Verne
TECHNOLOGY GROUP

Boletín de alertas

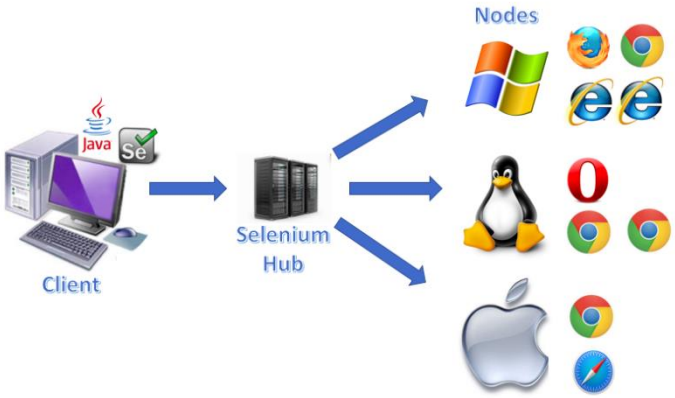
Newsletter Seguridad Verne

Vol. 31/24

ÍNDICE

CIBERATAQUE EN CURSO APUNTA A SERVICIOS DE SELENIUM GRID EXPUESTOS PARA MINERÍA DE CRIPTOMONEDAS

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Ciberataque	Selenium Grid	Alta



Los investigadores de ciberseguridad están haciendo sonar la alarma sobre una campaña en curso que aprovecha los servicios de Selenium Grid expuestos a Internet para la minería ilícita de criptomonedas.

La empresa de seguridad en la nube Wiz está rastreando la actividad bajo el nombre de SeleniumGreed

Sin que la mayoría de los usuarios lo sepan, la API Selenium WebDriver permite una interacción completa con la propia máquina, incluida la lectura y descarga de archivos y la ejecución de comandos remotos", dijeron los investigadores de Wiz Avigayil Mechtinger, Gili Tikochinski y Dor Laska .

De manera predeterminada, la autenticación no está habilitada para este servicio. Esto significa que muchas instancias de acceso público están mal configuradas y cualquier persona puede acceder a ellas y utilizarlas de forma abusiva con fines maliciosos.

Selenium Grid, parte del marco de pruebas automatizadas de Selenium, permite la ejecución paralela de pruebas en múltiples cargas de trabajo, diferentes navegadores y varias versiones de navegador.

Selenium Grid debe protegerse del acceso externo mediante permisos de firewall adecuados, advierten los mantenedores del proyecto en una documentación de soporte, afirmando que no hacerlo podría permitir que terceros ejecuten binarios arbitrarios y accedan a archivos y aplicaciones web internos.

Aún no se sabe exactamente quién está detrás de la campaña de ataques. Sin embargo, se trata de un atacante que ataca instancias expuestas públicamente de Selenium Grid y hace uso de la API WebDriver para ejecutar el código Python responsable de descargar y ejecutar un minero XMRig.

Todo comienza con el adversario enviando una solicitud al centro vulnerable Selenium Grid con el objetivo de ejecutar un programa Python que contiene una carga útil codificada en Base64 que genera un shell inverso a un servidor controlado por el atacante para obtener la carga útil final, una versión modificada del minero XMRig de código abierto.

En lugar de codificar la IP del pool en la configuración del minero, la generan dinámicamente en tiempo de ejecución, explicaron los investigadores. También configuran la función de huella digital TLS de XMRig dentro del código agregado (y dentro de la configuración), lo que garantiza que el minero solo se comunicará con servidores controlados por el actor de la amenaza.

Se dice que la dirección IP en cuestión pertenece a un servicio legítimo que ha sido comprometido por el actor de amenazas, ya que también se descubrió que alberga una instancia de Selenium Grid expuesta públicamente.

Wiz dijo que es posible ejecutar comandos remotos en versiones más nuevas de Selenium y que identificó más de 30.000 instancias expuestas a la ejecución de comandos remotos, lo que hace imperativo que los usuarios tomen medidas para cerrar la configuración incorrecta.

ESTE SERVICIO CONTRA DELITOS CIBERNÉTICOS BASADO EN INTELIGENCIA ARTIFICIAL COMBINA KITS DE PHISHING CON APLICACIONES MALICIOSAS PARA ANDROID

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Malware	Android	Alta

Se ha observado que un grupo de ciberdelincuencia de habla hispana llamado GXC Team combina kits de phishing con aplicaciones maliciosas para Android, llevando las ofertas de malware como servicio (MaaS) al siguiente nivel.

