Una nueva investigación ha revelado cerca de 200 dominios únicos de comando y control (C2) asociados con un malware conocido como Raspberry Robin.

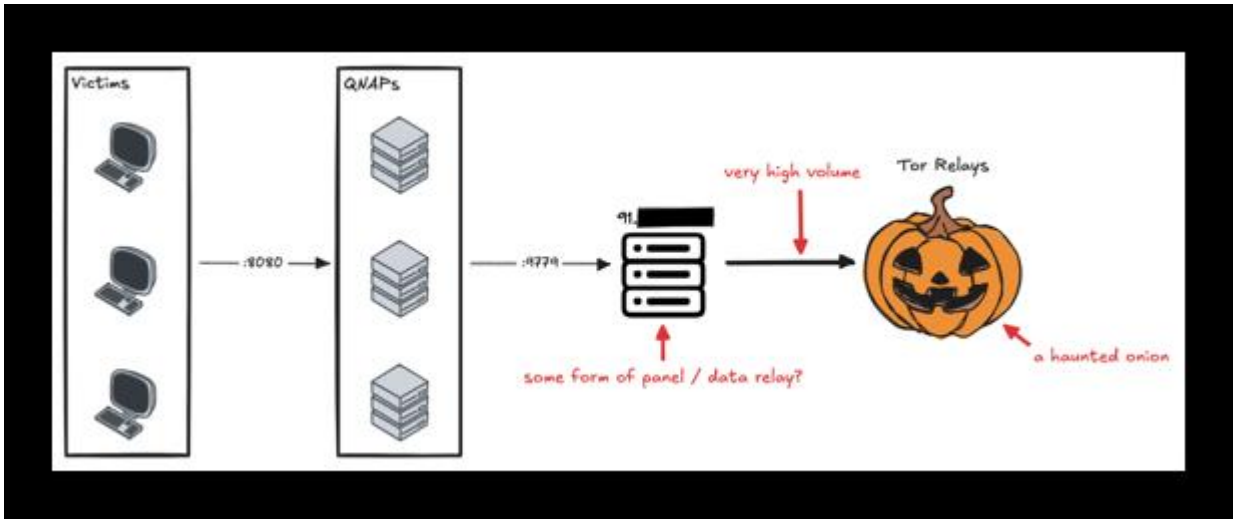
«Raspberry Robin (también llamado Roshtyak o Storm-0856) es un actor de amenazas complejo y en evolución que proporciona servicios de corredor de acceso inicial (IAB, por sus siglas en inglés) a varios grupos criminales, muchos de los cuales tienen vínculos con Rusia», señaló Silent Push en un informe.

Desde su aparición en 2019, este malware ha servido como canal para la distribución de diversas amenazas como SocGholish, Dridex, LockBit, IcedID, BumbleBee y TrueBot. También se le conoce como un gusano de QNAP, ya que utiliza dispositivos QNAP comprometidos para obtener y distribuir su carga maliciosa.

A lo largo del tiempo, las cadenas de ataque de Raspberry Robin han evolucionado para incluir nuevas técnicas de distribución. Entre ellas, la descarga a través de archivos comprimidos y Windows Script Files (WSF) enviados como adjuntos mediante el servicio de mensajería Discord. Además, los operadores del malware han aprovechado vulnerabilidades de día uno para escalar privilegios localmente antes de que estas fueran divulgadas públicamente.

También hay indicios de que este malware es ofrecido a otros actores maliciosos bajo un modelo de botnet de pago por instalación (PPI), permitiendo la entrega de software malicioso en etapas posteriores.

Por otra parte, Raspberry Robin ha implementado un mecanismo de propagación mediante dispositivos USB infectados. Este método consiste en utilizar una memoria USB comprometida que contiene un archivo de acceso directo de Windows (LNK) disfrazado de carpeta, con el objetivo de activar la instalación del malware.



El gobierno de los Estados Unidos ha revelado que un actor de amenazas vinculado al Estado ruso, identificado como Cadet Blizzard, podría haber utilizado Raspberry Robin como una herramienta de acceso inicial.

En su más reciente análisis, llevado a cabo en conjunto con Team Cymru, Silent Push identificó una dirección IP utilizada como relé de datos para conectar todos los dispositivos QNAP comprometidos, lo que permitió el hallazgo de más de 180 dominios únicos de C2.

«Esta dirección IP estaba conectada a través de relés de Tor, lo que probablemente permitió a los operadores de la red emitir nuevos comandos e interactuar con los dispositivos comprometidos», explicó la compañía. *«La dirección IP utilizada para este relé estaba ubicada en un país de la Unión Europea»*.

Un análisis más profundo de la infraestructura reveló que los dominios C2 de Raspberry Robin son de corta longitud (por ejemplo, q2[.]rs, m0[.]wf, h0[.]wf, 2i[.]pm) y que estos se rotan rápidamente entre dispositivos comprometidos mediante direcciones IP utilizando una técnica conocida como fast flux, diseñada para dificultar su eliminación.

Algunos de los principales dominios de nivel superior (TLDs) asociados con Raspberry Robin incluyen .wf, .pm, .re, .nz, .eu, .gy, .tw y .cx. Además, los dominios han sido registrados a

través de registradores menos comunes como Sarek Oy, 1API GmbH, NETIM, Epag[.]de, CentralNic Ltd y Open SRS. La mayoría de los dominios C2 identificados tienen servidores de nombres en una empresa búlgara llamada ClouDNS.

«El uso de Raspberry Robin por parte de actores de amenazas del gobierno ruso concuerda con su historial de colaboración con numerosos grupos de cibercriminales altamente peligrosos, muchos de los cuales tienen conexiones con Rusia», explicó la compañía. *«Entre estos grupos se encuentran LockBit, Dridex, SocGholish, DEV-0206, Evil Corp (DEV-0243), Fauppod, FIN11, Clop Gang y Lace Tempest (TA505)»*.