Investigadores en ciberseguridad han identificado una nueva campaña de phishing que distribuye una variante sin archivos del malware comercial conocido como Remcos RAT.

> *«Remcos RAT ofrece a sus compradores una variedad de funciones avanzadas para controlar de manera remota computadoras que pertenecen al comprador»*, explicó Xiaopeng Zhang, investigador de Fortinet FortiGuard Labs, en un análisis publicado la semana pasada.
>
> *«Sin embargo, los actores maliciosos han utilizado Remcos para recopilar información confidencial de las víctimas y tomar control remoto de sus computadoras para realizar actividades maliciosas adicionales».*

El ataque comienza con un correo electrónico de phishing que utiliza un señuelo temático de órdenes de compra para persuadir a los destinatarios a abrir un archivo adjunto de Microsoft Excel.

El documento malicioso de Excel explota una vulnerabilidad conocida de ejecución remota de código en Office (CVE-2017-0199, puntuación CVSS: 7.8) para descargar un archivo HTML Application (HTA) («cookienetbookinetcahce.hta») desde un servidor remoto («192.3.220[.]22») y ejecutarlo a través de mshta.exe.

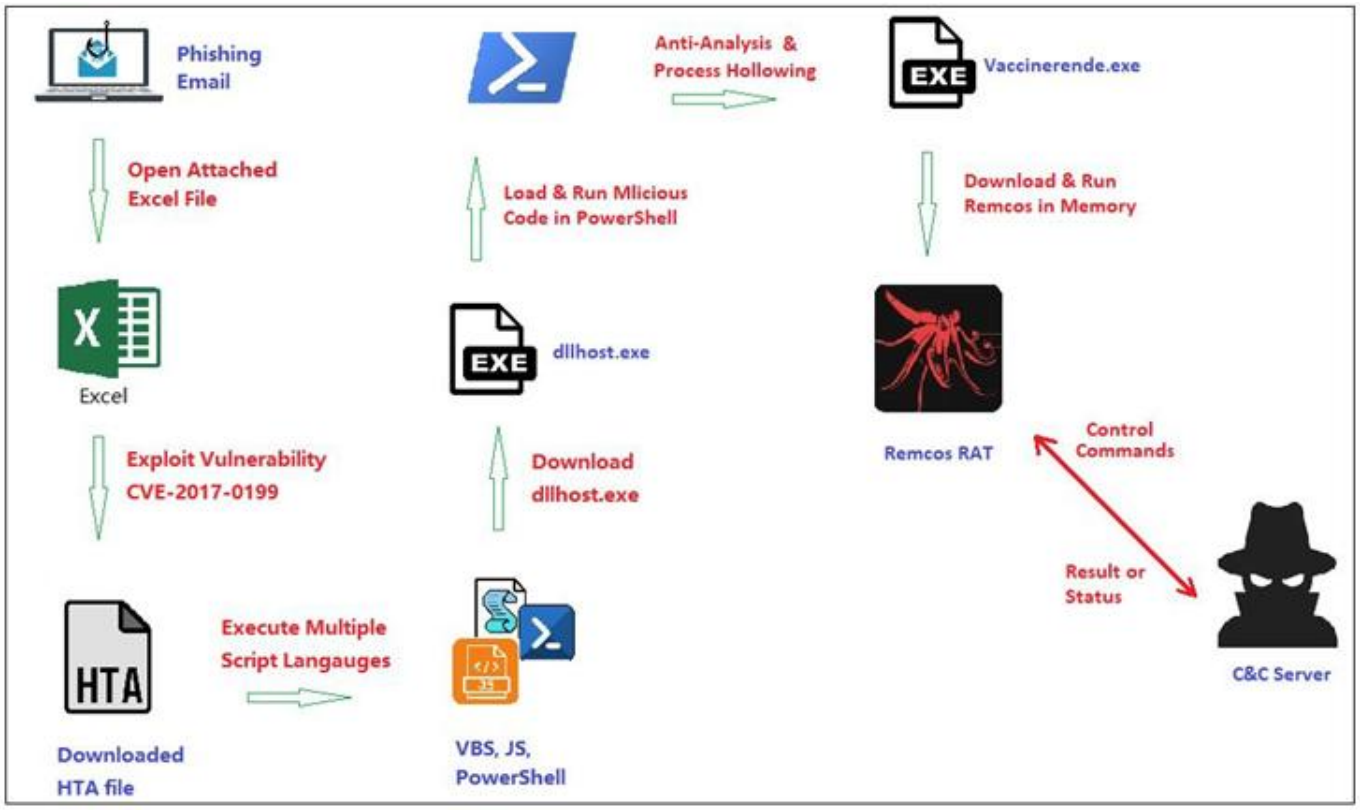
El archivo HTA está oculto en varias capas de JavaScript, Visual Basic Script y código PowerShell para evitar la detección. Su función principal es recuperar y ejecutar un archivo ejecutable desde el mismo servidor.

