Los cazadores de amenazas están advirtiendo sobre una nueva campaña maliciosa que utiliza sitios web falsos para engañar a los usuarios desprevenidos y hacer que ejecuten scripts maliciosos de PowerShell, lo que finalmente conduce a la instalación del malware NetSupport RAT.

El equipo de investigaciones de DomainTools (DTI) informó que detectó *«scripts maliciosos de PowerShell con múltiples etapas de descarga»* alojados en sitios fraudulentos que se hacen pasar por plataformas legítimas como Gitcode y DocuSign.

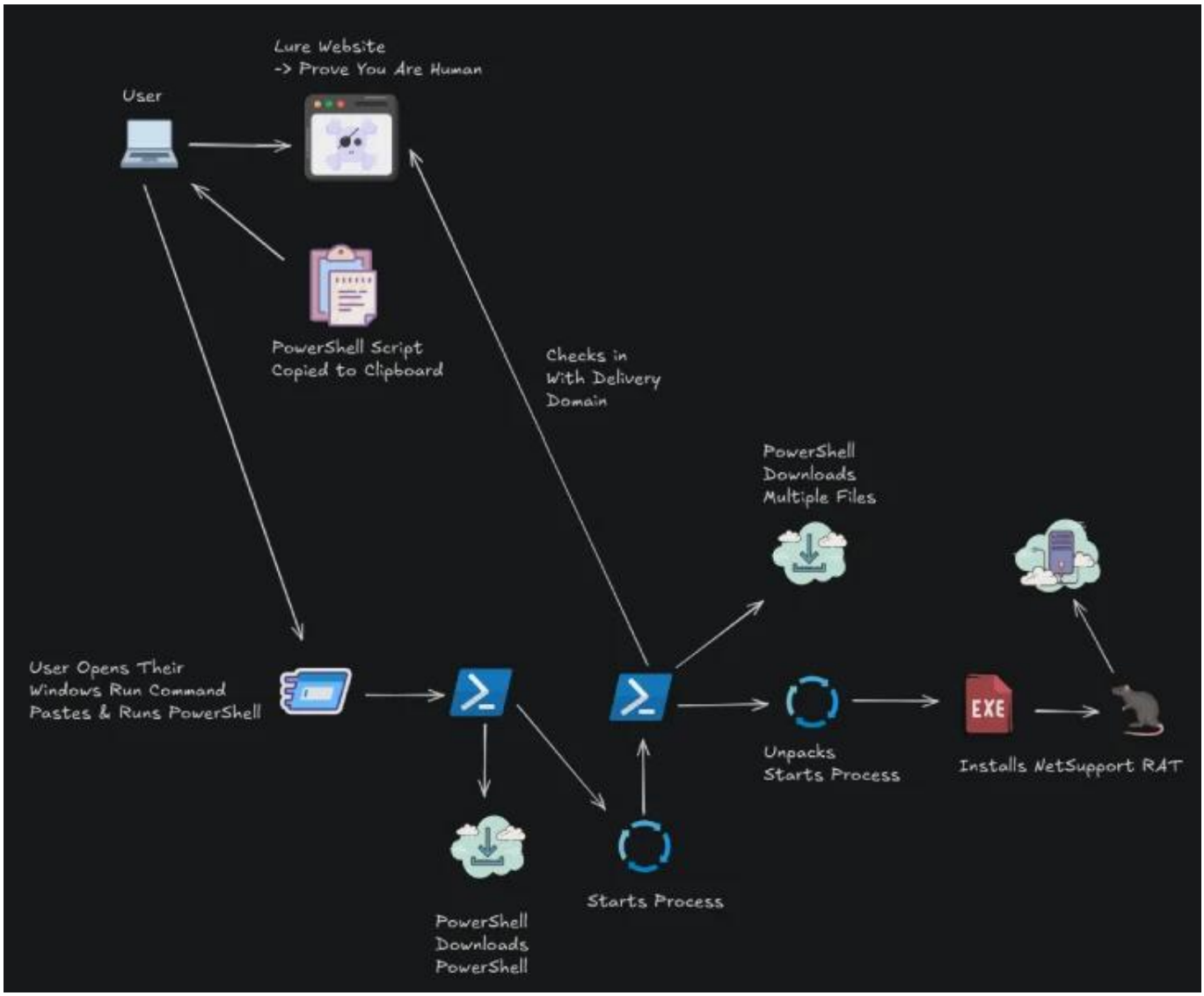
> *"Estos sitios intentan engañar a los usuarios para que copien y ejecuten un script inicial de PowerShell mediante el comando Ejecutar de Windows"*, explicó la empresa en un informe técnico.
>
> *"Al hacerlo, el script inicial descarga otro script de PowerShell que actúa como descargador, el cual obtiene y ejecuta cargas útiles adicionales, lo que termina con la instalación de NetSupport RAT en los equipos comprometidos".*

