El grupo de hackers detrás del compromiso de la cadena de suministro de SolarWinds siguió ampliando su arsenal de malware con nuevas herramientas y técnicas que se implementaron en ataques en 2019, una vez indicativos de la naturaleza esquiva de las campañas y la capacidad del adversario para mantener el acceso persistente por años.

Según la compañía de seguridad cibernética CrowdStrike, que detalló las tácticas novedosas adoptadas por el grupo de hacking Nobelium la semana pasada, se colocaron dos familias de malware sofisticado en los sistemas de las víctimas, una variante de Linux de GoldMax y un nuevo implante denominado TrailBlazer, mucho antes de que llegara la escala de los ataques a la luz.

Nobelium, el apodo asignado por Microsoft para la intrusión de SolarWinds en diciembre de 2020, también es rastreado por la comunidad de ciberseguridad más amplia con los nombres UNC2452 (FireEye), SolarStorm (Unit 42), StellarParticle (CrowdStrike), Dark Halo (Volexity) y Iron Ritual (SecureWorks).

Desde entonces, las actividades maliciosas se han atribuido a un actor patrocinado por el estado ruso llamado APT29 (también conocido como The Dukes y Cozy Bear), una operación de ciberespionaje asociada con el Servicio de Inteligencia Exterior del país que se sabe que está activa desde al menos 2008.

GoldMax (también conocido como SUNSHUTTLE), que fue descubierto por Microsoft y FireEye en marzo de 2021, es un malware basado en Golang que actúa como una puerta trasera de comando y control, estableciendo una conexión segura con un servidor remoto para ejecutar comandos arbitrarios en la máquina comprometida.

En septiembre de 2021, Kaspersky reveló detalles de una segunda variante de la backdoor GoldMax llamada Tomiris, que se implementó contra varias organizaciones gubernamentales en un estado miembro no identificado de la CEI en diciembre de 2020 y enero de 2021.

La última iteración es una implementación de Linux previamente indocumentada pero funcionalmente idéntica del malware de segunda etapa que se instaló en los entornos de las

víctimas a mediados de 2019, anterior a todas las demás muestras identificadas creadas para la plataforma Windows hasta ahora.

También se entregó en el mismo período TrailBlazer, una puerta trasera modular que ofrece a los atacantes un camino hacia el espionaje cibernético, al mismo tiempo que comparte puntos en común con GoldMax en la forma en que enmascara su tráfico de comando y control (C2) como solicitudes HTTP legítimas de notificaciones de Google.

Otros canales poco comunes utilizados por el actor para facilitar los ataques incluyen:

- Salto de credenciales para oscurecer el movimiento lateral
- Secuestro, suplantación y manipulación de aplicaciones y entidades de servicio de Office 365 (O365)
- Robo de cookies del navegador para eludir la autenticación multifactor

Además, los operadores llevaron a cabo múltiples instancias de robo de credenciales de dominio con meses de diferencia, cada vez que aprovecharon una técnica diferente, una de ellas fue el uso del ladrón de contraseñas Mimikatz en memoria, desde un host ya comprometido para garantizar el acceso por períodos prolongados de tiempo.

> *«La campaña StellarParticle, asociada con el grupo de adversario Cozy Bear, demuestra el amplio conocimiento de este actor de amenazas de los sistemas operativos Windows y Linux, Microsoft Azure, O365 y Active Directory, y su paciencia y conjunto de habilidades encubiertas para pasar desapercibido durante meses, y en algunos casos, año*s», dijeron los investigadores.