El archivo binario luego ejecuta otro programa de PowerShell ofuscado, aplicando una serie de técnicas de anti-análisis y anti-depuración para hacer más difícil su detección. En el siguiente paso, el código malicioso utiliza proceso hollowing para finalmente descargar y ejecutar Remcos RAT.

> *«En lugar de almacenar el archivo de Remcos localmente y ejecutarlo, lo despliega directamente en la memoria del proceso activo. Es decir, se trata de una variante sin archivos de Remcos»,* dijo Zhang.

Remcos RAT tiene la capacidad de extraer varios tipos de información del sistema comprometido, incluida la metadata del sistema, y puede ejecutar comandos enviados remotamente por el atacante a través de un servidor de comando y control (C2).

Estos comandos permiten al programa extraer archivos, enumerar y finalizar procesos, gestionar servicios del sistema, editar el Registro de Windows, ejecutar comandos y scripts, capturar el contenido del portapapeles, cambiar el fondo de escritorio de la víctima, activar la cámara y el micrófono, descargar cargas adicionales, grabar la pantalla e incluso deshabilitar el teclado o el mouse.



Este descubrimiento coincide con el informe de Wallarm sobre el abuso de las APIs de Docusign por parte de actores maliciosos para enviar facturas falsas que parecen auténticas, con el fin de engañar a usuarios desprevenidos y realizar campañas de phishing a gran escala.

El ataque implica la creación de una cuenta de DocuSign legítima y pagada, lo que permite a los atacantes modificar plantillas y usar la API directamente. Las cuentas luego se utilizan para crear plantillas de facturas diseñadas para imitar solicitudes de firmas electrónicas de marcas reconocidas, como Norton Antivirus.

> *«A diferencia de las estafas de phishing tradicionales que se basan en correos electrónicos falsificados y enlaces maliciosos, estos ataques utilizan cuentas auténticas de DocuSign y plantillas para hacerse pasar por empresas conocidas, logrando sorprender tanto a los usuarios como a las herramientas de seguridad»*, señaló la empresa.
>
> *«Si los usuarios firman electrónicamente el documento, el atacante puede usar el documento firmado para solicitar pagos fuera de DocuSign o enviarlo al departamento de finanzas para su pago».*

También se han observado campañas de phishing que utilizan una técnica poco convencional llamada concatenación de archivos ZIP para evadir herramientas de seguridad y distribuir troyanos de acceso remoto a las víctimas.

Esta técnica consiste en unir múltiples archivos ZIP en uno solo, lo que genera problemas de seguridad debido a cómo diferentes programas, como 7-Zip, WinRAR y el Explorador de archivos de Windows, descomprimen y procesan estos archivos, permitiendo que las cargas maliciosas pasen desapercibidas.

> *«Aprovechando las diferencias en cómo los lectores de ZIP y los gestores de archivos procesan archivos ZIP concatenados, los atacantes pueden insertar malware dirigido a usuarios de ciertas herramientas específicas»,* explicó Perception Point en un informe reciente.
>
> *«Los atacantes saben que estas herramientas a menudo omiten el contenido malicioso oculto dentro de archivos concatenados, permitiéndoles entregar sus cargas sin ser detectadas y atacar a usuarios que utilizan un programa específico para gestionar archivos».*

Además, un actor de amenazas conocido como Venture Wolf ha sido relacionado con ataques de phishing dirigidos a sectores rusos de manufactura, construcción, tecnología y telecomunicaciones mediante MetaStealer, una variante del malware RedLine Stealer.