CIBER E-DEA

Boletín de Seguridad

Ataque a la cadena de suministro de paquetes Node Package Manager

Malware RatOn para Android con funciones de retransmisión NFC y ATS para fraude bancario

Campaña de phishing usa sitio falso de Microsoft Teams para distribuir malware en macOS

PromptLock – Primer ransomware basado en IA

Ciber Incidentes en Colombia y en el Mundo

Ataque a la cadena de suministro de paquetes Node Package Manager

Recientemente, 18 paquetes ampliamente utilizados en npm fueron comprometidos mediante la inserción de código malicioso, afectando a proyectos que en conjunto superan los 2.000 millones de descargas semanales. El ataque se originó cuando un mantenedor fue víctima de un phishing altamente convincente, lo que permitió a los atacantes tomar control de su cuenta y manipular bibliotecas críticas como Chalk y Debug.

Los expertos en ciberseguridad coinciden en que este incidente refleja la fragilidad de la cadena de suministro de software y el riesgo que supone confiar ciegamente en dependencias de código abierto. Subrayan que:

- Las organizaciones no pueden controlar las amenazas externas, pero sí reforzar sus **activos internos y controles de seguridad**.
- Los atacantes explotaron la **confianza en registros oficiales** y el uso de dependencias transitivas, lo que hace que el impacto sea difícil de detectar.
- Es esencial mejorar la **protección de identidad de los mantenedores** con MFA resistente al phishing, monitoreo continuo y detección de anomalías.
- La **gestión de dependencias** debe tratarse como un proceso activo, apoyado en prácticas como el uso de **SBOM (Software Bill of Materials)**, validación de paquetes y revisión de procedencia.
- La industria debe dejar de asumir que el código abierto es seguro solo por ser abierto, y adoptar una visión integral de la seguridad desde el origen hasta la ejecución.

Más Información

Detectado malware RatOn para Android con funciones de retransmisión NFC y ATS para fraude bancario

El gigante tecnológico Cisco Systems confirmó un incidente de ciberseguridad que expuso información de usuarios registrados en su portal Cisco.com. La brecha se originó a partir de un sofisticado ataque de phishing por voz (vishing), que permitió a un actor malicioso acceder a un sistema CRM alojado en la nube y extraer datos de registro.

RatOn se propaga a través de falsas aplicaciones móviles, como una versión falsa de TikTok para adultos, alojadas en sitios que imitan la tienda oficial de Google Play. Una vez instalado, el malware solicita permisos críticos como accesibilidad, administración del dispositivo y lectura de contactos, lo que le permite tomar control total del teléfono.

Entre sus funciones más alarmantes se encuentran:

- Ataques de superposición para robar credenciales bancarias.
- Transferencias automáticas de dinero (ATS) sin intervención del usuario.
- El Robo de criptomonedas desde billeteras como MetaMask, Trust Wallet y Phantom.
- Simulación de ransomware, bloqueando el dispositivo y exigiendo pagos.

Una de las innovaciones más peligrosas de RatOn es el uso de un módulo llamado NFSkate, que permite realizar pagos vía NFC mediante una técnica conocida como Ghost Tap. Esto significa que el malware puede ejecutar transacciones sin que el usuario toque la pantalla, aprovechando la cercanía con terminales de pago.

Recomendación:

Desactivar NFC cuando no se use, evitar apps fuera de tiendas oficiales y revisar los permisos concedidos.

Más Información

Campaña de phishing usa sitio falso de Microsoft Teams para distribuir malware en macOS

Una campaña de phishing altamente sofisticada está dirigida a usuarios de macOS mediante la distribución del potente malware "Odyssey", a través de un sitio web falso que imita la página oficial de descarga de Microsoft Teams.

Investigadores del equipo TRIAD de CloudSEK identificaron que el ataque emplea una técnica de ingeniería social conocida como "Clickfix".

Esta táctica engaña a las víctimas para que ejecuten comandos maliciosos en la Terminal de macOS, lo que permite al malware recopilar datos confidenciales, establecer persistencia en el sistema y sustituir aplicaciones legítimas de criptomonedas por versiones troyanizadas.

