Según la última investigación de la compañía de seguridad cibernética SentinelOne, el ciberataque dirigido a Viasat que desconectó temporalmente los módems KS-SAT el 24 de febrero de 2022, el mismo día en que las fuerzas militares rusas invadieron Ucrania, fue consecuencia de un malware de limpieza.

Los hallazgos de limpieza se producen cuando la compañía de telecomunicaciones de Estados Unidos reveló que fue el objetivo de un ataque cibernético multifacético y deliberado contra su red KA-SAT, vinculándolo a una *«intrusión en la red basada en tierra por parte de un atacante que explota una configuración incorrecta en un dispositivo VPN para obtener acceso remoto al segmento de gestión de confianza de la red KA-SAT».*

Al obtener acceso, el atacante emitió *«comandos destructivos»* en decenas de miles de módems pertenecientes al servicio de banda ancha satelital que *«sobrescriben datos clave en la memoria flash de los módems, haciendo que los módems no pudieran acceder a la red, pero no permanentemente inutilizables».*

SentinelOne dijo que descubrió una nueva pieza de malware llamada *«ukrop»* el 15 de marzo, que proyecta todo el incidente bajo una nueva luz: un compromiso de la cadena de suministro del mecanismo de gestión KA-SAT para entregar el limpiaparabrisas, denominado AcidRain, a los módems y enrutadores y lograr una disrupción escalable.

AcidRain está diseñado como un ejecutable MIPS ELF de 32 bits que *«realiza un borrado en profundidad del sistema de archivos y varios archivos de dispositivos de almacenamiento conocidos. Si el código se ejecuta como raíz, AcidRain realiza una sobrescritura recursiva inicial y elimina los archivos no estándar en el sistema de archivos»,* dijeron los investigadores Juan Andres Guerrero-Saade y Max Van Amerongen.

Una vez que se completa el proceso de limpieza, el dispositivo se reinicia para dejarlo inoperable. Esto convierte a AcidRain en la séptima cepa de limpiaparabrisas descubierta desde inicios de año en relación con la guerra ruso-ucraniana después de WhisperGate, ShisperKill, HermeticWiper, IsaacWiper, CaddyWiper y DoubleZero.

Un análisis más detallado de la muestra del limpiador también descubrió una superposición de código *«interesante»* con un complemento de tercera etapa *«dstr»* utilizado en ataques que involucran una familia de malware llamada VPNFilter, que se ha atribuido al grupo Russian Sandworm (también conocido como Voodoo Bear).

A fines de febrero de 2022, el Centro Nacional de Seguridad Cibernética (NCSC) del Reino Unido, la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), la Agencia de Seguridad Nacional (NSA) y la Oficina Federal de Investigaciones (FBI) revelaron un sucesor de VPNFilter, llamando el marco de reemplazo Cyclops Blink.

Aún no está claro cómo los atacantes obtuvieron acceso a la VPN. En una declaración compartida con The Hacker News, Viasat confirmó que el malware de destrucción de datos se implementó en módems utilizando comandos de *«gestión legítima»,* pero se abstuvo de compartir más detalles al citar una investigación en curso.

La compañía declaró lo siguiente:

> *«Los hechos proporcionados ayer en el Informe de incidentes de Viasat son precisos. El análisis en el informe de SentinelLabs con respecto al binario 'ukrop' es consistente con los hechos de nuestro informe; específicamente, SentinelLabs identifica el ejecutable destructivo que se ejecutó en los módems utilizando un comando de administración legítimo como lo describió anteriormente Viasat.*
>
> *Como se indica en nuestro informe: «el atacante se movió lateralmente a través de esta red de administración confiable a un segmento de red específico utilizado para administrar y operar la red, y luego usó este acceso a la red para ejecutar comandos de administración legítimos y específicos en una gran cantidad de módems residenciales simultáneamente. .»*
>
> *Además, no vemos esto como un ataque o una vulnerabilidad en la cadena de suministro. Como señalamos, «Viasat no tiene evidencia de que el software de*

> *módem estándar o la distribución de firmware o los procesos de actualización involucrados en las operaciones normales de la red se hayan utilizado o comprometido en el ataque». Además, «no hay evidencia de que se haya accedido o comprometido ningún dato del usuario final».*
>
> *Debido a la investigación en curso y para garantizar la seguridad de nuestros sistemas frente a ataques continuos, no podemos compartir públicamente todos los detalles forenses del evento. A través de este proceso, hemos estado y continuamos cooperando con varias agencias gubernamentales y de aplicación de la ley de todo el mundo, que han tenido acceso a los detalles del evento.*
>
> *Esperamos poder proporcionar detalles forenses adicionales cuando se complete esta investigación».*