Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VELOCIRAPTOR BAJO ATAQUE: USO MALICIOSO DE UNA HERRAMIENTA FORENSE EN NUEVAS CAMPAÑAS CIBERNÉTICAS

02/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

El ecosistema de ciberseguridad empresarial enfrenta un nuevo desafío: la manipulación de herramientas legítimas de análisis forense y monitoreo con fines maliciosos. Investigaciones recientes revelaron que actores de amenazas han abusado de Velociraptor, una solución diseñada para la respuesta a incidentes, para instalar y ejecutar otros programas que facilitan el acceso remoto y la creación de túneles hacia servidores de comando y control. Este hallazgo confirma una tendencia en crecimiento donde los atacantes prefieren “vivir de la tierra” (LotL), utilizando software confiable para camuflar su actividad y reducir las probabilidades de detección.

Paralelamente, se han identificado campañas que explotan la confianza en herramientas corporativas ampliamente adoptadas como Microsoft Teams y la infraestructura de Active Directory Federation Services (ADFS). Estas técnicas, que incluyen suplantación de soporte técnico, instalación de software de control remoto y redirecciones a páginas falsas de Microsoft 365, reflejan un cambio en el panorama de amenazas: los cibercriminales ya no dependen únicamente de malware tradicional, sino que integran de manera creativa servicios empresariales legítimos para alcanzar sus objetivos.

VELOCIRAPTOR BAJO ATAQUE: USO MALICIOSO DE UNA HERRAMIENTA FORENSE EN NUEVAS CAMPAÑAS CIBERNÉTICAS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_02_3
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	02/09/2025
Es día cero (0 day):	No

