Se ha detectado que actores maliciosos están utilizando la táctica de ingeniería social conocida como ClickFix para desplegar una puerta trasera multifuncional llamada CORNFLAKE.V3.

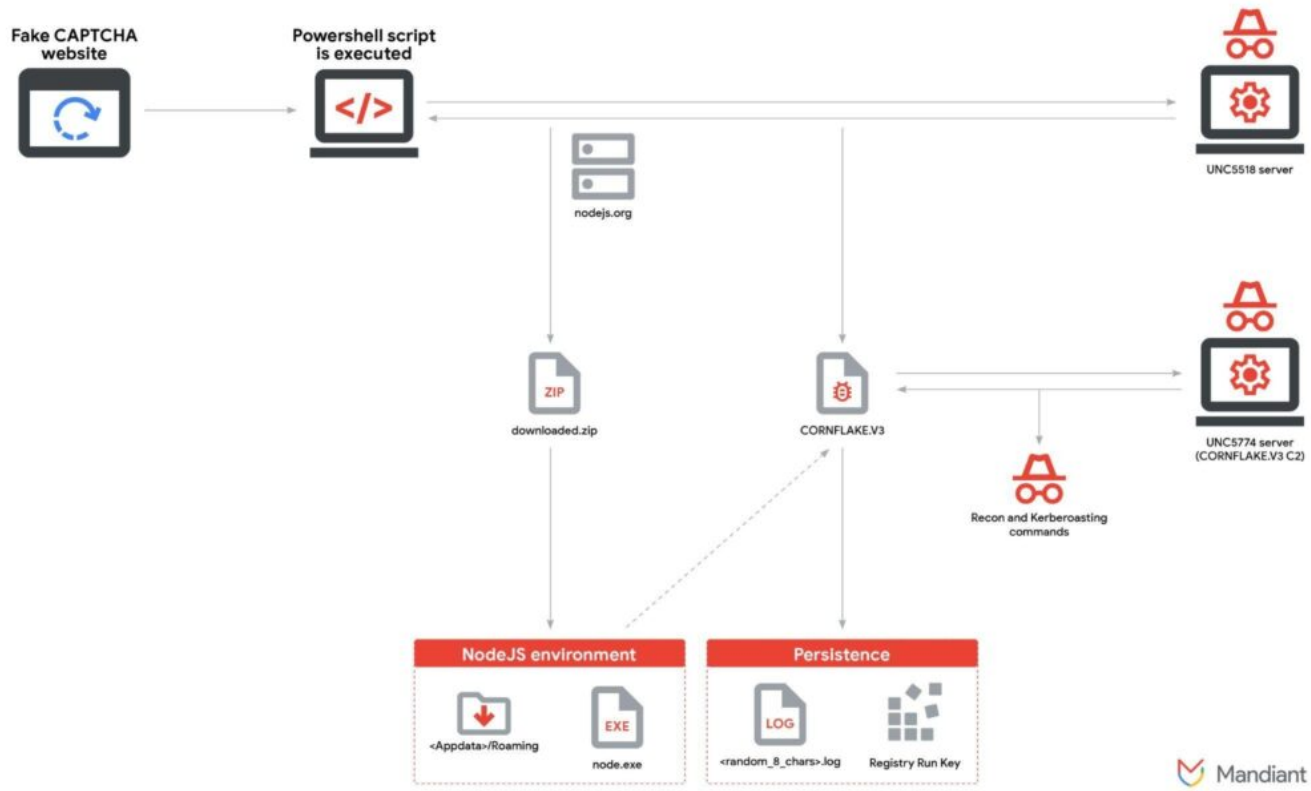
Mandiant, propiedad de Google, describió esta actividad —a la que rastrea como UNC5518— como parte de un esquema de *access-as-a-service*, en el que se emplean páginas falsas de CAPTCHA para engañar a los usuarios y lograr acceso inicial a sus sistemas, acceso que luego es monetizado por otros grupos de amenazas.

"El vector inicial de infección, denominado ClickFix, consiste en atraer a los usuarios a sitios web comprometidos donde se les induce a copiar un script malicioso de PowerShell y ejecutarlo mediante el cuadro de diálogo Ejecutar de Windows", señaló Google en un informe publicado hoy.

El acceso conseguido por UNC5518 se considera aprovechado al menos por dos grupos distintos para iniciar un proceso de infección en múltiples etapas y descargar cargas adicionales:

- UNC5774, un grupo con fines financieros que distribuye CORNFLAKE para desplegar diferentes cargas secundarias.
- UNC4108, un actor con motivación desconocida que utiliza PowerShell para instalar herramientas como VOLTMARKER y NetSupport RAT.

