Se ha descubierto un nuevo módulo para el troyano bancario TrickBot que permite a los atacantes aprovechar los sistemas comprometidos para lanzar ataques de fuerza bruta contra sistemas Windows seleccionados que ejecutan una conexión de Protocolo de Escritorio Remoto (RDP) expuesta a Internet.

El módulo, denominado *«rdpScanDll»*, fue descubierto el 30 de enero de este año, y se cree que todavía está en desarrollo, según la firma de seguridad cibernética Bitdefender, en un informe.

Según los investigadores, el módulo de fuerza bruta rdpScanDll hasta el momento ha intentado apuntar a 6013 servidores RDP pertenecientes a empresas de telecomunicaciones, educación y sectores financieros en Estados Unidos y Hong Kong.

Los autores detrás de TrickBot se especializan en lanzar nuevos módulos y versiones del troyano en un intento de expandir y refinar sus capacidades.

> *«La flexibilidad permitida por esta arquitectura modular convirtió a TrickBot en un malware muy complejo y sofisticado capaz de una amplia gama de actividades maliciosas, siempre que exista un complemento para él»,* dijeron los investigadores.
>
> *«Desde complementos para robar datos confidenciales de OpenSSH y OpenVPN, hasta módulos que realizan ataques de intercambio de SIM para tomar el control del número de teléfono de un usuario e incluso deshabilitar los mecanismos de seguridad incorporados de Windows antes de descargar sus módulos principales, TrickBot es un jack- de todos los oficios».*

Funcionamiento del módulo TrickBot RDP

Cuando TrickBot comienza su ejecución, crea una carpeta que contiene las cargas maliciosas cifradas y sus archivos de configuración asociados, que incluye una lista de servidores de

comando y control (C2) con los que el complemento necesita comunicarse para recuperar los comandos que se ejecutarán.

Según Bitdefender, el complemento rdpSanDll comparte su archivo de configuración con otro módulo llamado «vncDll», mientras utiliza un formato de URL estándar para comunicarse con los nuevos servidores C2: https://C&C/tag/computerID/controlEndpoint.

«C&C» se refiere al servidor C2, *«tag»* se refiere a la etiqueta de grupo utilizada por la muestra TrickBot, *«ComputerID»* es la ID de la computadora utilizada por el malware y *«ControlEndpoint»*, una lista de modos de ataque (check, trybute y bruto) y la lista de combinaciones de dirección IP – número de puerto a las que se dirigirá por meio de un ataque de fuerza bruta RDP.

Mientras que el modo «verificar» busca una conexión RDP de la lista de objetivos, el modo *«truebrute»* intenta una operación de fuerza bruta en el objetivo seleccionado utilizando una lista predeterminada de nombres de usuario y contraseñas obtenidas de los puntos finales *«/rdp/names» y «/rdp/dict»* respectivamente.

El modo «bruto», según los investigadores, al parecer sigue en desarrollo. No solo incluye un conjunto de funciones ejecutables que no se invocan, el modo *«no obtiene la lista de nombres de usuario, lo que hace que el complemento use contraseñas y nombres de usuario nulos para autenticarse en la lista de objetivos».*

Una vez que se agota la lista inicial de IP dirigidas recopiladas a través de *«/rdp/domains»*, el complemento recupera otro conjunto de IP nuevas utilizando un segundo punto final *«/rdp/over».*

Las dos listas, cada una con 49 y 5964 direcciones IP, incluían objetivos ubicados en Estados Unidos y Hong Kong que abarcaban las verticales de telecomunicaciones, educación, finanzas e investigación científica.

Además, el informe de Bitdefender detalló el mecanismo de entrega de actualizaciones de TrickBot, encontrando que los complementos responsables del movimiento lateral por medio de la red (WormDll, TabDll, Sharedll), recibieron la mayoría de las actualizaciones, seguidas de módulos que ayudaron a llevar a cabo el reconocimiento de *«sistema y red»* (SystemInfo, NetworkDll) y la recolección de datos (ImportDll, Pwgrab, aDll) en el transcurso de los últimos seis meses.

> *«Mientras monitoreábamos las actualizaciones de complementos maliciosos, observamos que los que se actualizaban con mayor frecuencia eran los que realizaban movimientos laterales: 32.07% de ellos eran gusanos, 31.44% eran shareDll y 16.35% eran tabDll»*, dijeron los investigadores.

Los investigadores también pudieron identificar al menos 3460 direcciones IP que actuaban como servidores C2 en todo el mundo, incluidos 556 servidores que se dedicaron exclusivamente a descargar nuevos complementos y 22 IP que cumplieron ambas funciones.

Difundido a través de campañas de phishing por correo electrónico, TrickBot comenzó su vida como troyano bancario en 2016, facilitando el robo financiero. Pero desde entonces ha evolucionado para entregar otros tipos de malware, incluido el notorio ransomware Ryuk, actuar como un ladrón de información, saquear billeteras de Bitcoin y cosechar correos electrónicos y credenciales.

Las campañas de mailspam que ofrece TrickBot utilizan marcas de terceros conocidas para el destinatario, como las facturas de las empresas contables y financieras.

Los correos electrónicos generalmente incluyen un archivo adjunto, como un documento de Microsoft Word o Excel, que al ejecutarse, solicitará al usuario que habilite las macros, ejecutando así un VBScript para ejecutar un script de PowerShell para descargar el malware.

TrickBot también se descarta como carga útil secundaria de otro malware, especialmente de la campaña de spam de bots de Emotet. Para obtener persistencia y evadir la detección, se

descubrió que el malware crea una tarea programada y un servicio, e incluso deshabilita y elimina el software antivirus Windows Defender.

Debido a esto, Microsoft implementó una función de Protección contra manipulaciones para proteger contra cambios maliciosos y no autorizados a los funcionarios de seguridad el año pasado.

> *«El nuevo módulo rdpScanDll puede ser el último de una larga línea de módulos que ha sido utilizado por el troyano TrickBot, pero es uno que destaca por el uso de una lista altamente específica de direcciones IP»*, según dijeron los investigadores.
>
> *«Utilizando una infraestructura existente de víctimas de TrickBot, el nuevo módulo sugiere que los atacantes también pueden centrarse en verticales que no sean financieras, como servicios de telecomunicaciones y educación e investigación».*