La empresa de ciberseguridad de Singapur Group-IB, que ha estado rastreando al actor del crimen electrónico desde enero de 2023, describió la solución de crimeware como una "sofisticada plataforma de phishing como servicio impulsada por IA capaz de atacar a usuarios de más de 36 bancos españoles, organismos gubernamentales y 30 instituciones en todo el mundo.

El kit de phishing tiene un precio de entre 150 y 900 dólares al mes, mientras que el paquete que incluye el kit de phishing y el malware para Android está disponible mediante suscripción por unos 500 dólares al mes.

Entre los objetivos de la campaña se encuentran usuarios de entidades financieras españolas, así como servicios tributarios y gubernamentales, comercio electrónico, bancos y casas de cambio de criptomonedas de Estados Unidos, Reino Unido, Eslovaquia y Brasil. Hasta el momento se han identificado hasta 288 dominios de phishing vinculados a la actividad.

También forma parte del espectro de servicios ofrecidos la venta de credenciales bancarias robadas y esquemas de codificación personalizados por encargo para otros grupos cibercriminales que apuntan a empresas bancarias, financieras y de criptomonedas.

A diferencia de los desarrolladores de phishing típicos, el equipo GXC combinó kits de phishing junto con un malware ladrón de OTP de SMS, haciendo que un escenario de ataque de phishing típico cambiara hacia una dirección ligeramente nueva, dijeron los investigadores de seguridad Anton Ushakov y Martijn van den Berk en un informe del jueves.

Lo que llama la atención aquí es que los actores de amenazas, en lugar de utilizar directamente una página falsa para obtener las credenciales, instan a las víctimas a descargar una aplicación bancaria basada en Android para evitar ataques de phishing. Estas páginas se distribuyen mediante smishing y otros métodos.

Una vez instalada, la aplicación solicita permisos para ser configurada como la aplicación de SMS predeterminada, lo que permite interceptar contraseñas de un solo uso (OTP) y otros mensajes y exfiltrarlos a un bot de Telegram bajo su control.

En la etapa final, la aplicación abre el sitio web de un banco genuino en WebView, lo que permite a los usuarios interactuar con él con normalidad, dijeron los investigadores. Después de eso, cada vez que el atacante activa el mensaje OTP, el malware para Android recibe y reenvía silenciosamente mensajes SMS con códigos OTP al chat de Telegram controlado por el actor de la amenaza.

Entre otros servicios publicitados por el actor de amenazas en un canal dedicado de Telegram se encuentran herramientas de llamadas de voz con inteligencia artificial que permiten a sus clientes generar llamadas de voz a posibles objetivos basándose en una serie de indicaciones directamente desde el kit de phishing.

Estas llamadas generalmente se hacen pasar por provenientes de un banco y les piden que proporcionen sus códigos de autenticación de dos factores (2FA), instalen aplicaciones maliciosas o realicen otras acciones arbitrarias.

El uso de este mecanismo simple pero efectivo mejora aún más el escenario de estafa para sus víctimas y demuestra con qué rapidez y facilidad los delincuentes adoptan e implementan herramientas de IA en sus esquemas, transformando los escenarios de fraude tradicionales en tácticas nuevas y más sofisticadas, señalaron los investigadores.

En un informe reciente, Mandiant, propiedad de Google, reveló cómo la clonación de voz impulsada por IA tiene la capacidad de imitar el habla humana con una "precisión asombrosa", lo que permite esquemas de phishing (o vishing) que suenan más auténticos y facilitan el acceso inicial, la escalada de privilegios y el movimiento lateral.

Los actores de amenazas pueden hacerse pasar por ejecutivos, colegas o incluso personal de soporte de TI para engañar a las víctimas para que revelen información confidencial, otorguen acceso remoto a los sistemas o transfieran fondos", dijo la firma de inteligencia de amenazas.

La confianza inherente asociada con una voz familiar puede ser explotada para manipular a las víctimas para que realicen acciones que normalmente no realizarían, como hacer clic en enlaces maliciosos, descargar malware o divulgar datos confidenciales.

Los kits de phishing, que también vienen con capacidades de adversario en el medio (AiTM), se han vuelto cada vez más populares a medida que reducen la barrera técnica de entrada para realizar campañas de phishing a gran escala.

EXPLOIT "EVILVIDEO" EN TELEGRAM: UNA AMENAZA DE SEGURIDAD CRÍTICA

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Malware	Telegram	Alta

En un descubrimiento reciente, investigadores de ciberseguridad han identificado una vulnerabilidad crítica en la aplicación de mensajería Telegram para Android, denominada "EvilVideo". Este exploit permitía a los atacantes enviar archivos APK maliciosos disfrazados de videos, comprometiendo potencialmente millones de dispositivos en todo el mundo.

