. Además, emplea técnicas avanzadas de evasión, como cargas útiles modulares y cambio frecuente de infraestructura de comando y control.

## Detalle de Vulnerabilidades

**CVE-2024-3094**
Afecta a las versiones 5.6.0 y 5.6.1 de XZ Utils, una biblioteca de compresión de datos. Permite que un atacante remoto ejecute código arbitrario en sistemas afectados antes de la autenticación, comprometiendo la máquina. Para mitigar el riesgo, se recomienda actualizar a versiones no comprometidas como XZ Utils 5.4.6.

**CVE-2024-3400**
Se refiere a una falla en el sistema o software que permite a un atacante realizar una acción no autorizada o comprometer la seguridad del sistema. Para obtener detalles específicos sobre esta vulnerabilidad

**CVE-2024-1709**
Afecta al software ConnectWise ScreenConnect, utilizado para el acceso remoto y el escritorio. Esta vulnerabilidad crítica permite que un atacante no autenticado ejecute código arbitrario de forma remota sin interacción del usuario.

**CVE-2024-0185**
Afecta al sistema operativo Microsoft Windows y está relacionada con una brecha de seguridad en el servicio de impresión. Esta vulnerabilidad permite a un atacante local ejecutar código arbitrario con privilegios elevados, comprometiendo el sistema afectado.

**CVE-2024-0100**
Afecta al NVIDIA Triton Inference Server para Linux. En este caso, un usuario puede corromper archivos del sistema a través de la API de trazado. Si se explota con éxito, esto podría provocar una denegación de servicio y alteración de datos.

**CVE-2024-0054**
Afecta a Microsoft Edge (Chromium-based) y está relacionada con un problema de divulgación de información en el navegador. Un atacante podría obtener información sensible del sistema afectado a través de un sitio web malicioso. Se recomienda actualizar a la versión más reciente de Microsoft Edge para corregir la vulnerabilidad.

## Recomendaciones

**1. Mejora en la Protección contra Ransomware:**

- Implementar soluciones de respaldo y recuperación que sean robustas y probadas regularmente.
- Configurar sistemas de detección y respuesta ante amenazas (EDR) para identificar y bloquear actividades sospechosas.

**2. Fortalecimiento de la Conciencia de Seguridad:**

- Realizar capacitaciones periódicas sobre ciberseguridad para todos los empleados, enfocándose en la detección de phishing y otras técnicas de ingeniería social.
- Utilizar simulaciones de ataques para evaluar y mejorar la respuesta de los empleados ante posibles amenazas.

**3. Actualización de Políticas de Seguridad:**

- Revisar y actualizar las políticas de seguridad de la información para asegurar que estén alineadas con las mejores prácticas actuales y las normativas internacionales, como la ISO 27001.
- Implementar una política de contraseñas seguras y multifactor (MFA) para todas las cuentas de usuario.