Después de un año de que se lanzaran los parches para frustrar los ataques de exploits de la NSA que se filtraron en Internet, cientos de miles de computadoras no cuentan con dichos parches y son vulnerables, según informa TechCrunch.

Primero, las herramientas de hacking de la NSA fueron utilizadas para difundir ransomware, luego se utilizaron para realizar ataques de minado de criptomonedas. Ahora, los investigadores aseguran que los piratas informáticos utilizan dichas herramientas filtradas para la creación de una red proxy maliciosa mucho más grande.

Nuevos hallazgos en las investigaciones de la compañía de seguridad Akamai, afirman que la vulnerabilidad UPnProxy, que aprovecha el protocolo de red Universal Plug and Play común, ahora puede apuntar a computadoras no parcheadas detrás del firewall del enrutador.

Los atacantes utilizaban UPnProxy para reasignar la configuración de reenvío de puerto en un enrutador afectado, permitiendo así la ofuscación y enrutamiento del tráfico malicioso, que puede ser utilizado para lanzar ataques distribuidos de denegación de servicio o propagación de malware y spam.

En la mayoría de los casos, las computadoras en red no se vieron afectadas debido a que estaban protegidas por las reglas de traducción de direcciones de red (NAT) del enrutador.

Sin embargo, Akamai afirma que los atacantes están utilizando explotaciones más poderosas para penetrar el enrutador y así infectar computadoras individuales en la red. Con esto, los atacantes cuentan con mayor alance de dispositivos objetivos y su red maliciosa se hace mucho más fuerte.

> *«Aunque es desafortunado ver que UPnProxy se aproveche activamente para atacar los sistemas que anteriormente estaban protegidos detrás del NAT, eventualmente iba a suceder»*, dijo Chad Seaman, de Akamai.

Las inyecciones utilizan dos vulnerabilidades, una es EternalBlue, una puerta trasera

desarrollada por la Agencia de Seguridad Nacional para atacar computadoras con sistema operativo Windows, y su «hermano», EternalRed, que se utiliza para los dispositivos con sistema Linux. Cuando UPnProxy modificó la asignación de puertos en un enrutador vulnerable, la familia Eternal de exploits se dirigió a los puertos de servicio utilizados por SMB, un protocolo de red común utilizado en la mayoría de las computadoras.

Akamai llama a este nuevo ataque «EternalSilence», y juntos, expanden demasiado la red proxy a muchos más dispositivos vulnerables.

La compañía de seguridad asegura que más de 45 mil dispositivos ya se encuentran bajo el control de dicha red masiva, potencialmente, esto representaría más de un millón de computadoras esperando comandos.

> *«El objetivo aquí no es un ataque dirigido», dijo Seaman. «Es un intento de aprovechar las hazañas probadas y comprobadas de los exploits, lanzar una red ancha es un estanque relativamente pequeño, con la esperanza de recoger un grupo de dispositivos que anteriormente eran inaccesibles».*

Pero las intrusiones basadas en Eternal son difíciles de detectar, dificultando que los administradores sepan si se encuentran infectados. Debido a esto, las correcciones para EternalBlue y EternalRed han estado disponibles por más de un año, y aún así, millones de dispositivos siguen sin los parches resultando vulnerables a la infección.

Aún así, poco a poco la cantidad de dispositivos vulnerables disminuye, pero Seaman afirmó que las nuevas capacidades de UPnProxy *«pueden ser un último esfuerzo para utilizar las vulnerabilidades conocidas contra un conjunto de máquinas posiblemente no parchadas y previamente inaccesibles».*

El parche contra las amenazas de Eternal resulta buena aunque sea tarde, pero no es un escudo contra el problema. Incluso deshabilitar UPnP no es una solución única.

> Seaman dijo que *«es el equivalente a tapar el agujero en el bote, pero no hace nada para tirar el agua que ha llegado a tu barco que se hunde».*

Actualizar un enrutador afectado y desactivar UPnP podría remediar el problema, pero Seaman asegura que en su opinión, el enrutador probablemente debería estar *«completamente reemplazado».*