El exploit "EvilVideo" se basa en la capacidad de los atacantes para manipular los metadatos y el encabezado de un archivo APK para que parezca un video legítimo, como un archivo MP4. Aquí está el proceso en detalle:

- Elaboración del APK Malicioso: Los atacantes modificaban el encabezado y los metadatos del archivo APK para imitar los de un archivo de video. Este archivo APK malicioso contenía cargas útiles que podían ir desde software espía hasta ransomware.
- Disfrazar la Carga Maliciosa: Los atacantes manipulaban los metadatos del archivo para garantizar que Telegram no lo marcara como sospechoso. El archivo se nombraba de manera engañosa, por ejemplo, "video_vacaciones.mp4".
- Entrega a través de Telegram: El archivo APK disfrazado se enviaba al objetivo mediante Telegram. La aplicación aceptaba y presentaba el archivo como un video, lo que engañaba al usuario.

Activación del Exploit: Cuando el usuario intentaba reproducir el "video", Telegram mostraba un mensaje de error indicando que el video no se podía reproducir y solicitaba abrir el archivo con una aplicación externa. Si el usuario aceptaba, el sistema operativo Android procesaba y ejecutaba el archivo como un APK, instalando así la carga maliciosa en el dispositivo.

Acciones Post-Explotación: Una vez instalado, el APK malicioso podía realizar diversas actividades dañinas, como la exfiltración de datos personales, cifrado de archivos o creación de puertas traseras para futuras explotaciones.

Telegram ha parcheado esta vulnerabilidad implementando procesos de validación de archivos más estrictos. Sin embargo, los usuarios deben adoptar mejores prácticas de seguridad:

- Mantener las Aplicaciones Actualizadas: Siempre asegúrese de tener la última versión de las aplicaciones para beneficiarse de parches de seguridad.
- Cautela con Archivos Desconocidos: Evite abrir archivos de fuentes desconocidas o no confiables, especialmente aquellos que solicitan la ejecución de aplicaciones externas.
- Uso de Software de Seguridad: Utilice aplicaciones de seguridad robustas para detectar y bloquear APK maliciosos, incluso cuando están disfrazados de archivos multimedia.

El exploit "EvilVideo" destaca la sofisticación y el ingenio de los atacantes cibernéticos en su búsqueda para comprometer dispositivos móviles. Aunque Telegram ha corregido esta vulnerabilidad, es crucial que los usuarios permanezcan vigilantes y adopten medidas de seguridad proactivas para proteger sus dispositivos y datos personales.

OPERACIÓN DE DESINFECCIÓN DE PLUGX POR AUTORIDADES FRANCESAS

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Troyano	Usuarios	Alta

En un esfuerzo significativo para combatir el cibercrimen, las autoridades judiciales francesas, en colaboración con Europol y la empresa de ciberseguridad Sekoia, han lanzado una operación de gran envergadura para eliminar el malware PlugX de los sistemas infectados. Esta operación, iniciada el 18 de julio de 2024, se proyecta que se extienda durante varios meses, beneficiando a alrededor de cien víctimas en Francia, Malta y Portugal.

PlugX es un troyano de acceso remoto (RAT) altamente peligroso que ha sido utilizado por actores de amenazas cibernéticas desde 2008, especialmente aquellos vinculados a China. Este malware se propaga a través de técnicas de carga lateral de DLL, lo que permite a los atacantes ejecutar comandos arbitrarios en los sistemas infectados, robar datos sensibles y esparcir el malware a otros dispositivos mediante unidades USB infectadas.

Una de las características más inquietantes de PlugX es su capacidad para permanecer oculto en el sistema durante largos períodos, lo que lo convierte en una herramienta preferida para el espionaje y el robo de información a largo plazo. Su persistencia y capacidad para eludir las detecciones tradicionales de malware han hecho que sea una amenaza constante para organizaciones y individuos por igual.

La operación fue facilitada por Sekoia, una firma de ciberseguridad francesa que previamente había sinkholeado un servidor de comando y control de PlugX en 2023. Utilizando la inteligencia recolectada y una solución de eliminación desarrollada específicamente, Sekoia ha trabajado estrechamente con Europol y las fuerzas del orden de varios países para implementar esta solución en los sistemas afectados.

Este esfuerzo coordinado no solo busca eliminar el malware PlugX de los sistemas infectados, sino también reforzar la seguridad cibernética de las infraestructuras críticas en los países afectados. La operación incluye identificar las máquinas comprometidas, notificar a los propietarios y proporcionar herramientas y soporte para la eliminación segura del malware.

