Una campaña de ClickFix dirigida a sistemas macOS, que abarca más de 250 dominios de acceso (*front-end*), ahora incorpora un mecanismo de identificación de visitantes antes de decidir si les mostrará o no un señuelo malicioso. Este cambio fue detectado por Microsoft Threat Intelligence mientras monitoreaba la infraestructura de la operación durante varias semanas.

Este filtro implementado del lado del servidor permite ocultar la página maliciosa frente a rastreadores automatizados y entornos *sandbox*, mostrando únicamente a determinados usuarios de macOS una supuesta descarga legítima de software. Microsoft indicó que la infraestructura completa distribuyó tanto MacSync como Atomic Stealer (AMOS); sin embargo, la cadena de ataque analizada mediante este mecanismo concluía con la ejecución de AMOS.

El ataque continúa dependiendo de la interacción del usuario, quien debe copiar y ejecutar un comando ofuscado en la aplicación Terminal. Dicho comando descarga una serie de scripts que terminan desplegando un *infostealer* capaz de sustraer credenciales, información almacenada en navegadores, repositorios de autenticación, billeteras de criptomonedas y archivos sensibles. Microsoft no reveló el número de víctimas, los sectores afectados ni la identidad de los responsables de la campaña.

Como medida preventiva, se recomienda no seguir instrucciones provenientes de sitios web, verificaciones CAPTCHA, servicios de chat o páginas de descarga que soliciten copiar y pegar comandos en Terminal.

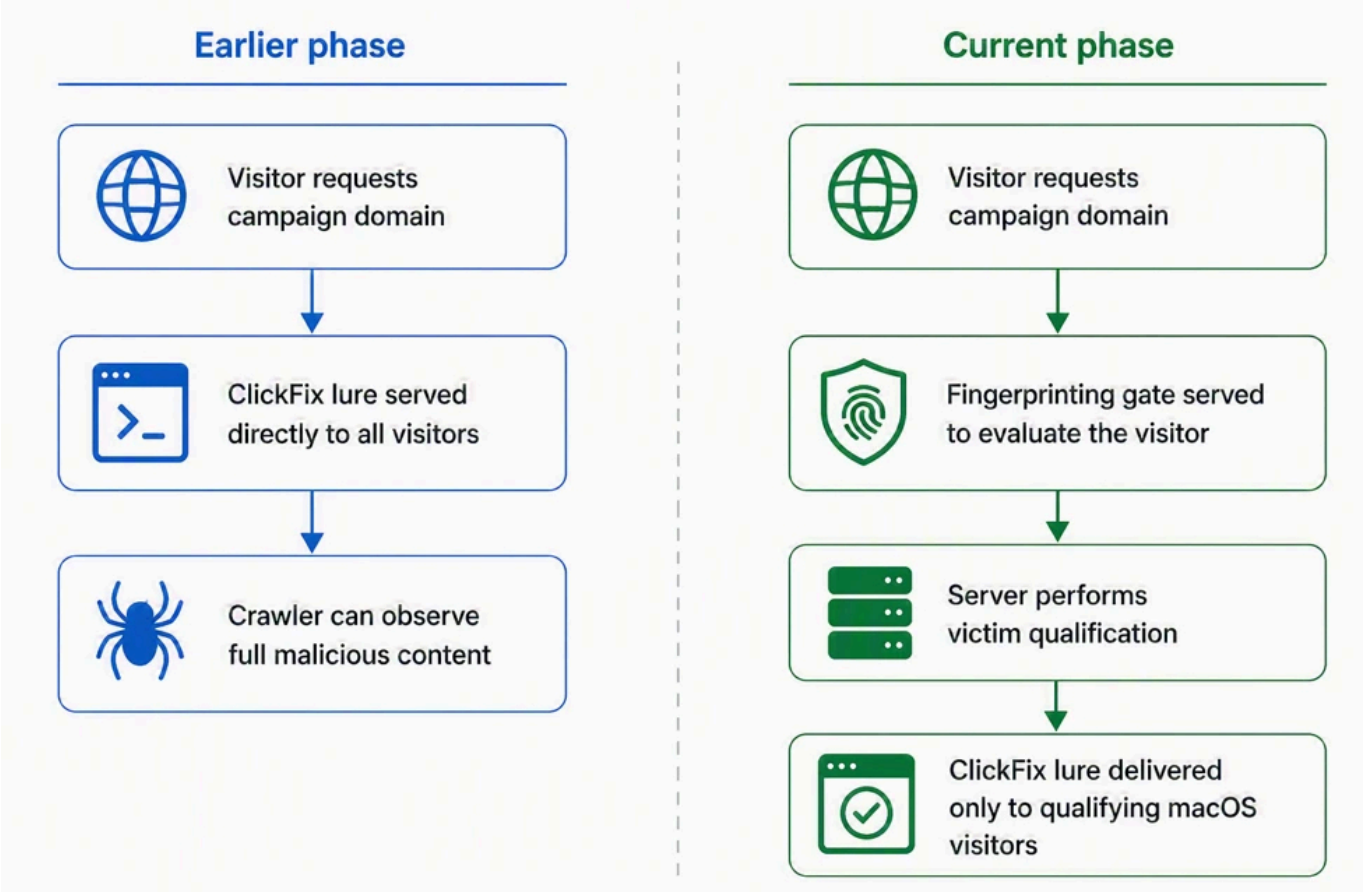
En un análisis publicado el 5 de agosto, Microsoft explicó que la infraestructura evolucionó durante el periodo de observación. Las primeras versiones de las páginas exponían directamente en el código HTML las instrucciones de ClickFix, la lógica utilizada para copiar contenido al portapapeles, el comando de *shell* ofuscado y la dirección codificada utilizada para la fase de preparación, lo que facilitaba su detección mediante herramientas de análisis estático.

