Investigadores de seguridad descubrieron una campaña de botnets sofisticada trabajando en curso, que utiliza fuerza bruta con más de 1.5 millones de servidores RDP de Windows de acceso público en Internet.

GoldBrute es el nombre que se le dio al esquema de botnets, que se diseñó para escalar gradualmente agregando cada nuevo sistema crackeado a su red, obligándolos a encontrar nuevos servidores RDP disponibles y luego a la fuerza bruta.

Para evadir las herramientas de seguridad y a los analistas de malware, los atacantes detrás de la campaña ordenan a cada máquina infectada que se dirija a millones de servidores con un conjunto único de combinación de nombre de usuario y contraseña para que un servidor específico reciba intentos de fuerza bruta de diferentes direcciones IP.

La campaña fue descubierta por Renato Mainho en Morphus Labs, funciona como se puede observar en la siguiente imagen:

Paso 1: Después de forzar con éxito un servidor RDP, el atacante instala en la máquina un malware botnet GoldBrute, basado en Java.

Paso 2: Para controlar las máquinas infectadas, los atacantes utilizan un servidor de control y comando fijo y centralizado, que intercambia comandos y datos por medio de una conexión WebSocket encriptada AES.

Paso 3 y 4: Cada máquina infectada recibe su primera tarea para analizar e informar una lista de al menos 80 nuevos servidores RDP de acceso público que pueden ser forzados por fuerza bruta.

Paso 5 y 6: Los atacantes asignan a cada máquina infectada un conjunto único de combinación de nombre de usuario y contraseña como su segunda tarea, obligándolos a intentarlo contra la lista de objetivos RDP que el sistema infectado recibe continuamente del servidor C&C.

Paso 7: En los intentos exitosos, la máquina infectada reporta las credenciales de inicio de sesión al servidor de C&C.

En este momento, no está claro exactamente cuántos servidores RDP ya se han visto comprometidos y participando en los ataques de fuerza bruta contra otros servidores RDP en Internet.

Una búsqueda rápida en Shodan mostró que se puede acceder a cerca de 2.4 millones de servidores RDP en Windows en Internet, y probablemente más de la mitad de ellos estén recibiendo intentos de fuerza bruta.

El Protocolo de Escritorio Remoto (RDP) apareció recientemente en las noticias por dos nuevas vulnerabilidades de seguridad, una que fue reparada por Microsoft y la otra que sigue sin arreglarse.

La vulnerabilidad que fue parcheada y apodada como BlueKeep (CVE-2019-0708), es un defecto que puede hacer que los atacantes remotos tomen el control de los servidores RDP, y en caso de que se explote con éxito, podría causar daños en todo el mundo, potencialmente mucho peor que los casos de WannaCry y NotPetya.

La vulnerabilidad sin parches reside en Windows y permitiría a los hackers del lado del cliente, eludir la pantalla de bloqueo en las sesiones de escritorio remoto.