Un repositorio de GitHub, que ha sido retirado y que ofrecía una herramienta de WordPress diseñada para publicar contenido en este sistema de gestión de contenidos (CMS), se estima que permitió el robo de más de 390,000 credenciales.

Este comportamiento malicioso es parte de una campaña de ataque más amplia realizada por un actor de amenazas identificado como MUT-1244 (siglas de «*misteriosa amenaza no atribuida*«) por Datadog Security Labs. La campaña incluye ataques de phishing y varios repositorios de GitHub modificados maliciosamente que contienen código de prueba de concepto (PoC) diseñado para explotar vulnerabilidades de seguridad conocidas.

> *«Las víctimas incluyen actores ofensivos, como pentesters e investigadores de seguridad, así como otros actores maliciosos. Entre los datos sensibles comprometidos se encuentran claves privadas SSH y credenciales de acceso a AWS,»* explicaron los investigadores Christophe Tafani-Dereeper, Matt Muir y Adrian Korn en un informe.

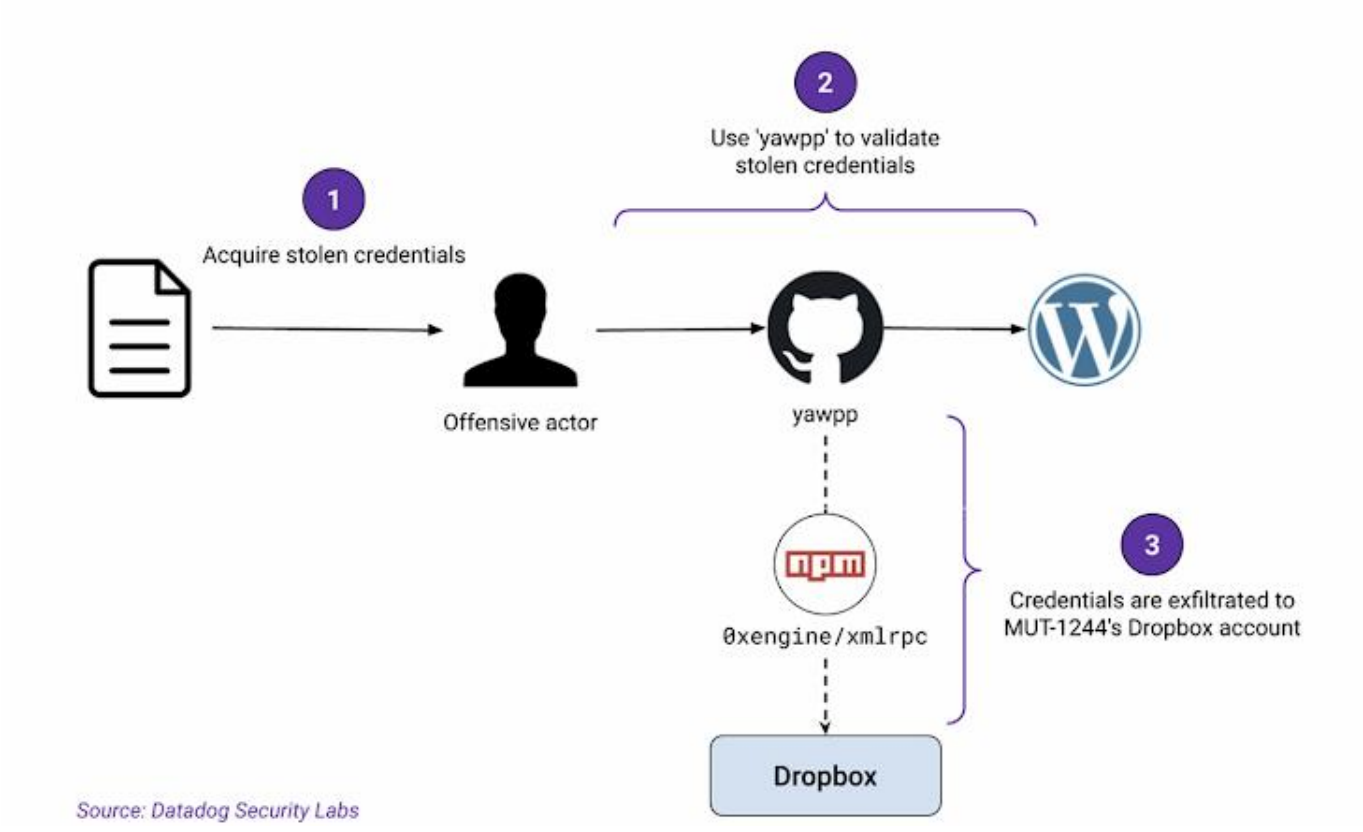
No resulta sorprendente que los investigadores de seguridad sean un objetivo atractivo para los cibercriminales, incluidos los grupos de amenazas respaldados por estados como Corea del Norte. Comprometer sus sistemas puede proporcionar información valiosa sobre posibles vulnerabilidades no divulgadas que podrían ser utilizadas para ejecutar ataques más avanzados.

