Una nueva botnet con gusanos que se propaga a través de GitHub y Pastebin para instalar mineros de criptomonedas y puertas traseras en sistemas de destino, ha regresado con capacidades ampliadas para comprometer aplicaciones web, cámaras IP y enrutadores.

A inicios del mes pasado, los investigadores de Juniper Threat Labs, documentaron una campaña de minería de cifrado denominada Gitpaste-12, que utilizaba GitHub para alojar código malicioso que contenía hasta 12 módulos de ataque conocidos que se ejecutan mediante comandos descargados de una URL de Pastebin.

Los ataques ocurrieron durante un período de 12 días a partir del 15 de octubre de 2020, antes de que tanto la URL de Pastebin como el repositorio se cerraran el 30 de octubre de 2020.

Ahora, según Juniper, la segunda ola de ataques comenzó el 10 de noviembre, utilizando cargas útiles de un repositorio de GitHub diferente, que entre otros, contiene un cripto minero de Linux («ls»), un archivo con una lista de contraseñas para fuerza bruta y un exploit de escalamiento de privilegios local para sistemas Linux x86_64.

La infección inicial ocurre a través de X10-unix, un binario escrito en el lenguaje de programación Go, que procede a descargar las cargas útiles de la siguiente etapa desde GitHub.

> *«El gusano lleva a cabo una amplia serie de ataques dirigidos a aplicaciones web, cámaras IP, enrutadores y más, que comprenden al menos 31 vulnerabilidades conocidas, siete de las cuales también se observaron en la muestra anterior de Gitpaste-12, así como intentos de comprometer la apertura Android Debuge Bridge Connections y backdoors de malware existentes»,* dijo el investigador de Juniper, Asher Langton.

En la lista de 31 vulnerabilidades, se incluyen fallas de código remoto en la interfaz de usuario de administración de tráfico F5 BIG-IP (CVE-2020-5902), Pi-hole (CVE-2020-8816), Tenda AC15 AC1900 (CVE-2020-10987) y vBulletin (CVE-2020-17496), además de un error de inyección SQL en FUEL CMS (CVE-2020-17463), todos los cuales, salieron a la luz este año.

Cabe mencionar que Ttint, una nueva variante de la botnet Mirai, se observó en octubre utilizando dos vulnerabilidades de día cero del enrutador Tenda, incluida CVE-2020-10987, para propagar un troyano de acceso remoto capaz de llevar a cabo ataques de denegación de servicio, ejecutar comandos maliciosos e implementar un shell inverso para acceso remoto.

Además de instalar X10-unix y el software de minería de Monero en la máquina, el malware también abre una puerta trasera que escucha en los puertos 30004 y 30005, carga la dirección IP externa de la víctima en un Pastebin privado e intenta conectarse a las conexiones de Android Debug Bridge en el puerto 5555.

En una conexión exitosa, se descarga un archivo APK de Android («weixin.apk»), que finalmente instala una versión ARM CPU de X10-unix.

Hasta ahora, se han detectado al menos 100 huéspedes distintos propagando la infección, según las estimaciones de los investigadores.

Se puede encontrar aquí el conjunto completo de binarios maliciosos y otros indicadores de compromiso (IoC) relevantes asociados con la campaña, para fines de investigación.