Los hackers detrás del malware CopperStealer resurgieron con dos nuevas campañas en marzo y abril de 2023, que están diseñadas para entregar dos cargas novedosas denominadas CopperStealth y CopperPhish.

Trend Micro está rastreando al grupo motivado financieramente bajo el nombre de Water Orthrus. También se considera que el adversario está detrás de otra campaña conocida como Scranos, detallada por Bitdefender en 2019.

Activo desde al menos 2021, Water Orthrus tiene un historial de aprovechamiento de las redes de pago por instalación (PPI) para redirigir a las víctimas que aterrizan en sitios de descarga de software hackeados para dejar caer un ladrón de información con nombre en código CopperStealer.

Otra campaña detectada en agosto de 2022 implicó el uso de CopperStealer para distribuir extensiones de navegador web basadas en Chromium que son capaces de realizar transacciones no autorizadas y transferir criptomonedas de las billeteras de las víctimas a las que están bajo el control de los atacantes.

Las últimas secuencias de ataque documentadas por Trend Micro no marcan una gran desviación, propagando CopperStealth empaquetándolo como instaladores de herramientas gratuitas en sitios web chinos para compartir software.

> *«La cadena de infección de CopperStealth implica descargar y cargar un rootkit, que después inyecta su carga útil en explorer.exe y otro proceso del sistema»,* dijeron en un informe técnico los investigadores de seguridad Jaromir Horejsi y Joseph C Chen.

> *«Estas cargas útiles son responsables de descargar y ejecutar tareas adicionales. El rootkit también bloquea el acceso a las claves de registro bloqueadas y evita que se ejecuten ciertos ejecutables y controladores».*

La lista de denegación de controladores contiene secuencias de bytes pertenecientes a empresas chinas de software de seguridad como Huorong, Kingsoft y Qihoo 360.

CopperStealth también incorpora un módulo de tareas que le permite llamar a un servidor remoto y recuperar el comando que se ejecutará en la máquina infectada, equipando al malware para que suelte más cargas útiles.

Los sitios web para compartir archivos actúan como conducto para el kit de phishing CopperPhish

La campaña CopperPhish, detectada en todo el mundo en abril de 2023, aprovecha un proceso análogo para implementar el malware a través de redes PPI detrás de sitios web anónimos gratuitos para compartir archivos.

> *«Los visitantes serán redirigidos a una página de descarga diseñada por la red PPI después de hacer clic en sus anuncios, que pretendían ser un enlace de descarga. El archivo descargado es PrivateLoader, que descarga y ejecuta muchos programas maliciosos diferentes»,* dijeron los investigadores.

El servicio de descarga, que también se ofrece en forma de PPI, se usa después para recuperar e iniciar CopperPhish, un kit de phishing que es responsable de recolectar información de tarjetas de crédito.

Lo logra *«iniciando un proceso rundll32 e inyectando un programa simple con una ventana del navegador (escrito en Visual Basic)»,* que carga una página de phishing que insta a las víctimas a escanear un código QR para verificar su identidad e ingresar un código de confirmación para *«restaurar la red de su dispositivo».*

> *«La ventana no tiene controles que puedan usarse para minimizarla o cerrarla. La*

> *víctima podría cerrar el proceso del navegador en el Administrador de tareas o en el Explorador de procesos, pero también tendría que terminar el proceso de carga útil principal, de lo contrario, el proceso del navegador volverá a ocurrir debido al subproceso de persistencia»*, agregaron los investigadores.

Una vez que se ingresan los detalles confidenciales en la página, el malware CopperPhish muestra el mensaje *«la verificación de identidad ha pasado»* junto con un código de confirmación que la víctima puede ingresar en la pantalla antes mencionada.

Proporcionar el código de confirmación correcto también hace que el malware se desinstale y elimine todos los archivos de phishing caídos de la máquina.

> *«La verificación de credenciales y el código de confirmación son dos características útiles que hacen que este kit de phishing sea más exitoso, ya que la víctima no puede simplemente cerrar la ventana o ingresar información falsa solo para deshacerse de la ventana»,* dijeron los investigadores.

La atribución a Water Orthrus se basa en el hecho de que tanto CopperStealth como CopperPhish comparten características de código fuente similares a las de CopperStealer, lo que plantea la posibilidad de que las tres cepas hayan sido desarrolladas por el mismo autor.

Los objetivos dispares de las campañas representan la evolución de las tácticas del actor de amenazas, lo que indica un intento de agregar nuevas capacidades a su arsenal y expandir sus horizontes financieros.

Los hallazgos se producen cuando se utilizan anuncios maliciosos de Google para atraer a los usuarios a que descarguen instaladores falsos para herramientas de inteligencia artificial como Midjourney y ChatGPT de OpenAI que, en última instancia, eliminan a los ladrones como Vidar y RedLine.

También siguen el descubrimiento de un nuevo servicio de monetización de tráfico llamado TrafficStealer que aprovecha los contenedores de configuraciones incorrectas para redirigir el tráfico a sitios web y generar clics de anuncios falsos como parte de un esquema ilícito de obtención de dinero.