Investigadores de ciberseguridad han expuesto una nueva campaña de malware sofisticada que utiliza anuncios pagados en motores de búsqueda como Google para distribuir software malicioso a usuarios desprevenidos que buscan herramientas populares como GitHub Desktop.

Si bien las campañas de *malvertising* se han vuelto habituales en los últimos años, esta operación introduce un giro particular: la inserción de un *commit* de GitHub en la URL de una página que incluye enlaces alterados dirigidos a infraestructura controlada por atacantes.

*"Incluso cuando un enlace parece llevar a una plataforma confiable como GitHub, la URL subyacente puede manipularse para redirigir a un sitio fraudulento"*, señaló Arctic Wolf en un informe publicado la semana pasada.

Desde al menos diciembre de 2024, los ataques se han enfocado exclusivamente en empresas de TI y desarrollo de software en Europa Occidental. Los enlaces dentro del *commit* manipulado redirigen a las víctimas hacia una descarga maliciosa alojada en un dominio falso ("gitpage[.]app").

El malware de primera etapa, distribuido mediante resultados de búsqueda envenenados, consiste en un instalador de Microsoft Software Installer (MSI) de 128 MB que, debido a su gran tamaño, evade la mayoría de los entornos de análisis en línea. Además, emplea una rutina de descifrado restringida por unidad de procesamiento gráfico (GPU), manteniendo la carga útil cifrada en sistemas que carecen de GPU real. La técnica ha sido bautizada como GPUGate.

*"Los sistemas sin controladores adecuados de GPU suelen ser máquinas virtuales (VMs), entornos de prueba o laboratorios de análisis antiguos que los investigadores usan con frecuencia"*, explicó la compañía de ciberseguridad. *"El ejecutable [...] emplea funciones de la GPU para generar una clave de cifrado que descifra la carga, y durante el proceso verifica el nombre del dispositivo GPU"*.

Además de incluir múltiples archivos basura para aumentar el tamaño y dificultar el análisis,

el malware detiene su ejecución si el nombre del dispositivo tiene menos de 10 caracteres o si las funciones de GPU no están disponibles.

