Chronologie de Pacific Rim 2018-2024

4 DÉC 2018

Attaque Cloud Snooper

Nouvelle backdoor et rootkit SSH, pivot vers les ressources cloud, et première utilisation du Traffic Signaling : Socket Filters ATT&CK (T1205.002) pour dissimuler le trafic de communication C2.

22 AVR 2020

Attaque Asnarök (CVE-2020-12271)

L'attaque Asnarök utilise la vulnérabilité d'injection SQL (CVE-2020-12271) et ATT&CK T1059 pour effectuer une attaque de masse sur les appareils et déployer un Trojan.

24 AVR 2020

Appareil Asnarök identifié à Chengdu, en Chine

La rétro-chasse trouve un appareil à Chengdu apparemment utilisé pour tester les exploits utilisés dans Asnarök.

17 JUIN 2020

Attaque Bookmark (CVE-2020-15069)

Les attaquants commencent l'exploitation de CVE-2020-15069 associée à une élévation des privilèges locaux qui permet de déployer un shell web sur des appareils utilisant un portail web orienté WAN à l'aide d'un réseau d'anonymisation.

9 JUIL 2020

Implant déployé sur l'appareil du développeur de l'exploit

Après avoir identifié avec une grande certitude un appareil utilisé par le développeur de l'exploit, Sophos déploie un implant pour collecter des données télémétriques supplémentaires.

14 JUIL 2020

Appareil utilisé pour développer CVE-2020-15069 identifié

Découverte d'un appareil (enregistré sous le nom de « TStark ») utilisé pour développer l'exploit CVE-2020-15069 lié à l'université de Chengdu.

31 AOÛT 2020

Sophos apporte son aide après la cyberattaque chinoise contre une organisation tibétaine.

Sophos et Volexity assistent l'organisation tibétaine en exil ciblée avec des outils trouvés 10 jours plus tôt sur l'appareil TStark et d'autres malwares liés à de multiples acteurs chinois.

27 NOV 2020

Attaques zero-day Cyberoam (CVE-2020-29574)

Les appareils Cyberoam ciblés par l'exploit zero-day CVE-2020-29574 pour créer de nouveaux comptes admin.

21 MAR 2022

Un chercheur sous pseudonyme basé en Chine revendique le bounty CVE-2022-1040

Un chercheur en sécurité sous pseudonyme signale un zero-day (CVE-2022-1040) à Sophos via son programme de bug bounty, prétendant être au Japon mais le soumettant depuis une adresse IP chinoise. L'exploit inclut un bug d'injection de commande OpenSSL.

24 MAR 2022

La rétro-chasse trouve des attaques CVE-2022-1040 avant le signalement du bug

La rétro-chasse révèle des attaques CVE-2022-1040 antérieures au signalement du bug contre une organisation tibétaine en exil et une agence gouvernementale.

2 AVR 2022

Sophos signale un bug dans OpenSSL (CVE-2022-1292)

Sophos signale un bug dans OpenSSL, auquel est attribué le code CVE-2022-1292.

15 AOÛT 2022

Un implant découvre un bootkit UEFI en cours de développement sur un appareil à Chengdu

Un bootkit UEFI en cours de développement est découvert sur un appareil acheté par une organisation à Chengdu. Sophos crée des détections pour le kit, mais on ne le voit jamais déployé.

16 SEP 2022

Premières attaques Covert Channels (CVE-2022-3236)

Sophos et Microsoft identifient un appareil compromis dans une organisation de services financiers qui est la première instance d'une attaque Covert Channels (CVE-2022-3236).

17 MAI 2023

Découverte d'attaques par hooking du firmware des appareils

Sophos découvre un shell distant avec un hook de firmware permettant la persistance sur un seul appareil, installé à l'aide d'identifiants admin compromis.

27 NOV 2023

Attaques contournant le correctif CVE-2022-3236 sur des anciens firmwares

L'analyse d'activités suspectes révèle que des attaquants contournent le correctif CVE-2022-3236 avec une attaque qui ne fonctionne que sur les anciennes versions du firmware.

Sophos X-Ops