Investigadores en ciberseguridad han identificado una nueva puerta trasera basada en PHP denominada *Glutton*, que ha sido empleada en ataques cibernéticos dirigidos a países como China, Estados Unidos, Camboya, Pakistán y Sudáfrica.

QiAnXin XLab, que detectó esta actividad maliciosa a finales de abril de 2024, atribuyó con moderada confianza este malware inédito al grupo chino de amenazas persistentes avanzadas conocido como *Winnti* (también llamado APT41).

> *«Es interesante notar que nuestra investigación mostró que los creadores de Glutton se enfocaron intencionalmente en sistemas dentro del mercado del cibercrimen. Al sabotear estas operaciones, buscaban utilizar las herramientas de los propios ciberdelincuentes en su contra, en un típico caso de 'no hay honor entre ladrones'»*, declaró la compañía.

El malware *Glutton* está diseñado para recolectar información confidencial del sistema, desplegar un componente de puerta trasera basado en ELF y realizar inyecciones de código en marcos populares de PHP como Baota (BT), ThinkPHP, Yii y Laravel. El código ELF también muestra una *«similitud casi total»* con una herramienta ya conocida de *Winnti*, llamada *PWNLNX*.

Aunque se han encontrado vínculos con *Winnti*, los investigadores de XLab señalaron que no pueden establecer una conexión definitiva entre esta puerta trasera y el grupo debido a la ausencia de técnicas de camuflaje comúnmente asociadas con ellos. Según la compañía, estas deficiencias resultan *«atípicamente inferiores al nivel habitual».*

Entre estas carencias se incluyen la ausencia de comunicaciones cifradas para el comando y control (C2), el uso de HTTP en lugar de HTTPS para la descarga de cargas maliciosas y la falta de cualquier tipo de ofuscación en las muestras analizadas.

En su núcleo, *Glutton* es un marco de malware modular que puede infectar archivos PHP en los dispositivos objetivo y desplegar puertas traseras. Se cree que los atacantes logran el

acceso inicial explotando vulnerabilidades *zero-day* y *N-day*, además de realizar ataques de fuerza bruta.

Un método adicional y poco convencional empleado por los atacantes consiste en anunciar en foros de cibercrimen sistemas empresariales comprometidos que contienen *l0ader_shell*, una puerta trasera inyectada en archivos PHP, lo que permite lanzar ataques contra otros actores maliciosos.

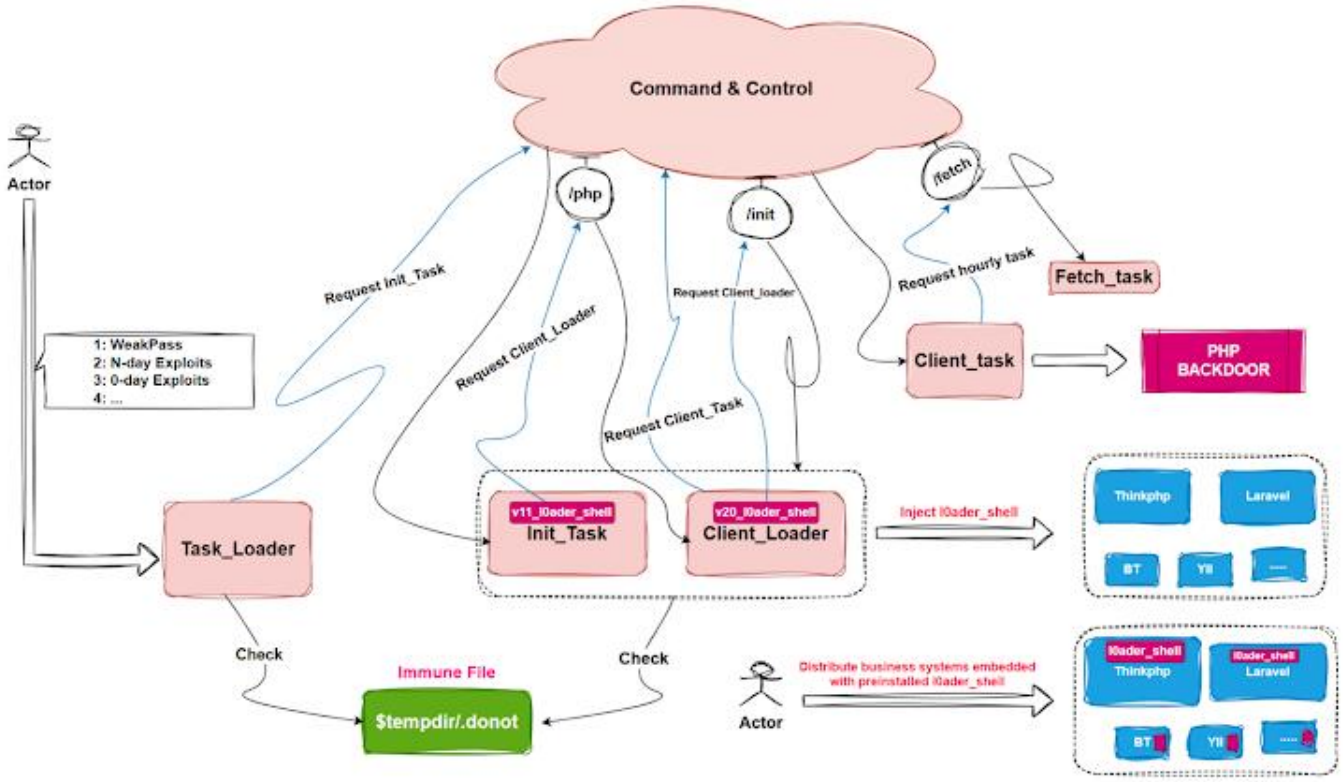
El módulo clave que facilita los ataques es *task_loader*, encargado de analizar el entorno de ejecución y descargar componentes adicionales, como *init_task*. Este último se ocupa de descargar una puerta trasera basada en ELF que se hace pasar por el Administrador de Procesos FastCGI («/lib/php-fpm»), infectar archivos PHP con código malicioso para ejecutar nuevas cargas útiles, recolectar información sensible y modificar archivos del sistema.

