Cronología de Pacific Rim 2018-2024

4 DIC 2018

Ataque Cloud Snooper

Puerta trasera SSH y rootkit nuevos, cambio a los recursos en la nube, y primer uso de la técnica Señalización de tráfico: filtros de socket ATT&CK (T1205.002) para ocultar el tráfico de comunicaciones C2.

22 ABR 2020

Ataque Asnarök (CVE-2020-12271)

El ataque Asnarök utiliza la vulnerabilidad de inyección SQL (CVE-2020-12271) y ATT&CK T1059 para perpetrar un ataque masivo a dispositivos y desplegar un troyano.

24 ABR 2020

Dispositivo Asnarök identificado en Chengdu, China

Una búsqueda retrospectiva encuentra un dispositivo en Chengdu aparentemente utilizado para probar los exploits empleados en Asnarök.

17 JUN 2020

Ataque Bookmark (CVE-2020-15069)

Los atacantes comienzan a explotar la vulnerabilidad CVE-2020-15069, en combinación con un aumento de privilegios locales, para desplegar una shell web en dispositivos que usan un portal web orientado a la WAN mediante una red de anonimización.

9 JUL 2020

Implante desplegado en el dispositivo del desarrollador del exploit

Tras identificar con alta fiabilidad un dispositivo utilizado por el desarrollador del exploit, Sophos despliega un implante para recabar telemetría adicional.

14 JUL 2020

Identificado el dispositivo utilizado para desarrollar CVE-2020-15069

Se descubre el dispositivo (registrado con el nombre de "TStark") utilizado para desarrollar el exploit CVE-2020-15069 vinculado a la Universidad de Chengdu.

31 AGO 2020

Sophos presta asistencia a una organización tibetana tras el ciberataque chino

Sophos y Volexity asisten a una organización tibetana exiliada que ha sido atacada con herramientas encontradas diez días antes en el dispositivo TStark y otro malware vinculado a múltiples ciberdelincuentes chinos.

27 NOV 2020

Ataque de día cero a Cyberoam (CVE-2020-29574)

Dispositivos Cyberoam son atacados por el exploit de día cero CVE-2020-29574 para crear nuevas cuentas de administrador.

21 MAR 2022

Un investigador bajo seudónimo con base en China reclama una recompensa por detectar CVE-2022-1040

Un investigador de seguridad bajo seudónimo notifica a Sophos una vulnerabilidad de día cero (CVE-2022-1040) a través de un programa de recompensas por detectar errores, afirmando estar en Japón pero presentándola desde una dirección IP china. El exploit incluye un error de inyección de comandos en OpenSSL.

24 MAR 2022

Una búsqueda retroactiva detecta ataques CVE-2022-1040 antes de que se notificara el error

Una búsqueda retroactiva revela ataques CVE-2022-1040 contra una organización tibetana en el exilio y una agencia gubernamental antes de que se notificara el error.

2 ABR 2022

Sophos informa de un error en OpenSSL (CVE-2022-1292)

Sophos informa de un error en OpenSSL, al que se le asigna CVE-2022-1292.

15 AGO 2022

Un implante descubre un bootkit UEFI en desarrollo en un dispositivo en Chengdu

Se detecta un bootkit UEFI en desarrollo en un dispositivo adquirido por una organización en Chengdu. Sophos crea detecciones para el kit, pero nunca se llega a desplegar.

16 SEP 2022

Primeros ataques Covert Channels (CVE-2022-3236)

Sophos y Microsoft identifican un dispositivo vulnerado en una organización de servicios financieros que constituye el primer caso de un ataque Covert Channels (CVE-2022-3236).

17 MAY 2023

Se descubren ataques mediante enlaces al firmware de los dispositivos

Sophos detecta una shell remota con un enlace al firmware que permite la persistencia en un único dispositivo, instalado mediante credenciales de administrador vulneradas.

27 NOV 2023

Ataques que eluden el parche CVE-2022-3236 en firmware antiguo

El análisis de la actividad sospechosa revela que los atacantes burlan el parche CVE-2022-3236 con un ataque que solo funciona en versiones de firmware más antiguas.

Sophos X-Ops