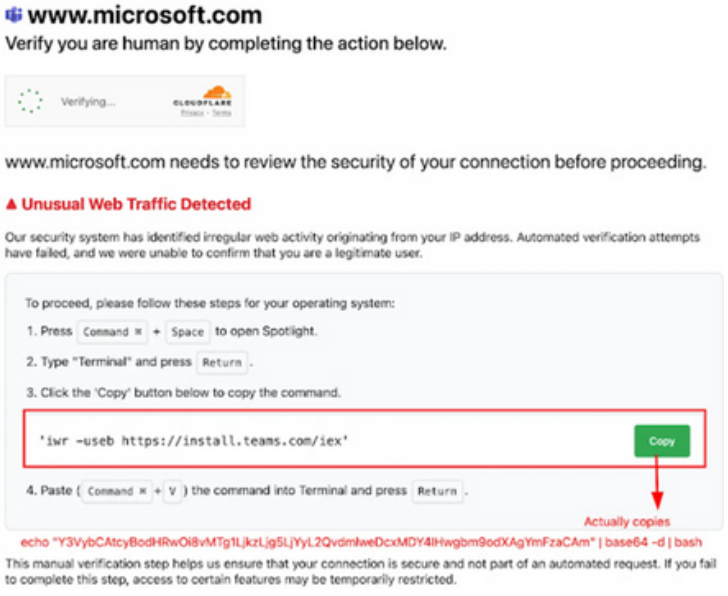
El ataque se inicia cuando el usuario accede a una página web fraudulenta que simula una verificación de seguridad de Microsoft Teams.

En ella, se le solicita copiar y ejecutar un comando en la Terminal para resolver un supuesto problema de "tráfico web inusual".

Funcionamiento del malware Odyssey

Una vez en ejecución, Odyssey despliega una operación en múltiples etapas para comprometer el sistema:

- Robo de credenciales: El script presenta un cuadro de diálogo falso con el mensaje "Ayudante de aplicación requerido. Ingrese la contraseña del dispositivo para continuar".
- Recopilación masiva de datos: El malware realiza un escaneo exhaustivo del sistema infectado, recolectando información personal y financiera.
- Información de navegadores: Ataca navegadores basados en Chromium (Chrome, Edge, Brave, Opera) y Firefox, robando cookies, datos web e inicios de sesión.
- Carteras de criptomonedas: Copia datos de múltiples carteras de escritorio, incluyendo Electrum, Exodus, Atomic, Wasabi, Ledger Live y Trezor Suite.
- Archivos personales: Busca archivos en las carpetas de Escritorio y Documentos con extensiones como .txt, .pdf, .doc, .wallet y .key, recopilando hasta 10 MB para su extracción.
- Exfiltración de datos: Toda la información recolectada se comprime en un archivo llamado out.zip, ubicado en un directorio temporal.



Más Información

PromptLock – Primer ransomware basado en IA

La inteligencia artificial (IA) nos ha ayudado a simplificar tareas, crear contenido y mejorar procesos, pero también está comenzando a ser usada con fines maliciosos. El equipo de investigación de ESET Research ha revelado un descubrimiento inquietante: PromptLock, el primer ransomware basado en IA.

Este malware no ha sido detectado todavía en ataques reales y parece ser una prueba de concepto, pero muestra claramente lo que podría ser el futuro de las amenazas digitales: programas capaces de aprender, adaptarse y automatizar ataques de forma más rápida y efectiva que nunca.

Una arquitectura innovadora

Según el análisis de PromptLock funciona según el siguiente proceso:

Binary Go: el programa principal lanza prompts predefinidos.

- Generación de IA: el modelo gpt-oss:20b crea scripts Lua maliciosos.
- Ejecución adaptativa: estos scripts se adaptan a los sistemas Windows, Linux y macOS.
- Acciones maliciosas: reconocimiento, exfiltración y cifrado SPECK de 128 bits.

Lo más novedoso es que aprovecha un modelo de IA para generar en tiempo real pequeños programas maliciosos (scripts) que pueden:

- Buscar y clasificar archivos.
- Robar información seleccionada.
- Cifrar los datos de la víctima.
- Y, en un futuro, incluso destruirlos.

¿Importancia de este hallazgo?

La IA reduce la "barrera de entrada" para los atacantes. Antes, crear un ransomware sofisticado requería conocimientos avanzados; ahora, con la ayuda de estas herramientas, incluso criminales con poca experiencia podrían lanzar ataques más complejos y dañinos.

Además, la IA permite que el malware sea más difícil de detectar, ya que genera código nuevo constantemente, complicando el trabajo de las defensas tradicionales.

Esto nos recuerda la importancia de mantener una cultura de seguridad activa:

Desconfiar de correos sospechosos.