En los últimos años, ha surgido un patrón en el que los atacantes explotan las revelaciones de vulnerabilidades creando perfiles falsos en GitHub que alojan PoCs aparentemente legítimos. Sin embargo, estos repositorios están diseñados para robar información o incluso extorsionar a cambio de acceso a los exploits.

Las campañas de MUT-1244 incluyen tanto repositorios de GitHub troyanizados como correos electrónicos de phishing. Estos son utilizados para entregar malware de segunda etapa que puede instalar un minero de criptomonedas y robar información del sistema, claves SSH privadas, variables de entorno, y datos en carpetas específicas (por ejemplo, ~/.aws),

transfiriéndolos a File.io.

Un ejemplo de estos repositorios era *«github[.]com/hpc20235/yawpp,»* que se promocionaba como *«Yet Another WordPress Poster»* (Otro Publicador de WordPress). Antes de ser eliminado por GitHub, este proyecto contenía dos scripts: uno para verificar credenciales de WordPress y otro para generar publicaciones a través de la API XML-RPC.



Sin embargo, esta herramienta también contenía un código malicioso en forma de una dependencia npm comprometida, un paquete llamado @0xengine/xmlrpc, que distribuía el mismo malware. Este paquete fue publicado en npm en octubre de 2023 como una implementación de servidor y cliente XML-RPC basada en JavaScript para Node.js. Actualmente, ya no está disponible para descargar.

Cabe destacar que la empresa de ciberseguridad Checkmarx informó recientemente que este paquete npm estuvo activo por más de un año y acumuló alrededor de 1,790 descargas.

Se estima que el proyecto de GitHub yawpp facilitó la exfiltración de más de 390,000 credenciales, probablemente asociadas a cuentas de WordPress, hacia una cuenta de Dropbox controlada por los atacantes. Esto se logró comprometiendo a otros actores maliciosos que tenían acceso ilícito a estas credenciales.

Otro vector de ataque identificado consiste en correos electrónicos de phishing dirigidos a académicos. Estos correos los engañan para que visiten enlaces que los instruyen a ejecutar comandos en el terminal bajo el pretexto de actualizar el kernel. Este hallazgo representa el primer caso documentado de un ataque estilo ClickFix contra sistemas Linux.

> *«El segundo método de acceso inicial que emplea MUT-1244 es un grupo de usuarios malintencionados en GitHub que publican pruebas de concepto falsas para vulnerabilidades CVE. La mayoría de estas cuentas fueron creadas en octubre o noviembre de 2024, no tienen actividad legítima y utilizan imágenes de perfil generadas por inteligencia artificial»,* señalaron los investigadores.

Algunos de estos repositorios falsos de PoC (Prueba de Concepto) fueron destacados previamente por Alex Kaganovich, jefe global del equipo rojo de seguridad ofensiva de Colgate-Palmolive, a mediados de octubre de 2024. Pero, en un giro interesante, el malware de segunda etapa se introduce a través de cuatro métodos diferentes:

- Archivo de compilación de configuración con puerta trasera.
- Carga maliciosa incrustada en un archivo PDF.
- Uso de un *dropper* en Python.
- Inclusión de un paquete malicioso de npm llamado «0xengine/meow».

> *«El grupo MUT-1244 logró comprometer los sistemas de docenas de víctimas,*

> *principalmente integrantes de equipos rojos, investigadores de seguridad y cualquier persona interesada en descargar código de explotación de PoC. Esto permitió a MUT-1244 acceder a información sensible, incluidas claves privadas de SSH, credenciales de AWS e historiales de comandos»,* dijeron los investigadores.