El nuevo mecanismo de filtrado incorpora un script de aproximadamente 2,5 KB escrito en

JavaScript. Este recopila información del navegador mediante valores de `navigator`, incluyendo la plataforma del dispositivo —que en un equipo Mac real debería reportarse como MacIntel—, además de las dimensiones de la pantalla y de la ventana, junto con parámetros gráficos obtenidos mediante WebGL, utilizados para diferenciar hardware Apple auténtico de máquinas virtuales o entornos emulados.

Asimismo, el script verifica la zona horaria del dispositivo, comprueba si la página se encuentra embebida dentro de un iframe y determina si el sistema informa compatibilidad con pantallas táctiles, característica poco habitual en computadoras Mac de escritorio. También incorpora dos mecanismos orientados a detectar investigadores de seguridad: un contador que incrementa su valor cuando la consola de desarrollo del navegador permanece abierta y una llamada a `canPlayType("video/mp4")`, reutilizada como una técnica de detección para identificar navegadores utilizados en análisis que simulan soporte de códecs mediante JavaScript. Toda esta información se agrupa bajo la etiqueta `mode:"php"` y se envía automáticamente al servidor sin requerir interacción del usuario.

Una vez recopilada la huella digital del navegador, esta es enviada al servidor, que determina dinámicamente el contenido que recibirá cada visitante. Los rastreadores web, entornos *sandbox* o usuarios ubicados en regiones no deseadas pueden recibir una página vacía, una falsa extensión para navegador o incluso un sitio empresarial completamente ajeno. En contraste, cuando la solicitud coincide con el perfil esperado de un equipo Mac legítimo, el usuario visualiza una página inspirada en GitHub que ofrece una aparente descarga para macOS acompañada de un distintivo falso de «Verified Publisher».



Microsoft Security Research y el investigador de seguridad senior Srinivasan Govindarajan señalaron que la apariencia inofensiva de un dominio no constituye evidencia de que este sea seguro. La decisión sobre el contenido entregado se realiza del lado del servidor para cada solicitud individual, por lo que dos accesos consecutivos a la misma dirección pueden mostrar páginas completamente diferentes.

Durante el periodo de seguimiento, Microsoft confirmó la existencia de más de 250 dominios de acceso vinculados con la campaña. Muchos de ellos combinan la palabra «file» con términos del diccionario, como *filecopperbasket[.]sbs* y *applefilevault[.]com*. No obstante, la compañía advirtió que este patrón únicamente constituye un indicador preliminar de búsqueda, ya que la evidencia más sólida proviene de la combinación entre dominios desechables, comportamientos compartidos de la infraestructura y la presencia del

mecanismo de identificación de visitantes.

Después de que la víctima ejecuta el comando indicado, este establece comunicación con una ruta del tipo /curl/, desde donde descarga scripts adicionales antes de iniciar la ejecución de AMOS, tal como se observó en la cadena analizada por Microsoft. La empresa también confirmó que la infraestructura utilizada distribuyó MacSync, aunque no logró asociar cada dominio específico con una carga maliciosa determinada.

Como parte de las medidas defensivas, Microsoft recomienda monitorear sesiones de navegación seguidas por actividad inusual en Terminal, especialmente la ejecución de comandos `curl` redirigidos hacia zsh, procesos de decodificación Base64, el uso de osascript y la creación de archivos comprimidos seguida de solicitudes HTTP POST hacia servidores externos.

Debido a que la página maliciosa únicamente se presenta a visitantes que cumplen determinados criterios, Microsoft considera más efectivo detectar el mecanismo de filtrado que el malware en sí. Para ello, recomienda identificar formularios de huellas digitales que se envían automáticamente, campos ocultos destinados al reconocimiento del dispositivo, la presencia del artefacto `mode:"php"` y bloquear la infraestructura compartida de preparación, así como las rutas /curl/, en lugar de centrar los esfuerzos únicamente en los dominios temporales utilizados como fachada.

Por otra parte, Apple publicó macOS 26.4 el 24 de marzo de 2026 y, el 3 de agosto, detalló nuevas funciones de protección incorporadas al sistema. Entre ellas destaca un mensaje de confirmación mostrado por Terminal cuando el usuario no ha utilizado la aplicación durante más de 30 días, no dispone de herramientas habituales de desarrollo instaladas y pega contenido procedente de navegadores o aplicaciones de mensajería. Adicionalmente, XProtect ahora puede rastrear los comandos pegados en cualquier emulador de terminal, analizar el árbol de procesos generado y los artefactos de red asociados, bloqueando aquellas actividades vinculadas con malware previamente identificado.

Aunque el informe describe con detalle tanto la infraestructura empleada como el

mecanismo técnico utilizado por los atacantes, Microsoft no proporcionó información sobre la magnitud real de la campaña ni sobre la identidad de los responsables. A partir de la evidencia disponible, el nuevo mecanismo de filtrado parece estar orientado principalmente a dificultar el análisis automatizado de la infraestructura, más que a modificar la cadena de ataque. En esencia, la estrategia sigue siendo la misma: ocultar el contenido malicioso a herramientas de análisis y mostrar el señuelo únicamente a usuarios de macOS que cumplan determinados criterios, manteniendo como requisito indispensable que la víctima copie y ejecute manualmente el comando en Terminal. Negarse a realizar esta acción continúa siendo la medida de protección más eficaz.

Esta operación representa una evolución de la tendencia identificada por Microsoft en mayo, cuando las campañas dirigidas a distribuir *infostealers* para macOS comenzaron a utilizar comandos ejecutados desde Terminal para descargar scripts remotos, sustituyendo el método tradicional basado en la distribución de imágenes de disco para su instalación manual.