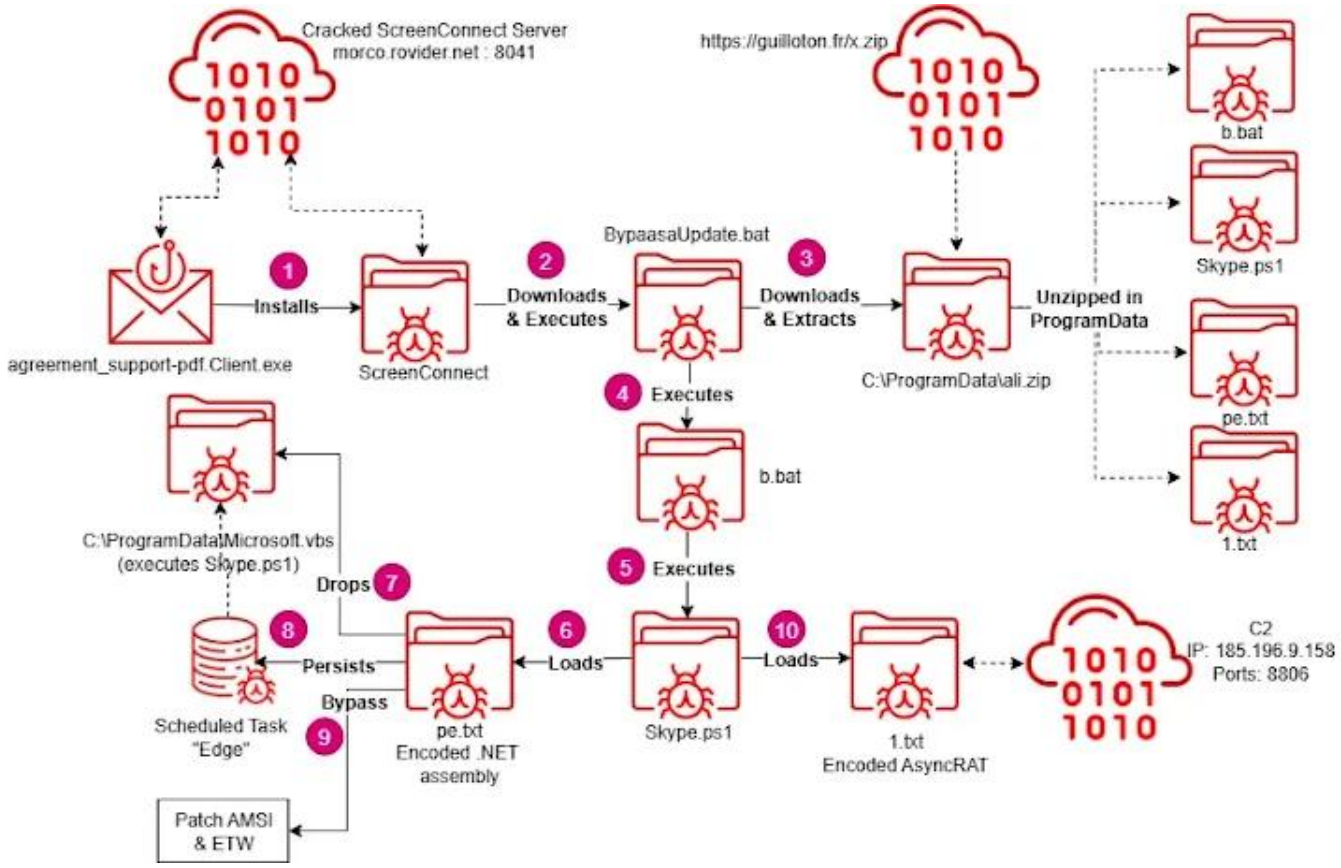
El ataque prosigue con la ejecución de un script en Visual Basic que activa un script de PowerShell. Este último se ejecuta con privilegios de administrador, añade exclusiones en Microsoft Defender, configura tareas programadas para garantizar persistencia y, finalmente, lanza ejecutables extraídos de un archivo ZIP descargado.

El objetivo final es facilitar el robo de información y la instalación de cargas adicionales, mientras se evita la detección. Se estima que los operadores de la campaña poseen dominio nativo del idioma ruso, debido a comentarios escritos en ruso encontrados en el script de PowerShell.

Un análisis más profundo del dominio utilizado por los atacantes reveló que también funciona como base de operaciones para Atomic macOS Stealer (AMOS), lo que apunta a un enfoque multiplataforma.

*"Al aprovechar la estructura de commits de GitHub y el uso de anuncios de Google, los atacantes logran imitar de forma convincente repositorios de software legítimos y redirigir a los usuarios hacia cargas maliciosas, eludiendo tanto la revisión humana como las defensas en los endpoints"*, añadió Arctic Wolf.

La revelación coincide con un informe de Acronis sobre la evolución de una campaña de ConnectWise ScreenConnect troyanizada, que emplea este software de acceso remoto para desplegar AsyncRAT, PureHVNC RAT y un troyano personalizado basado en PowerShell en equipos comprometidos, dentro de ataques de ingeniería social contra organizaciones en EE. UU. desde marzo de 2025.




El RAT hecho a medida en PowerShell, ejecutado a través de un archivo JavaScript descargado desde un servidor de ScreenConnect vulnerado, incluye funciones básicas como ejecutar programas, descargar y ejecutar archivos, además de un mecanismo simple de persistencia.

*"Los atacantes ahora utilizan un instalador ClickOnce para ScreenConnect, que carece de configuración incrustada y obtiene los componentes en tiempo de ejecución"*, explicó el proveedor de seguridad. *"Esta evolución vuelve menos efectivas las técnicas tradicionales de detección estática y dificulta la prevención, dejando a los defensores con pocas opciones confiables"*.