Los expertos en ciberseguridad han emitido una alerta sobre una nueva operación maliciosa que utiliza inyecciones web para propagar un nuevo tipo de malware dirigido a macOS, denominado FrigidStealer.

Esta actividad ha sido vinculada a un actor de amenazas previamente desconocido, identificado como TA2727, quien también emplea ladrones de información en otras plataformas, como Windows (Lumma Stealer o DeerStealer) y Android (Marcher).

Según el equipo de investigación de amenazas de Proofpoint, TA2727 es un *«grupo malicioso que emplea falsas actualizaciones como señuelo para distribuir diversas cargas de malware».*

Se trata de una de las recientes agrupaciones de actividades maliciosas identificadas, junto con TA2726, un operador de un sistema de distribución de tráfico (*Traffic Distribution System* o TDS), utilizado para canalizar tráfico malicioso hacia otros actores con el fin de diseminar software malicioso. Se estima que este actor, motivado por beneficios financieros, ha estado activo al menos desde septiembre de 2022.

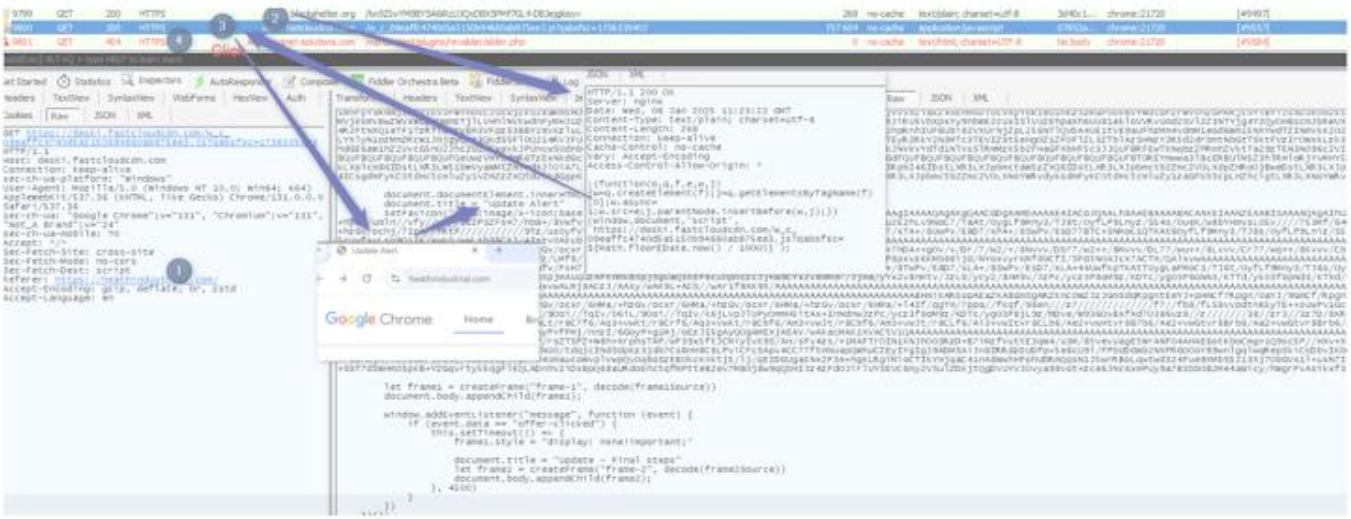
Según una empresa de seguridad, TA2726 opera como un TDS en favor de TA2727 y otro grupo denominado TA569, responsable de distribuir un *loader* basado en JavaScript conocido como SocGholish (*FakeUpdates*), el cual suele disfrazarse como una actualización de navegador en sitios legítimos que han sido vulnerados.

> *«TA2726 tiene intereses económicos y colabora con otros actores con la misma motivación, como TA569 y TA2727. Esto sugiere que probablemente sea el responsable de comprometer servidores y páginas web, permitiendo a otros actores insertar código malicioso»,* explicó la compañía.

TA569 y TA2727 comparten la estrategia de explotar sitios web infectados con JavaScript malicioso que finge ser una actualización de navegadores como Google Chrome o Microsoft Edge. No obstante, TA2727 se distingue por su capacidad para personalizar sus ataques en función de la ubicación del usuario o el tipo de dispositivo que emplea.

Si una persona accede a un sitio contaminado desde Francia o el Reino Unido utilizando Windows, se le solicitará descargar un instalador MSI que ejecuta Hijack Loader (*DOILoader*), el cual posteriormente carga Lumma Stealer.

En contraste, si el acceso proviene de un dispositivo Android, la redirección conduce a la instalación de un troyano bancario llamado Marcher, el cual ha estado activo por más de diez años.



Pero hay más. Desde enero de 2025, esta campaña ha evolucionado para incluir a usuarios de macOS fuera de América del Norte. Ahora, se les redirige a una página de actualización fraudulenta que descarga un nuevo ladrón de información llamado FrigidStealer.

El instalador de FrigidStealer, al igual que otras amenazas dirigidas a macOS, requiere que el usuario inicie manualmente una aplicación no firmada para eludir el sistema de seguridad Gatekeeper. Una vez ejecutado, el malware instala un archivo Mach-O incrustado.

> *«El archivo ejecutable fue desarrollado en Go y tenía una firma ad-hoc. Se creó utilizando WailsIO, una herramienta que permite mostrar contenido en el navegador*

> *del usuario, reforzando la ilusión de que la instalación de Chrome o Safari es legítima»,* detalló Proofpoint.

FrigidStealer comparte similitudes con otras familias de *stealers* dirigidos a macOS. Emplea AppleScript para solicitar la contraseña del sistema al usuario, lo que le otorga permisos elevados y le permite extraer archivos y datos sensibles desde navegadores web, Apple Notes y aplicaciones relacionadas con criptomonedas.

> *«Los ciberdelincuentes están utilizando vulneraciones en sitios web para propagar malware tanto a empresas como a usuarios individuales. Es lógico pensar que estos ataques seguirán adaptándose a cada víctima, incluyendo usuarios de Mac, quienes siguen siendo minoría en entornos empresariales frente a Windows»,* advirtió la empresa.

Este caso coincide con una reciente investigación de Tonmoy Jitu, de Denwp Research, quien reveló los detalles de un nuevo *backdoor* para macOS denominado Tiny FUD. Este malware es completamente indetectable y utiliza técnicas como la manipulación de nombres, la inyección en el *dynamic link daemon* (DYLD) y la ejecución remota de comandos a través de servidores C2 (*command-and-control*).

Asimismo, la aparición de nuevas amenazas como Astral Stealer y Flesh Stealer ha intensificado las preocupaciones de seguridad. Ambas variantes están diseñadas para recopilar información sensible, evitar ser detectadas y asegurar su permanencia en los sistemas comprometidos.

> *«Flesh Stealer es especialmente hábil en la identificación de entornos virtualizados. Este malware evita ejecutarse en máquinas virtuales para dificultar el análisis forense, lo que demuestra un conocimiento avanzado sobre las tácticas de investigación en ciberseguridad»,* destacó Flashpoint en un informe reciente.