La cadena de ataque también incluye un módulo llamado *client_loader*, una versión mejorada de *init_task*, que emplea una infraestructura de red actualizada y añade la capacidad de descargar y ejecutar un cliente comprometido. Además, modifica archivos del sistema como «/etc/init.d/network» para asegurar la persistencia del ataque.

La puerta trasera PHP es una herramienta avanzada que incluye 22 comandos diferentes. Entre sus capacidades se encuentran cambiar entre conexiones C2 mediante TCP y UDP, abrir una shell, transferir archivos (descargar o subir), realizar tareas de manejo de archivos y directorios, y ejecutar código PHP personalizado. Además, este sistema permite descargar y ejecutar nuevas cargas útiles de PHP al consultar periódicamente el servidor de comando y control (C2).

> *«Estas cargas son extremadamente modulares, capaces de operar por separado o de ejecutarse en serie a través del task_loader para formar un completo marco de ataque. Toda la ejecución ocurre dentro de procesos PHP o PHP-FPM (FastCGI), lo que asegura que no queden rastros de archivos en el sistema, logrando así un perfil de sigilo»,* señaló XLab.

Un detalle relevante es el uso de la herramienta HackBrowserData en los sistemas de operadores de ciberdelincuencia para extraer información sensible, posiblemente con la intención de emplearla en campañas futuras de phishing o ingeniería social.



> *«Además de atacar a las víctimas habituales del ámbito 'whitehat' mediante actividades criminales, Glutton muestra un enfoque estratégico al aprovechar recursos de los mismos operadores de ciberdelincuencia. Esto genera una cadena de ataques recursiva, utilizando las actividades de los atacantes en su contra»*, explicó XLab.

Este informe fue publicado pocas semanas después de que XLab revelara una versión actualizada del malware APT41, llamado *Mélofée*, que incluye mecanismos avanzados de

persistencia y *«un controlador de kernel cifrado con RC4 para ocultar rastros de archivos, procesos y conexiones de red».*

Una vez desplegado, el backdoor para Linux puede comunicarse con un servidor C2 para recibir y ejecutar múltiples comandos. Estas acciones incluyen recopilar información del sistema y procesos, iniciar una shell, gestionar procesos, realizar operaciones con archivos y directorios, e incluso desinstalarse.

> *«Mélofée presenta una funcionalidad sencilla combinada con capacidades de ocultación altamente efectivas. Las muestras de este malware son escasas, lo que sugiere que los atacantes lo reservan para objetivos de alto valor»,* agregó XLab.