El grupo de hackers Evilnum, que es conocido por apuntar al sector fintech al menos desde 2018, ha cambiado sus tácticas para incluir un nuevo troyano de acceso remoto (RAT) basado en Python, que puede robar contraseñas, documentos, cookies del navegador, credenciales de correo electrónico, entre otra información confidencial.

En un análisis publicado este jueves por los investigadores de Cybereason, el grupo Evilnum no solo ha modificado su cadena de infección, sino que también ha implementado una Python RAT llamada «PyVil RAT», que tiene capacidades para recopilar información, tomar capturas de pantalla, capturar pulsaciones de teclas, abrir shell SSH, e implementar nuevas herramientas.

> *«Desde los primeros informes en 2018 hasta hoy, los TTP del grupo han evolucionado con distintas herramientas, mientras que el grupo ha seguido enfocándose en los objetivos de fintech»,* dijo la compañía de seguridad.
>
> *«Estas variaciones incluyen un cambio en la cadena de infección y persistencia, nueva infraestructura que se expande con el tiempo y el uso de un nuevo troyano de acceso remoto (RAT) con script de Python».*

En los últimos dos años, Evilnum se ha relacionado con varias campañas de malware contra empresas en el Reino Unido y la UE, que involucran puertas traseras escritas en JavaScript y C#, así como por medio de herramientas compradas al proveedor de malware como servicio, Golden Chickens.

En julio, se descubrió que el grupo APT apuntaba a empresas con correos electrónicos de suplantación de identidad (spear-phishing), que contienen un enlace a un archivo ZIP alojado en Google Drive para robar licencias de software, información de tarjetas de crédito de clientes e inversiones y documentos comerciales.

Aunque el modus operandi de lograr un punto de apoyo inicial en el sistema comprometido sigue siendo el mismo, el procedimiento de infección ha sido testigo de un cambio importante.

Además de utilizar correos electrónicos de spear-phishing con documentos falsos de Conocer a Su Cliente (KYC) para engañar a los empleados de la industria financiera para que activen el malware, los ataques han dejado de usar troyanos basados en JavaScript con capacidades de puerta trasera a un simple cuentagotas de JavaScript que ofrece cargas útiles maliciosas ocultas en versiones modificadas de ejecutables legítimos en un intento de escapar a la detección.

> *«Este JavaScript es la primera etapa en esta nueva cadena de infección, que culmina con la entrega de la carga útil, una RAT escrita en Python compilada con py2exe que los investigadores de Nocturns denominaron PyVil RAT»,* dijeron los investigadores.

El procedimiento de entrega multiproceso («ddpp.exe»), luego de la ejecución, descomprime el shellcode para establecer comunicación con un servidor controlado por el atacante y recibe un segundo ejecutable encriptado («fplayer.exe») que funciona como el descargador de la siguiente etapa para recuperar el Python RAT.

> *«En campañas anteriores del grupo, las herramientas de Evilnum evitaban el uso de dominios en las comunicaciones con el C2, utilizando únicamente direcciones IP. Si bien la dirección IP C2 cambia cada pocas semanas, la lista de dominios asociados con esta dirección IP sigue creciendo»*, dijeron los investigadores.