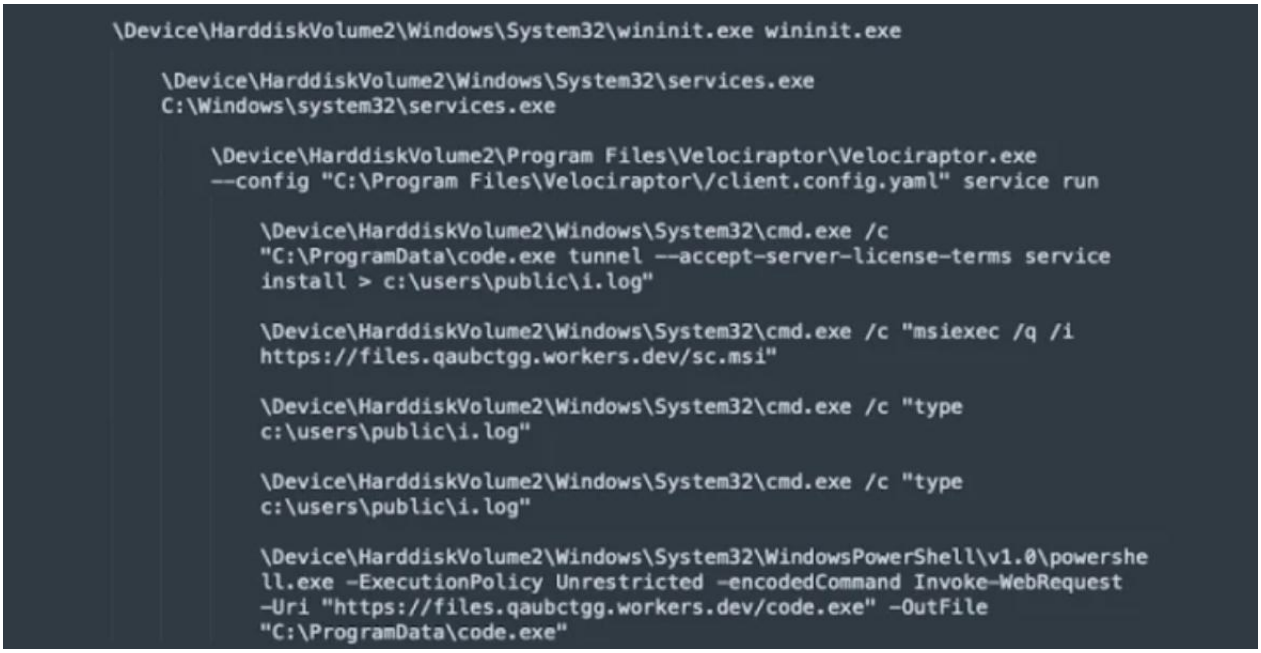
RESUMEN

Las investigaciones más recientes en ciberseguridad revelan un patrón preocupante: los atacantes están aprovechando herramientas legítimas de administración y monitoreo para evadir controles de seguridad, al mismo tiempo que perfeccionan técnicas de ingeniería social en plataformas corporativas como Microsoft Teams. A continuación, se presentan tres hallazgos clave que todo equipo de TI y ciberseguridad en la empresa debe conocer.

Velociraptor convertido en arma para acceso remoto

Se detectaron que actores maliciosos usaron el software Velociraptor, originalmente diseñado para análisis forense y respuesta a incidentes, como vector de ataque.

- El ataque inicia con msiexec de Windows para descargar un instalador MSI desde un dominio en Cloudflare Workers.
- Una vez instalado, Velociraptor contacta otro dominio malicioso y descarga Visual Studio Code con funciones de túnel activadas, lo que habilita acceso remoto y ejecución de código.
- Posteriormente, los atacantes despliegan herramientas adicionales como Cloudflare Tunnel y Radmin.



Recomendación: Monitorear uso no autorizado de Velociraptor y cualquier comportamiento inusual asociado a instalación de herramientas administrativas. Este tipo de hallazgo debe considerarse precursor de ataques de ransomware.

Microsoft Teams bajo ataque: phishing disfrazado de soporte técnico

Investigadores alertaron sobre campañas activas que utilizan Microsoft Teams como canal inicial de acceso. Los atacantes:

- Crean inquilinos falsos o comprometen cuentas legítimas.
- Envían mensajes directos o realizan llamadas suplantando al área de mesa de ayuda/soporte IT.
- Convencen a los usuarios de instalar software de control remoto como AnyDesk o DWAgent, y desde ahí despliegan cargas útiles en PowerShell para robar credenciales y mantener persistencia.

Este enfoque explota la confianza en las herramientas colaborativas internas y evita controles tradicionales como los filtros de correo electrónico.

Malvertising y ADFS: campañas de phishing más creíbles

Una tercera campaña descubierta utiliza enlaces legítimos de office[.]com y la integración con Active Directory Federation Services (ADFS) para redirigir a usuarios hacia páginas falsas de inicio de sesión de Microsoft 365.

El truco: los atacantes configuran su propio tenant malicioso con ADFS, logrando que el propio Microsoft redireccione al dominio controlado por ellos. Aunque no se trata de una vulnerabilidad, esta técnica hace que la detección basada en URL sea mucho más difícil.

Medidas de protección recomendadas

1. Implementar EDR/antivirus avanzado con reglas para detectar instalación no autorizada de software como Velociraptor o VS Code en contextos inusuales.
2. Revisar periódicamente los logs de Teams (ej. ChatCreated, MessageSent) para identificar actividades sospechosas.
3. Fortalecer la concientización de usuarios sobre tácticas de suplantación de soporte IT.
4. Establecer listas blancas de aplicaciones autorizadas para bloquear instalaciones no aprobadas.
5. Monitorear y validar los dominios de autenticación asociados a ADFS y Microsoft 365.
6. Realizar copias de seguridad regulares y pruebas de restauración.
7. Mantener planes de respuesta a incidentes actualizados para escenarios de ransomware y phishing.

Conclusión

El abuso de herramientas de confianza como Velociraptor, el phishing mediante Microsoft Teams y el uso creativo de ADFS en campañas de malvertising confirman que los atacantes están apostando por estrategias de bajo perfil y alta credibilidad. La defensa empresarial requiere no solo tecnología, sino también procesos de monitoreo continuo y capacitación para enfrentar esta nueva ola de amenazas.

NOTICIA COMPLETA

https://devel.group/blog/velociraptor-bajo-ataque-uso-malicioso-de-una-herramienta-forense-en-nuevas-campanas-ciberneticas/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/