Los actores de amenazas están explotando las vulnerabilidades de seguridad en los programas de escritorio remoto como Sunlogin y AweSun para implementar el malware PlugX.

AhnLab Security Emergency Response Center (ASEC), en un nuevo análisis, dijo que se está marcando el abuso continuo de las vulnerabilidades para entregar una variedad de cargas útiles en sistemas comprometidos.

Esto incluye el marco de trabajo posterior a la explotación de Sliver, el minero de criptomonedas XMRig, Gh0st RAT y el ransomware Paradise. PlugX es la última incorporación a la lista.

Los hackers con sede en China utilizan ampliamente el malware modular, y se agregan continuamente nuevas funciones para ayudar a realizar el control del sistema y el robo de información.

En los ataques observador pos ASEC, la explotación exitosa de las vulnerabilidades es seguida por la ejecución de un comando de PowerShell que recupera un ejecutable y un archivo DLL de un servidor remoto.

Este ejecutable es un servicio de servidor HTTP legítimo de la empresa de seguridad cibernética ESET, que se usa para cargar el archivo DLL mediante una técnica llamada carga lateral de DLL y, en última instancia, ejecuta la carga útil de PlugX en la memoria.

> *«Los operadores de PlugX usan una gran variedad de binarios confiables que son vulnerables a la carga lateral de DLL, incluyendo numerosos ejecutables de antivirus. Se ha demostrado que esto es efectivo al infectar a las víctimas»*, dijo Security Joes.

La backdoor también se destaca por su capacidad para iniciar servicios arbitrarios, descargar y ejecutar archivos desde una fuente externa y soltar complementos que pueden recopilar

datos y propagarse mediante el Protocolo de Escritorio Remoto (RDP).

> *«Se están agregando nuevas funciones incluso hasta el día de hoy, ya que continúa viendo un uso constante en los ataques. Cuando se instala la puerta trasera, PlugX, los acores de amenazas pueden obtener el control del sistema infectado sin el conocimiento del usuario».*