Un malware de alta sofisticación que se camufla como un minero de criptomonedas ha conseguido evadir la detección durante más de cinco años, infectando más de un millón de dispositivos en todo el mundo en el proceso.

Esto según las conclusiones de Kaspersky, que ha bautizado la amenaza como StripedFly, describiéndola como un *«intrincado marco modular que es compatible tanto con sistemas Linux como con Windows».*

El proveedor ruso de ciberseguridad, que detectó las muestras por primera vez en 2017, afirmó que este minero forma parte de una entidad mucho más grande que utiliza un exploit personalizado del SMBv1 EternalBlue, atribuido al Equation Group, para infiltrarse en sistemas de acceso público.

El código malicioso, entregado a través del exploit, tiene la capacidad de descargar archivos binarios desde un repositorio remoto en Bitbucket y ejecutar scripts de PowerShell. Además, dispone de una colección de características expandibles similares a complementos para recopilar datos sensibles e incluso desinstalarse.

Este código malicioso se inyecta en el proceso wininit.exe, un proceso de Windows legítimo que se inicia mediante el administrador de arranque (BOOTMGR) y maneja la inicialización de diversos servicios.

> *«La carga útil del malware está estructurada como un código binario monolítico diseñado para admitir módulos enchufables que permiten extender o actualizar su funcionalidad»,* señalaron los investigadores de seguridad Sergey Belov, Vilen Kamalov y Sergey Lozhkin en un informe técnico publicado la semana pasada.

> *«Viene con un túnel de red TOR incorporado para la comunicación con servidores de comandos, junto con funcionalidad de actualización y entrega a través de servicios confiables como GitLab, GitHub y Bitbucket, todos utilizando archivos cifrados*

> *personalizados».*

Otros módulos de espionaje notables permiten recopilar credenciales cada dos horas, tomar capturas de pantalla en el dispositivo de la víctima sin ser detectado, grabar la entrada del micrófono y establecer un proxy inverso para ejecutar acciones remotas.

Una vez que el malware se ha establecido con éxito, procede a deshabilitar el protocolo SMBv1 en el host infectado y a propagar el malware a otras máquinas mediante un módulo de gusano a través de SMB y SSH, utilizando claves recopiladas en los sistemas hackeados.

StripedFly logra la persistencia ya sea mediante la modificación del Registro de Windows o la creación de entradas en el programador de tareas si el intérprete de PowerShell está instalado y se dispone de acceso administrativo. En Linux, la persistencia se logra mediante un servicio de usuario systemd, un archivo .desktop que se inicia automáticamente o mediante la modificación de archivos /etc/rc*, profile, bashrc o inittab.

También se descarga un minero de criptomonedas Monero que utiliza solicitudes de DNS sobre HTTPS (DoH) para resolver los servidores de la piscina, añadiendo una capa adicional de sigilo a las actividades maliciosas. Se ha evaluado que el minero se utiliza como señuelo para evitar que el software de seguridad descubra la verdadera capacidad del malware.

Con el fin de minimizar la huella, los componentes del malware que se pueden descargar se alojan como binarios cifrados en diversos servicios de alojamiento de repositorios de código, como Bitbucket, GitHub o GitLab.

Por ejemplo, el repositorio de Bitbucket operado por el actor de amenazas desde junio de 2018 incluye archivos ejecutables capaces de servir la carga útil inicial de infección en Windows y Linux, buscar nuevas actualizaciones y, en última instancia, actualizar el malware.

La comunicación con el servidor de comando y control (C2), que está alojado en la red TOR, se lleva a cabo mediante una implementación personalizada y ligera de un cliente TOR que

no se basa en ningún método públicamente documentado.

> *«El nivel de dedicación demostrado por esta funcionalidad es notable. El objetivo de ocultar el servidor C2 a toda costa impulsó el desarrollo de un proyecto único y que consume mucho tiempo: la creación de su propio cliente TOR»*, afirmaron los investigadores.

Otra característica destacada es que estos repositorios actúan como mecanismos de respaldo para que el malware descargue los archivos de actualización cuando su fuente principal (es decir, el servidor C2) no responde.

Kaspersky también descubrió una familia de ransomware llamada ThunderCrypt que comparte importantes similitudes de código fuente con StripedFly, a excepción del módulo de infección SMBv1. Se dice que ThunderCrypt se utilizó contra objetivos en Taiwán en 2017.

Los orígenes de StripedFly siguen siendo desconocidos en la actualidad, aunque la sofisticación de este marco y sus similitudes con EternalBlue muestran todas las características de un actor de amenazas persistentes avanzado (APT).

Cabe señalar que, aunque la filtración del exploit EternalBlue por parte de Shadow Brokers ocurrió el 14 de abril de 2017, la versión identificada más temprana de StripedFly que incorpora EternalBlue data de un año atrás, el 9 de abril de 2016. Desde la filtración, el exploit de EternalBlue ha sido reutilizado por grupos de piratería norcoreanos y rusos para difundir el malware WannaCry y Petya.

Dicho esto, también hay indicios de que grupos de piratería informática chinos podrían haber tenido acceso a algunos de los exploits del Equation Group antes de que fueran filtrados en línea, como reveló Check Point en febrero de 2021.

Kaspersky afirmó que las similitudes con el malware asociado al Equation Group también se reflejan en el estilo de programación y prácticas que se asemejan a las observadas en

STRAITBIZARRE (SBZ), otra plataforma de espionaje cibernético utilizada por el supuesto colectivo adversario vinculado a Estados Unidos.

Este desarrollo ocurre casi dos años después de que los investigadores del laboratorio Pangu de China detallaran un backdoor de *«máximo nivel»* llamado Bvp47, que supuestamente fue utilizado por el Equation Group en más de 287 objetivos en varios sectores de 45 países.

No cabe duda de que un aspecto esencial de la campaña que sigue siendo un enigma, salvo para quienes diseñaron el malware, es su verdadero propósito.

> *«A pesar de que el ransomware ThunderCrypt sugiere un motivo comercial por parte de sus creadores, plantea la pregunta de por qué no optaron por un camino potencialmente más lucrativo»,* señalaron los investigadores.

> *«Es difícil aceptar la idea de que un malware tan sofisticado y diseñado de manera profesional tenga un propósito tan insignificante, teniendo en cuenta todas las pruebas en sentido contrario».*