FireEye y Microsoft informaron este jueves que descubrieron tres cepas de malware más en relación con el ataque a la cadena de suministro de SolarWinds, incluyendo una *«puerta trasera sofisticada de segunda etapa»,* ya que la investigación sobre la campaña de espionaje en expansión continúa brindando nuevas pistas sobre las tácticas del actor de amenazas y técnicas.

Nombrado como GoldMax (también conocido como SUNSHUTTLE), GoldFinder y Sibot, el nuevo conjunto de malware se suma a una lista creciente de herramientas maliciosas como Sunspot, Sunburst, Teardrop y Raindrop, que fueron entregadas sigilosamente a las redes empresariales por supuestos operativos rusos.

> *«Estas herramientas son nuevas piezas de malware que son exclusivas de este actor. Están hechos a medida para redes específicas y se evalúa su introducción luego de que el actor haya obtenido acceso a través de credenciales comprometidas o el binario SolarWinds y después de moverse lateralmente con Teardrop y otras acciones prácticas del teclado»,* dijo Microsoft.

La compañía también nombró al actor de amenazas detrás de los ataques contra SolarWinds como NOBELIUM, que también está siendo rastreado bajo distintos apodos por la comunidad de ciberseguridad, incluidos UNC2454 (FireEye), SolarStorm (Palo Alto Unit 42), StellarParticle (CrowdStrike) y Dark Halo (Volexidad).

Aunque Sunspot se implementó en el entorno de construcción para inyectar la puerta trasera Sunburst en la plataforma de monitoreo de red Orion de SolarWinds, Teardrop y Raindrop se han utilizado principalmente como herramientas posteriores a la explotación para moverse lateralmente a través de la red y entregar Cobalt Strike Beacon.

Detectado entre agosto y septiembre e 2020, SUNSHUTTLE es un malware basado en Golang

que actúa como una puerta trasera de comando y control, estableciendo una conexión segura con un servidor controlado por el atacante para recibir comandos para descargar y ejecutar archivos, cargar archivos desde el sistema a servidor y ejecute los comandos del sistema operativo en la máquina comprometida.

Por su parte, FireEye dijo que observó el malware en una víctima comprometida por UNC2452, pero agregó que no ha podido verificar completamente la conexión de la puerta trasera con el actor de la amenaza. La compañía también declaró que describió SUNSHUTTLE en agosto de 2020 luego de que una entidad anónima con sede en Estados Unidos lo cargara en un repositorio público de malware.

Una de las características más notables de GoldMax es poder ocultar su tráfico de red malicioso con tráfico aparentemente benigno mediante la selección pseudoaleatoria de referencias de una lista de URL de sitios web popuylares (como Bing, Yahoo, Facebook, Twitter, Google, etc.) para solicitudes HTTP GET de señuelo que apuntan a dominios C2.

> *«La nueva puerta trasera SUNSHUTTLE es una backdoor sofisticada de segunda etapa que demuestra técnicas de evasión de detección sencillas pero elegantes a través de sus capacidades de tráfico integradas para comunicaciones C2. SUNSHUTTLE funcionaría como una puerta trasera de segunda etapa en tal compromiso para realizar el reconocimiento de la red junto con otras herramientas relacionadas con Sunburst»,* dijo FireEye.

GoldFinder, también escrito en Go, es una herramienta de rastreo HTTP para registrar la ruta que toma un paquete para llegar a un servidor C2. Por el contrario, Sibot es un malware de doble propósito implementado en VBScript, que está diseñado para lograr la persistencia en las máquinas infectadas antes de descargar y ejecutar una carga útil desde el servidor C2. Microsoft dijo que logró observar tres variantes ofuscadas de Sibot.

Incluso cuando las diferentes piezas del rompecabezas de ataque de SolarWinds encajan en su lugar, el desarrollo una vez más subraya el alcance y la sofisticación en la gama de métodos utilizados para penetrar, propagarse y persistir en los entornos de las víctimas.

> *«Estas capacidades difieren de las herramientas y patrones de ataque NOBELIUM previamente conocidos, y reiteran la sofisticación del actor. En todas las etapas del ataque, el actor demostró un profundo conocimiento de las herramientas de software, las implementaciones, el software y los sistemas de seguridad comunes en las redes, y las técnicas utilizadas con frecuencia por los equipos de respuesta a incidentes»*, dijo la compañía.