Investigadores de seguridad descubrieron una pieza de spyware de Linux que actualmente no se ha detectado completamente en todos los principales productos de software de seguridad antivirus, mismo que incluye funcionalidades que se han visto muy rara vez con respecto a la mayoría de malware para Linux.

Aunque no existen muchas muestras de malware para Linux, en comparación con Windows, una gran cantidad de malware que se enfoca en el entorno Linux se centra principalmente en los ataques de minería de datos de criptomonedas para obtener ganancias financieras y crear botnets para realizar ataques DDoS mediante el secuestro de servidores vulnerables.

Sin embargo, los investigadores de la compañía de seguridad Intezer Labs, descubrieron recientemente un nuevo implante de backdoor en Linux que al parecer está en fase de desarrollo y prueba, pero ya incluye varios módulos maliciosos para espiar a usuarios de escritorio de Linux.

EvilGnome: Nuevo spyware para Linux

Nombrado como EvilGnome, el malware fue diseñado para tomar capturas de pantalla de escritorio, robar archivos, capturar grabaciones de audio desde el micrófono del usuario, además de descargar y ejecutar más módulos maliciosos de segunda etapa.

De acuerdo con un nuevo informe que Intezer Labs compartió con The Hacker News antes de su lanzamiento, la muestra de EvilGnome que se descubrió en VirusTotal también contiene una funcionalidad de keylogger inacabada, lo que indica que su desarrollador lo pudo haber cargado en línea por error.

EvilGnome se disfraza como una extensión legítima de GNOME, un programa que permite a los usuarios de Linux ampliar la funcionalidad de sus escritorios.

Según los investigadores, el implante se entrega en forma de un script de shell de archivo auto extraíble creado con «makeelf», un script de shell pequeño que genera un archivo comprimido tar auto extraíble.

El implante de Linux también gana persistencia en un sistema específico utilizando crontab, similar al programador de tareas de Windows, y envía datos de usuario robados a un servidor remoto controlado por un atacante.

> *«La persistencia se logra registrando gnome-shell-ext.sh para ejecutar cada minuto en crontab. Finalmente, el script ejecuta gnome-shell-ext.sh, que a su vez landa el principal ejecutable gnome-shell-ext»,* dijeron los investigadores.

Módulos de spyware de EvilGnome

El Spy Agent de EvilGnome contiene cinco módulos maliciosos, llamados *«shooters»,* que se explican a continuación:

- ShooterSound: Este módulo utiliza PulseAudio para capturar el audio del micrófono del usuario y carga los datos recabados en el servidor de control y comando del atacante.
- ShooterImage: Este módulo utiliza la biblioteca de código abierto de Cairo para crear capturas de pantalla y cargarlas en el servidor de C&C. Esto al abrir una conexión con el servidor de visualización XOrg, que es el backend del escritorio de Gnome.
- ShooterFile: Este módulo utiliza una lista de filtros para escanear el sistema de archivos en buscar de archivos recién creados y los carga en el servidor de C&C.
- ShooterPing: Este módulo recibe nuevos comandos del servidor de C&C, como la descarga y ejecución de nuevos archivos, establecer nuevos filtros para el escaneo de archivos, descargar y establecer una nueva configuración de tiempo de ejecución, exfiltrar la salida almacenada al servidor de C&C y detener la ejecución de cualquier módulo de disparo.
- ShooterKey: Este módulo no está implementado, por lo que probablemente es un módulo de registro de pulsaciones de teclado sin terminar.

Particularmente, todos los módulos anteriores cifran sus datos de salida y descifran los comandos recibidos del servidor de C&C con la clave RC5 *«sdg62_AS.sa $ die3»*, utilizando una versión modificada de una biblioteca de código abierto rusa.

Posible conexión de EvilGnome con el grupo de hackers Gamaredon

Por otro lado, los investigadores también encontraron conexiones entre EvilGnome y Gamaredon Group, un presunto grupo de hackers ruso que ha estado activo desde al menos 2013 y se ha dirigido a personas que trabajan con el gobierno ucraniano.

Similitudes entre EvilGnome y Gamaredon Group

EvilGnome utiliza un proveedor de hosting que ha sido utilizado por Gamaredon Group durante años y sigue siendo utilizado por ellos hasta ahora.

Se descubrió que EvilGnome también opera en una dirección IP controlada por el grupo Gamaredon hace dos meses.

Los atacantes EvilGnome también están utilizando el TTLD *'.space'* para sus dominios, al igual que el grupo Gamaredon.

EvilGnome emplea técnicas y módulos, como el uso de SFX, la persistencia con el programador de tareas y la implementación de herramientas de robo de información, que se asemejan las herramientas de Windows del grupo Gamaredon.

¿Cómo detectar el malware EvilGnome?

Para verificar si tu sistema Linux está infectado con el spyware EvilGnome, puedes buscar el ejecutable *«gnome-shell-ext»* en el directorio *«~/.cache/gnome-software/gnome-shell-extensions».*

> *«Creemos que esta es una versión de prueba prematura. Anticipamos que se descubran y revisen versiones más nuevas en el futuro, lo que potencialmente podría arrojar más luz sobre las operaciones del grupo»,* dijeron los investigadores.

Ya que los productos de seguridad y antivirus actualmente no detectan el malware EvilGnome, los investigadores recomiendan a los usuarios de Linux que bloqueen las direcciones IP de Comando y Control enumeradas en la sección IOC de la publicación del blog de Intezer.