La cadena de ataque generalmente comienza cuando la víctima llega a una página falsa de verificación CAPTCHA tras interactuar con resultados de búsqueda manipulados mediante técnicas de envenenamiento SEO o anuncios maliciosos.



Después, el usuario es engañado para ejecutar un comando malicioso de PowerShell desde el cuadro Ejecutar de Windows, lo que descarga desde un servidor remoto la siguiente carga maliciosa. El script descargado comprueba si se está ejecutando en un entorno virtualizado y, finalmente, lanza CORNFLAKE.V3.

Detectado en versiones tanto de JavaScript como de PHP, CORNFLAKE.V3 es una puerta trasera que permite ejecutar cargas útiles a través de HTTP, incluyendo ejecutables, bibliotecas DLL, archivos JavaScript, scripts por lotes y comandos de PowerShell. También recopila información básica del sistema y la envía a un servidor externo, utilizando túneles de Cloudflare para evadir la detección.

"CORNFLAKE.V3 es una versión mejorada de CORNFLAKE.V2, con el que comparte buena parte de su código", explicó el investigador de Mandiant, Marco Galli. *"A diferencia de V2,*

que solo actuaba como descargador, V3 incorpora persistencia en el host mediante una clave Run en el registro, además de admitir más tipos de cargas”.

Ambas generaciones difieren notablemente de su predecesor original, un descargador en C que utilizaba sockets TCP para las comunicaciones C2 y solo era capaz de ejecutar DLL.

La persistencia en el host se logra mediante modificaciones en el Registro de Windows. A través de CORNFLAKE.V3 se entregan al menos tres cargas distintas: una utilidad para reconocimiento en Active Directory, un script para robar credenciales mediante Kerberoasting, y otra puerta trasera denominada WINDYTWIST.SEA, una versión en C de WINDYTWIST que permite retransmitir tráfico TCP, abrir una shell remota, ejecutar comandos y autodesinstalarse.

Algunas variantes de WINDYTWIST.SEA también han intentado propagarse lateralmente en la red de las máquinas comprometidas.

“Para mitigar la ejecución de malware a través de ClickFix, las organizaciones deberían deshabilitar el cuadro de diálogo Ejecutar de Windows en la medida de lo posible”, advirtió Galli. *“Los ejercicios de simulación regulares son fundamentales para contrarrestar esta y otras tácticas de ingeniería social. Asimismo, contar con registros y sistemas de monitoreo robustos es esencial para detectar la ejecución de cargas adicionales como las asociadas a CORNFLAKE.V3”*.

Infecciones USB que distribuyen el minero XMRig

La revelación coincide con el descubrimiento de una campaña activa desde septiembre de 2024 que utiliza memorias USB para infectar otros equipos e instalar *cryptominers*.

“Esto demuestra la vigencia del acceso inicial a través de dispositivos USB comprometidos”, indicó Mandiant. *“El bajo costo y la capacidad de evadir medidas de seguridad de red hacen de esta técnica una opción atractiva para los atacantes”*.

La cadena de ataque comienza cuando la víctima es inducida a ejecutar un acceso directo de Windows (archivo LNK) en la memoria USB comprometida. Dicho acceso directo ejecuta un script de Visual Basic que se encuentra en la misma carpeta, el cual a su vez lanza un archivo por lotes para iniciar la infección:

- DIRTYBULK, un lanzador de DLL en C++ que activa otros componentes maliciosos como CUTFAIL.
- CUTFAIL, un *dropper* en C++ que descifra e instala malware en el sistema, como HIGHREPS y PUMPBENCH, además de librerías externas como OpenSSL, libcurl y WinPthreadGC.
- HIGHREPS, un descargador que obtiene archivos adicionales para asegurar la persistencia de PUMPBENCH.
- PUMPBENCH, una puerta trasera en C++ que realiza reconocimiento, habilita acceso remoto mediante comunicación con un servidor PostgreSQL, y descarga XMRig.
- XMRig, un software de código abierto para minar criptomonedas como Monero, Dero y Ravencoin.

"PUMPBENCH se propaga infectando unidades USB", explicó Mandiant. *"Escanea el sistema en busca de discos disponibles y luego crea un archivo por lotes, un script VB, un acceso directo y un archivo DAT"*.