Investigadores de seguridad cibernética descubrieron una nueva variante de WatchBog, una red de bots de malware basada en la minería de criptomonedas en Linux, que ahora también incluye un módulo para explorar Internet en busca de servidores RDP de Windows vulnerables a la falla BlueKeep.

BlueKeep es una vulnerabilidad de ejecución remota de código altamente crítica, con módulos de gusano, vulnerable en los Servicios de Escritorio Remoto de Windows, que podría permitir que un hacker remoto no autenticado tome el control total de los sistemas vulnerables con tan solo enviar solicitudes especialmente diseñadas por medio del protocolo RDP.

Aunque los parches para la vulnerabilidad de BlueKeep (CVE-2019-0708) ya fueron lanzados por Microsoft en mayo de este año, más de 800 mil máquinas con Windows a las que se puede acceder por medio de Internet siguen siendo vulnerables a esta falla.

Afortunadamente, aún después de que muchas personas en la comunidad de seguridad desarrollaron explotaciones remotas de código de trabajo para BlueKeep, no existe ninguna vulnerabilidad pública de prueba de concepto (PoC) disponible hasta ahora, lo que posiblemente impida que hackers oportunistas causen estragos.

Sin embargo, la empresa de ciberseguridad Immunity lanzó ayer una versión actualizada de su herramienta comercial automatizada de evaluación de vulnerabilidades y pruebas de penetración (VAPT), CANVAS 7.23, que incluye un nuevo módulo para el exploit de BlueKeep RDP.

Parece que los atacantes detrás de WatchBog están utilizando su red de botnets para preparar *«una lista de sistemas vulnerables para atacar en el futuro o vender a terceros para obtener ganancias»,* dijeron los investigadores de Intezer Lab, que descubrieron la variante de WatchBog.

> *«La incorporación del escáner BlueKeep por una botnet de Linux puede indicar que*

> *WatchBog está comenzando a explotar oportunidades financieras en una plataforma diferente»*, dijeron los investigadores.

El escáner BlueKeep incluido en WatchBog escanea Internet y luego envía la lista de hosts RDP recién descubiertos, como una cadena de datos hexadecimal cifrada mediante RC4, a los servidores controlados por el atacante.

Según el investigador, la nueva variante WatchBog ya ha comprometido más de 4,500 máquinas Linux en los últimos dos meses.

Aunque WatchBog está operando desde fines del año pasado, los atacantes están distribuyendo su nueva variante en una campaña en curso que está activa desde inicios de junio de este año.

La variante WatchBog recién descubierta incluye un nuevo módulo de expansión junto con vulnerabilidades para algunas fallas recientemente parcheadas en las aplicaciones de Linux, lo que permite a los atacantes encontrar y comprometer más sistemas Linux rápidamente.

La botnet WatchBog para Linux contiene varios módulos, como se explica estructuralmente a continuación, que aprovechan las vulnerabilidades recientemente parcheadas en las aplicaciones Exim, Jira, Solr, Jenkins, ThinkPHP y Nexus para comprometer las máquinas Linux.

Módulo PWN

- CVE-2019-11581 (Jira)
- CVE-2019-10149 (Exim)
- CVE-2019-0192 (Solr)
- CVE-2019-1000861 (Jenkins)
- CVE-2019-7238 (Nexus Repository Manager 3)

Módulo Scanning

- BlueKeep Scanner
- Jira Scanner
- Solr Scanner

Módulo de fuerza bruta

- Instancias CouchDB
- Instancias Redis

Módulo de extensión

- Apache ActiveMQ (CVE-2016-3088)
- Solr (CVE-2019-0192)
- Code Execution over Redis

Después de que los módulos de escaneo y fuerza bruta descubren una máquina Linux que ejecuta la aplicación vulnerable, WatchBog implementa una secuencia de comandos en la máquina seleccionada para descargar los módulos de mineros de Monero del sitio web de Pastebin.

El script malicioso también gana persistencia en el sistema infectado por medio de crontab y descarga un nuevo módulo separador, que viene en forma de un ejecutable ELF compilado de Cython vinculado dinámicamente.

Los investigadores recomendaron a los administradores de Linux y Windows que mantengan su software y sistemas operativos actualizados contra las vulnerabilidades conocidas para evitar ser víctimas de dichas campañas de ataque.

Puedes saber si WatchBog infectó tu sistema Linux comprobando la existencia del archivo *«/tmp/.tmplassstgggzzzqpppppp12233333»* o *«/tmp/.gooobb».*