Microsoft advirtió el jueves sobre una *«campaña masiva de correo electrónico»*, que está impulsando el malware STRRAT basado en Java para robar datos confidenciales de los sistemas infectados mientras se disfraza como una infección de ransomware.

> *«Este RAT es famoso por su comportamiento como ransomware, basado en añadir el nombre del archivo de extensión .crimson a archivos sin necesidad de encriptarlos»,* dijo el equipo de seguridad de Inteligencia de Microsoft.

Esta ola de ataques, que la compañía detectó hace unos días, comienza con correos electrónicos no deseados enviados desde cuentas de correo electrónico comprometidas con *«Pagos salientes»* en el asunto, lo que atrae a los destinatarios para que abran documentos PDF maliciosos que dicen ser remesas, pero que en realidad, se conectan a un dominio fraudulento para descargar el malware STRRAT.

Además de establecer conexiones a un servidor de comando y control durante la ejecución, el malware cuenta con una variedad de características que le permiten recopilar contraseñas del navegador, registrar pulsaciones de teclas y ejecutar comandos remotos y scripts de PowerShell.

STRRAT surgió por primera vez en el panorama de amenazas en junio de 2020, con la compañía alemana de seguridad cibernética G Data, observando el malware de Windows (versión 1.2) en correos electrónicos de phishing que contienen archivos adjuntos maliciosos de Jar (Java Archive).

> *«El RAT tiene un enfoque en el robo de credenciales de los navegadores y clientes de correo electrónico y contraseñas a través de keylogging. Es compatible con los siguientes navegadores y clientes de correo electrónico: Firefox, Internet Explorer, Chrome, Foxmail, Outlook, Thunderbird»,* dijo Karsten Kahn, analista de G Data.

Sus capacidades de ransomware son, en el mejor de los casos, rudimentarias en el sentido de que la etapa de cifrado solo cambia el nombre de los archivos mediante el sufijo «.crimson». *«Si se elimina la extensión, los archivos se pueden abrir como de costumbre»*, dijo Kahn.

Microsoft también dijo que la versión 1.5 es más confusa y modular que las versiones anteriores, lo que sugiere que los atacantes detrás de la operación están trabajando activamente para improvisar su conjunto de herramientas. Pero el hecho de que el comportamiento de cifrado falso permanezca sin cambios indica que el grupo puede estar apuntando a ganar dinero rápidamente con usuarios desprevenidos mediante la extorsión.

Los indicadores de compromiso (IoC) asociados con la campaña están disponibles en GitHub.