Los actores maliciosos están utilizando las notificaciones del navegador como un nuevo vector de ataques de phishing para distribuir enlaces dañinos mediante una plataforma de comando y control (C2) llamada Matrix Push C2.

"Este framework nativo del navegador y sin archivos aprovecha notificaciones push, alertas falsas y redirecciones de enlaces para atacar víctimas en distintos sistemas operativos", señaló la investigadora de BlackFog, Brenda Robb, en un informe publicado el jueves.

En este tipo de ataques, las víctimas potenciales son manipuladas mediante técnicas de ingeniería social para que permitan las notificaciones del navegador, ya sea en sitios web maliciosos o en portales legítimos que han sido vulnerados.

Una vez que el usuario acepta recibir notificaciones, los atacantes explotan el mecanismo de notificaciones push integrado en el navegador para enviar alertas que aparentan provenir del sistema operativo o del propio navegador, usando marcas confiables, logotipos familiares y lenguaje convincente para mantener el engaño.

Entre estos mensajes pueden incluirse advertencias sobre supuestos inicios de sesión sospechosos o actualizaciones del navegador, acompañados de botones como "Verificar" o "Actualizar", que al ser pulsados conducen a la víctima a un sitio falso.

Lo que hace que esta técnica sea especialmente ingeniosa es que todo el ataque se ejecuta directamente desde el navegador, sin necesidad de comprometer previamente el sistema mediante otros métodos. De cierta forma, resulta comparable a ClickFix, ya que los usuarios son inducidos a seguir pasos que terminan comprometiendo su propio dispositivo, evadiendo así los controles de seguridad tradicionales.

Eso no es todo. Dado que el ataque opera desde el navegador, también se convierte en una amenaza multiplataforma. Esto significa que cualquier aplicación de navegador en cualquier sistema operativo que acepte las notificaciones maliciosas puede pasar a formar parte del conjunto de clientes, otorgando a los atacantes un canal persistente de comunicación.

Matrix Push C2 se comercializa como un kit de malware como servicio (MaaS) dirigido a otros actores de amenazas. Se vende directamente en canales de *crimeware*, usualmente a través de Telegram y foros de ciberdelincuencia, siguiendo un modelo de suscripción escalonado: alrededor de $150 por un mes, $405 por tres meses, $765 por seis meses y $1,500 por un año completo.

"Los pagos se realizan en criptomonedas, y los compradores se comunican directamente con el operador para obtener acceso", explicó el Dr. Darren Williams, fundador y CEO de BlackFog. *"Matrix Push se detectó por primera vez a inicios de octubre y ha estado activo desde entonces. No hay evidencia de versiones previas, marcas anteriores o infraestructura antigua. Todo indica que se trata de un kit recién lanzado"*.

La herramienta se presenta como un panel de control basado en la web, permitiendo a los usuarios enviar notificaciones, monitorear en tiempo real a cada víctima, identificar con cuáles alertas interactúan, generar enlaces cortos mediante un acortador integrado e incluso registrar las extensiones instaladas en el navegador, incluyendo monederos de criptomonedas.

"El núcleo del ataque es la ingeniería social, y Matrix Push C2 incluye plantillas configurables para maximizar la credibilidad de sus mensajes falsos", detalló Robb. *"Los atacantes pueden adaptar fácilmente sus notificaciones y páginas de destino para hacerse pasar por compañías y servicios ampliamente reconocidos"*.

Algunas de las plantillas disponibles para verificaciones falsas están asociadas con marcas muy conocidas como MetaMask, Netflix, Cloudflare, PayPal y TikTok. La plataforma también incorpora una sección de *"Analytics & Reports"*, que permite a los clientes evaluar la eficacia de sus campañas y ajustarlas según sea necesario.

"Matrix Push C2 nos muestra un cambio en la forma en que los atacantes obtienen acceso inicial e intentan explotar a los usuarios", señaló BlackFog. *"Una vez que el endpoint del usuario (computadora o dispositivo móvil) se encuentra bajo este tipo de influencia, el atacante puede escalar progresivamente el ataque"*.

"Podrían enviar más mensajes de phishing para robar credenciales, engañar al usuario para instalar un malware más persistente o incluso aprovechar vulnerabilidades del navegador para obtener mayor control del sistema. En última instancia, el objetivo suele ser robar datos o monetizar el acceso, por ejemplo drenando monederos de criptomonedas o exfiltrando información personal".

Aumento de ataques que abusan de Velociraptor

Este desarrollo coincide con la observación de Huntress, que reportó un *"aumento significativo"* en ataques que aprovechan Velociraptor, una herramienta legítima de análisis forense digital y respuesta a incidentes (DFIR), durante los últimos tres meses.

El 12 de noviembre de 2025, la compañía de ciberseguridad informó que actores de amenazas habían desplegado Velociraptor tras obtener acceso inicial mediante la explotación de una vulnerabilidad en Windows Server Update Services (CVE-2025-59287, puntuación CVSS: 9.8), corregida por Microsoft a finales del mes pasado.

Posteriormente, los atacantes habrían ejecutado consultas de descubrimiento con el propósito de realizar reconocimiento y obtener información sobre usuarios, servicios en ejecución y configuraciones. Huntress señaló que el ataque fue contenido antes de que pudiera avanzar más.

Este hallazgo demuestra que los actores de amenazas no solo emplean frameworks C2 personalizados, sino que también aprovechan herramientas legítimas de ciberseguridad ofensiva y respuesta a incidentes.

"Hemos visto a actores de amenazas utilizar herramientas legítimas durante suficiente tiempo para saber que Velociraptor no será la primera herramienta de doble uso y de código abierto que aparecerá en ataques — ni será la última", concluyeron los investigadores de Huntress.