Se sospecha que estos sitios web falsos están siendo promocionados a través de campañas de ingeniería social, posiblemente por correo electrónico o redes sociales.

Los scripts maliciosos disponibles en los sitios que imitan a Gitcode están diseñados para obtener una serie de scripts intermedios desde un servidor externo (específicamente "tradingviewtool[.]com"), los cuales son ejecutados secuencialmente hasta activar el NetSupport RAT en los sistemas infectados.

DomainTools también señaló que detectó múltiples páginas que imitan a DocuSign (por ejemplo, docusign.sa[.]com), las cuales distribuyen el mismo troyano de acceso remoto, pero con una variación: emplean mecanismos de verificación tipo CAPTCHA estilo ClickFix para engañar a las víctimas y hacer que ejecuten el script de PowerShell.

Al igual que en cadenas de ataque recientes asociadas con el infostealer EDDIESTEALER, los usuarios que visitan estos sitios deben *"verificar que no son un robot"* completando un desafío CAPTCHA.



Una vez superada esta verificación, se copia de manera oculta un comando de PowerShell ofuscado en el portapapeles del usuario —una táctica conocida como *clipboard poisoning*—.

Luego, se le indica que abra el cuadro de ejecución de Windows (“Win + R”), pegue el contenido (“CTRL + V”) y presione Enter, lo que lanza el script.

El código descargado obtiene un ejecutable llamado “wbdims.exe” desde GitHub, cuya función es garantizar que la carga maliciosa se ejecute automáticamente cada vez que el usuario inicie sesión.

> *“Si bien esta carga útil ya no estaba disponible al momento de la investigación, se espera que se comunique con el sitio de entrega a través de ‘docusign.sa[.]com/verification/c.php’. Al hacerlo, se produce una actualización en el navegador para mostrar el contenido de ‘docusign.sa[.]com/verification/s.php?an=1’”,* comentó DomainTools.

Este proceso permite la ejecución de un segundo script de PowerShell, el cual descarga y ejecuta una tercera carga comprimida en ZIP desde el mismo servidor, modificando el parámetro de URL “an” a “2”. El script descomprime el archivo y lanza un ejecutable llamado “jp2launcher.exe”, lo que concluye con la instalación del NetSupport RAT.

> *“La estructura en múltiples etapas —scripts que descargan otros scripts, que a su vez descargan y ejecutan más scripts— probablemente busca eludir mecanismos de detección y dificultar el análisis por parte de investigadores de seguridad”,* indicó la compañía.

Aunque aún no se conoce quién está detrás de esta campaña, DomainTools destacó similitudes con una operación anterior vinculada a SocGholish (también conocido como FakeUpdates), detectada en octubre de 2024, tanto en la forma de registrar los dominios como en los patrones de entrega.

> *“Cabe destacar que las técnicas utilizadas son comunes, y NetSupport Manager es una herramienta legítima de administración remota que ha sido aprovechada como RAT por diversos grupos de amenazas como FIN7, Scarlet Goldfinch, Storm-0408, entre otros”.*