Investigadores de seguridad cibernética descubrieron un nuevo ataque cibernético que se cree, es el primer intento de los creadores de la vulnerabilidad BlueKeep RDP en la naturaleza, para comprometer en masa a los sistemas vulnerables para la minería de criptomonedas.

En mayo de este año, Microsoft lanzó un parche para un error de ejecución remota de código altamente crítico, denominado BlueKeep, en sus servicios de escritorio remoto de Windows, que podría explotarse de forma remota para tomar el control total de los sistemas vulnerables al enviar solicitudes especialmente diseñadas sobre RDP.

BlueKeep, rastreado como CVE-2019-0708, es una vulnerabilidad que se puede eliminar porque puede ser armado por un posible malware para propagarse de forma automática de una computadora vulnerable a otra sin requerir la interacción de las víctimas.

Se ha considerado que BlueKeep es una amenaza tan grave que desde su descubrimiento, Microsoft e incluso agencias gubernamentales como la NSA y GCHQ, han estado alentando de forma continua a los usuarios y administradores de Windows a aplicar parches de seguridad antes de que los piratas informáticos se apoderen de sus sistemas.

Incluso muchas compañías de seguridad e investigadores individuales de seguridad cibernética que desarrollaron con éxito un exploit totalmente funcional para BlueKeep, se comprometieron a no lanzarlo al público por un bien mayor, especialmente porque casi un millón de sistemas se encontraron vulnerables aún después de un mes del lanzamiento de los parches.

Por esta razón, los piratas informáticos aficionados tardaron casi seis meses en encontrar un exploit BlueKeep que aún no es confiable y ni siquiera tiene un componente que se pueda eliminar.

El exploit BlueKeep extiene malware de criptomonedas

La explotación de BlueKeep en la naturaleza fue especulada por primera vez por Kevin

Beaumont el sábado cuando sus múltiples sistemas de honeypot EternalPot RDP, se bloquearon y se reiniciaron de pronto.

- 

Marcus Hutchins, el investigador que ayudó a detener la propagación del ransomware WannaCry en 2017, analizó los volcados de memoria compartidos por Beaumont y confirmó *«artefactos BlueKeep en la memoria y el código de shell para lanzar un minero de Monero».*

> *«Finalmente, confirmamos que este segmento apunta a un shellcode ejecutable. En este punto, podemos afirmar intentos válidos de explotación de BlueKeep en la naturaleza, con un shellcode que incluso coincide con el del shellcode en el módulo BlueKeep Metasploit!»*, dijo Hutchins en su blog.

El exploit contiene comandos codificados de PowerShell como la carga útil inicial, que luego descarga el binario ejecutable malicioso final de un servidor remoto controlado por el atacante y lo ejecuta en los sistemas de destino.

Según el servicio de VirusTotal de Google, el binario malicioso es un malware de criptomonedas que extrae Monero (XMR) utilizando la potencia informática de los sistemas infectados para generar ingresos para los atacantes.

Hutchins confirmó que el malware propagado por este exploit BlueKeep no contiene ninguna capacidad de propagación automática para saltar sin ayuda de una computadora a otra.

A diferencia de esto, parece que los atacantes desconocidos primero escanean Internet para encontrar sistemas vulnerables y luego los explotan.

Sin un componente susceptible de gusano, los atacantes solo podrían comprometer los

sistemas vulnerables que están conectados directamente a Internet, pero no aquellos que están conectados internamente y son accesibles desde ellos.

Aunque los hackers sofisticados ya podrían haber estado explotando la falla BlueKeep para comprometer de forma sigilosa a las víctimas, la falla aún no se ha explotado a mayor escala, como WannaCry o NotPetya.

Sin embargo, hasta ahora no está claro cuántos sistemas vulnerables de Windows BlueKeep se han visto comprometidos en los últimos ataques cibernéticos para implementar el minero Monero.

Si no puedes actualizar tus sistemas vulnerables o los de tu organización, puedes tomar en cuenta las siguientes mitigaciones:

- Deshabilitar los servicios RDP, si no son necesarios.
- Bloquear el puerto 3389 utilizando un firewall o hacer accesible por medio de una VPN privada.
- Habilitar la autenticación de nivel de red (NLA): Es una mitigación parcial para evitar que cualquier atacante no autenticado explote esta falla wormable.