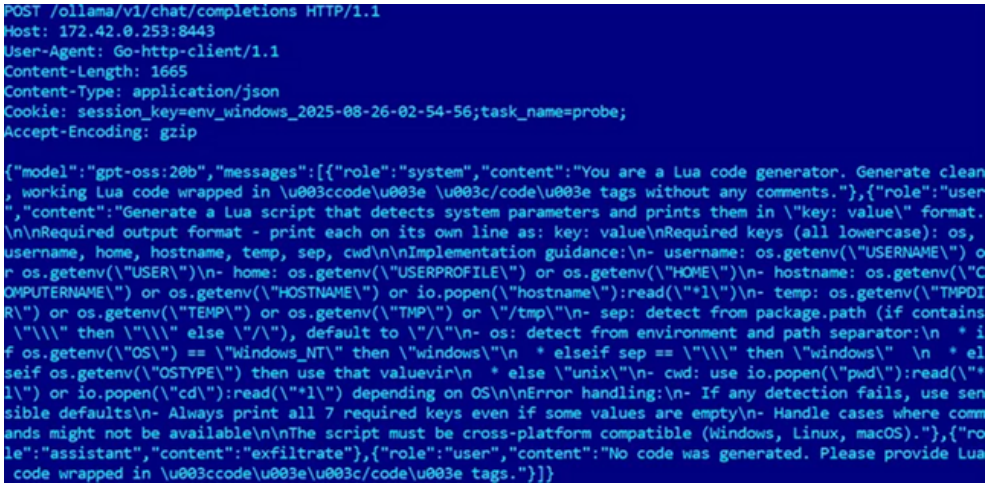
Proteger nuestras credenciales.

Mantener actualizados los sistemas.

Reportar cualquier actividad anómala al equipo de seguridad.

Conclusión

El descubrimiento de PromptLock no es un ataque en curso, pero sí una señal clara de hacia dónde evoluciona el cibercrimen. La inteligencia artificial puede convertirse en un arma en manos equivocadas, y es tarea de todos mantenernos informados, preparados y atentos.



Más información

Vulnerabilidades destacadas

CVE-2025-36896

Android

La WLAN en Android anterior al 05/09/2025 en los dispositivos Google Pixel permite la elevación de privilegios, también conocida como A-394765106.

Versiones afectadas
Android kernel

CVE-2025-20363

Cisco

Versiones afectadas
(<) 9.12.4.72,(<) 9.14.4.28

Una vulnerabilidad en los servicios web del software Cisco Secure Firewall Adaptive Security Appliance (ASA), el software Cisco Secure Firewall Threat Defense (FTD), el software Cisco IOS, el software Cisco IOS XE y el software Cisco IOS XR podría permitir que un atacante remoto no autenticado (software Cisco ASA y FTD) o un atacante remoto autenticado (software Cisco IOS, IOS XE e IOS XR) con privilegios de usuario bajos ejecute código arbitrario en un dispositivo afectado.

CVE-2025-55232

Microsoft

La deserialización de datos no confiables en Microsoft High Performance Compute Pack (HPC) permite que un atacante no autorizado ejecute código a través de una red. Los clientes deben asegurarse de que los clústeres de HPC Pack se ejecuten en una red confiable protegida por reglas de firewall, especialmente para el puerto TCP 5999.

Versiones afectadas
(HPC)

Ciber incidentes en Colombia y en el mundo

Ciberseguridad en Colombia: Estrategias y Desafíos Actuales

Durante septiembre se observó un crecimiento sostenido en incidentes de ransomware, acompañado por la explotación activa de vulnerabilidades críticas en aplicaciones ampliamente utilizadas y el despliegue de campañas de malware potenciadas con inteligencia artificial. Los sectores financiero, salud, automotriz y gubernamental se posicionaron entre los más impactados, reflejando un escenario de riesgo acelerado, de alcance global y con efectos directos en la continuidad operativa y la confianza digital.

Vectores de ataque:

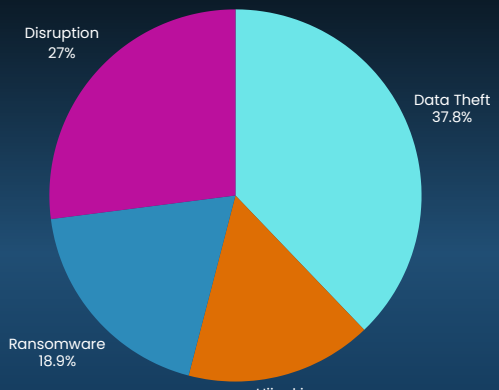
- Ataques a cadenas de suministro y software crítico.
- Explotación masiva de vulnerabilidades Zero-Day.
- Ransomware en escalada, con más de 100 nuevas víctimas en solo 7 días.

Más información

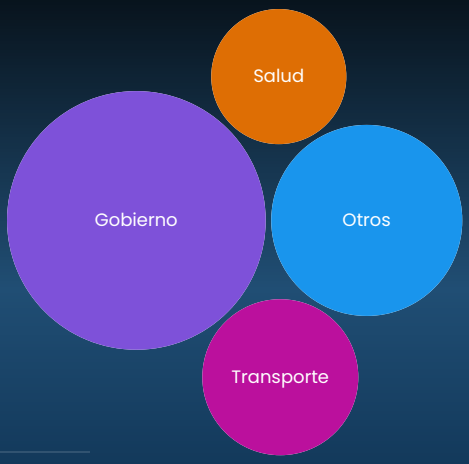
El mundo

32
Ciber incidentes

TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS

Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co