Uno de los mayores desafíos de la operación ha sido el marco legal que rodea la intervención en los sistemas infectados. A pesar de estas dificultades, la colaboración entre agencias como la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) en Francia, Europol y otros organismos internacionales ha sido fundamental para superar estos obstáculos y avanzar con la operación.

La operación subraya la importancia de la cooperación internacional en la lucha contra el cibercrimen. Las amenazas cibernéticas no respetan las fronteras nacionales, y la colaboración entre países y organizaciones es esencial para mitigar estos riesgos de manera efectiva.

El impacto de esta operación es significativo, no solo en términos de la eliminación de PlugX, sino también como un precedente para futuras acciones coordinadas contra el cibercrimen. La capacidad de las autoridades para responder de manera rápida y eficaz a las amenazas cibernéticas es crucial en un mundo cada vez más digitalizado.

Esta operación también destaca la importancia de la conciencia y la educación en ciberseguridad. Los usuarios deben estar atentos a las amenazas y seguir las mejores prácticas de seguridad, como mantener sus sistemas actualizados y ser cautelosos al interactuar con archivos y enlaces desconocidos.

En conclusión, la operación para eliminar PlugX es un ejemplo destacado de cómo la cooperación internacional y la acción proactiva pueden combatir eficazmente las amenazas cibernéticas. Mientras el cibercrimen continúa evolucionando, este tipo de esfuerzos conjuntos serán esenciales para proteger la seguridad y la privacidad de los usuarios en todo el mundo.

MÚLTIPLES VULNERABILIDADES EN MICOLLAB DE MITEL: UN RIESGO CRÍTICO

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Vulnerabilidad	CVE-2024-41714	MICOLLAB	Media

El Instituto Nacional de Ciberseguridad (INCIBE) ha emitido una alerta sobre varias vulnerabilidades críticas en MiCollab, una solución de colaboración y comunicación unificada desarrollada por Mitel. Estas vulnerabilidades podrían permitir a los atacantes ejecutar código arbitrario, acceder a información confidencial y comprometer la integridad del sistema afectado.

Las vulnerabilidades identificadas afectan diferentes componentes de MiCollab y se han catalogado con los siguientes CVE (Common Vulnerabilities and Exposures):

- CVE-2024-41714: Vulnerabilidad en el módulo de autenticación que permite la omisión de autenticación, permitiendo a un atacante acceder al sistema sin credenciales válidas.
- CVE-2024-35287: Fallo en la validación de entrada en el módulo de gestión de archivos, lo que puede ser explotado para ejecutar comandos arbitrarios en el sistema.

- CVE-2024-41712: Exposición de información sensible a través de un endpoint no seguro, permitiendo a los atacantes acceder a datos confidenciales almacenados en el servidor.

La explotación de estas vulnerabilidades puede tener consecuencias graves para las organizaciones que utilizan MiCollab. Los atacantes pueden:

- Ejecutar código malicioso: Tomar control del servidor afectado y desplegar malware o ransomware.
- Acceder a información confidencial: Obtener datos sensibles como credenciales de usuario, comunicaciones internas y documentos confidenciales.
- Interrumpir operaciones: Causar interrupciones en los servicios de comunicación y colaboración, impactando negativamente en la productividad de la empresa.

INCIBE ha recomendado a todas las organizaciones que utilicen MiCollab tomar medidas inmediatas para mitigar los riesgos asociados con estas vulnerabilidades. Entre las acciones sugeridas se incluyen:

- Actualizar el software: Instalar las últimas actualizaciones y parches proporcionados por Mitel para cerrar las vulnerabilidades identificadas.
- Revisar configuraciones de seguridad: Asegurarse de que las configuraciones del sistema sigan las mejores prácticas de seguridad, limitando el acceso no autorizado y protegiendo los datos sensibles.
- Monitorear la actividad del sistema: Implementar sistemas de detección y respuesta ante intrusiones (IDR) para monitorear cualquier actividad sospechosa en el sistema.

Las vulnerabilidades en MiCollab de Mitel representan un riesgo significativo para las organizaciones que dependen de esta herramienta para sus comunicaciones y colaboración. La acción proactiva y la aplicación de las actualizaciones de seguridad son esenciales para proteger los sistemas y datos contra posibles ataques. Para obtener más detalles y actualizaciones, se recomienda consultar el sitio web del INCIBE y los comunicados oficiales de Mitel

.

> SERVICIOS VERNE PARA PYMES

¿TE GUSTARÍA AMPLIAR INFORMACIÓN O RECIBIR ASESORAMIENTO DE UN ESPECIALISTA?

www.vernegroup.com

CONTACTA