Los expertos en ciberseguridad han detectado un complejo ataque de múltiples fases que utiliza señuelos de phishing con temas de facturas para distribuir una amplia gama de malware, como Venom RAT, Remcos RAT, XWorm, NanoCore RAT y un programa para robar información de billeteras de criptomonedas.

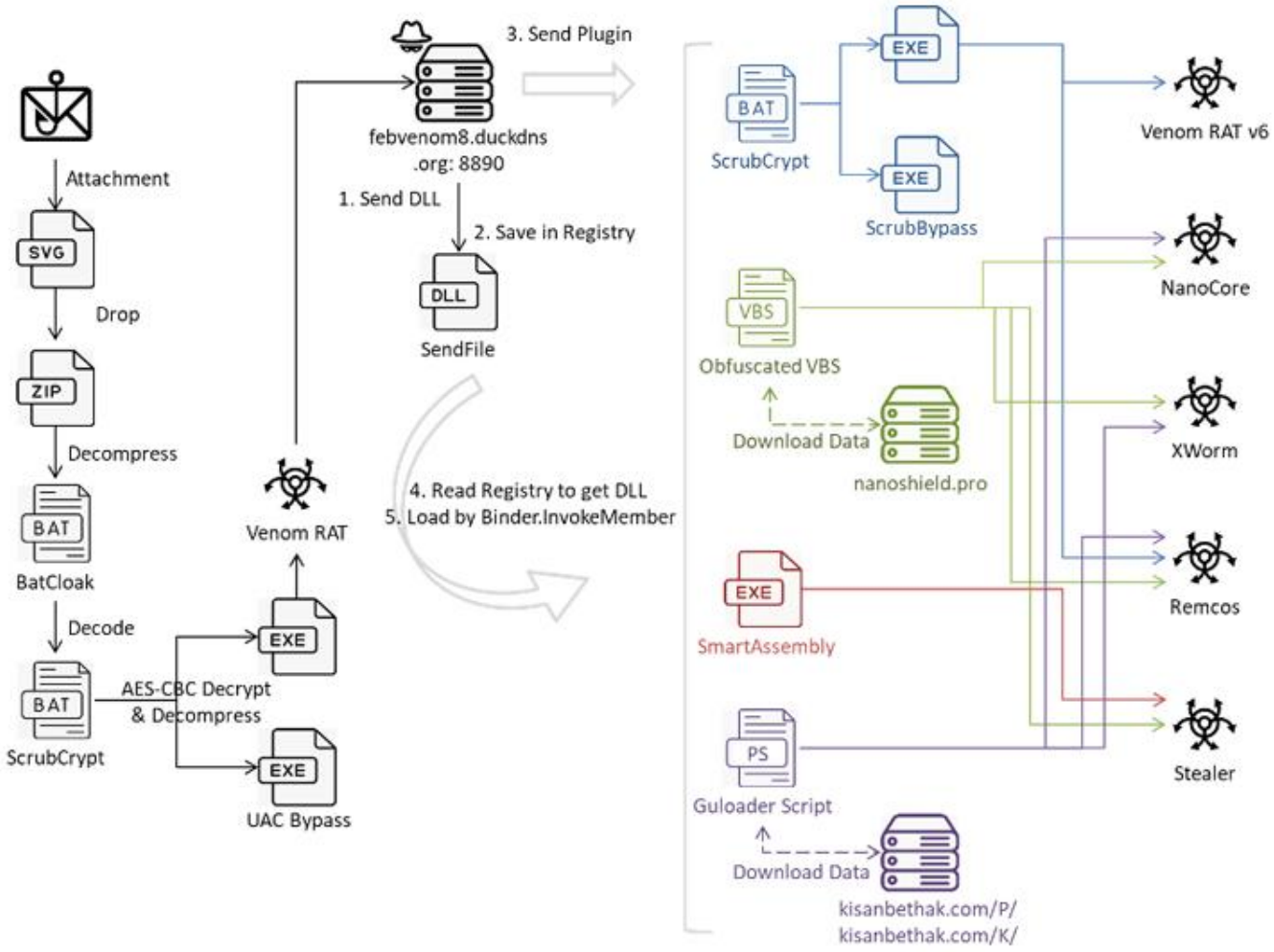
Según un informe técnico de Fortinet FortiGuard Labs, los correos electrónicos vienen con archivos adjuntos en formato Scalable Vector Graphics (SVG) que, al ser abiertos, desencadenan la secuencia de infección.

Lo notable de este modus operandi es la utilización del motor de obfuscación de malware BatCloak y ScrubCrypt para entregar el malware a través de scripts por lotes ofuscados.

BatCloak, disponible para otros actores de amenazas desde finales de 2022, tiene sus raíces en una herramienta llamada Jlaive. Su principal función es cargar una carga útil de siguiente etapa de manera que evite los mecanismos de detección tradicionales.

ScrubCrypt, un programa para cifrar información que fue mencionado por primera vez por Fortinet en marzo de 2023 en relación con una campaña de criptominería organizada por la banda 8220, se considera una de las versiones de BatCloak, según investigaciones de Trend Micro del año pasado.

En la campaña más reciente analizada por la empresa de ciberseguridad, el archivo SVG actúa como un canal para descargar un archivo ZIP que contiene un script por lotes probablemente creado con BatCloak. Luego, este script descomprime el archivo por lotes de ScrubCrypt para finalmente ejecutar Venom RAT, pero primero establece una presencia persistente en el sistema y toma medidas para eludir las protecciones de AMSI y ETW.



Venom RAT, un derivado de Quasar RAT, permite a los atacantes tomar el control de los sistemas comprometidos, recolectar información confidencial y ejecutar comandos recibidos desde un servidor de control y comando (C2).

> *«A pesar de que el programa principal de Venom RAT puede parecer simple, mantiene canales de comunicación con el servidor C2 para obtener complementos adicionales para diversas actividades»,* dijo la investigadora de seguridad Cara Lin. Esto incluye Venom RAT v6.0.3 con funciones de keylogger, NanoCore RAT, XWorm

> y Remcos RAT.
>
> *«Este complemento [Remcos RAT] fue distribuido desde el C2 de VenomRAT utilizando tres métodos: un script VBS ofuscado llamado 'remcos.vbs', ScrubCrypt y GuLoader PowerShell»,* agregó Lin.

También se entrega utilizando el sistema de complementos un programa para robar información que recopila detalles del sistema y transfiere datos desde carpetas asociadas con billeteras y aplicaciones como Atomic Wallet, Electrum, Ethereum, Exodus, Jaxx Liberty (que fue retirada en marzo de 2023), Zcash, Foxmail y Telegram hacia un servidor remoto.

> *«Este análisis revela un ataque sofisticado que utiliza múltiples capas de obfuscación y técnicas de evasión para distribuir y ejecutar VenomRAT a través de ScrubCrypt»,* dijo Lin.
>
> *«Los atacantes utilizan una variedad de métodos, incluidos correos electrónicos de phishing con archivos adjuntos maliciosos, archivos de script ofuscados y Guloader PowerShell, para infiltrar y comprometer sistemas víctimas. Además, la implementación de complementos mediante diferentes cargas útiles resalta la versatilidad y adaptabilidad de la campaña de ataque».*