Cronologia di Pacific Rim 2018-2024

4 DIC 2018

Attacco Cloud Snooper

Nuovi backdoor e rootkit su SSH, con pivot verso le risorse cloud, e primo utilizzo della tecnica ATT&CK (T1205.002) "Traffic Signaling: Socket Filters" per nascondere il traffico delle comunicazioni C2

22 APR 2020

Attacco Asnarök (CVE-2020-12271)

L'attacco Asnarök sfrutta la vulnerabilità agli attacchi di SQL Injection (CVE-2020-12271) e la tecnica ATT&CK T1059 per sferrare attacchi di massa contro i dispositivi e distribuire trojan

24 APR 2020

Identificato dispositivo Asnarök a Chengdu, in Cina

Un threat hunting retroattivo individua a Chengdu un dispositivo che sembrerebbe essere stato impiegato per testare gli exploit usati in Asnarök

17 GIU 2020

Attacco Bookmark (CVE-2020-15069)

Gli hacker iniziano a sfruttare CVE-2020-15069 in una catena di attacco che include privilege escalation a livello locale, per distribuire web shell su dispositivi che eseguono un portale web connesso alla WAN attraverso una rete anonimizzante

9 LUG 2020

Impianto distribuito sul dispositivo dello sviluppatore di un exploit

Dopo aver identificato con un alto grado di sicurezza un dispositivo utilizzato dallo sviluppatore di un exploit, Sophos distribuisce un impianto per raccogliere ulteriori dati di telemetria

14 LUG 2020

Identificato dispositivo usato per sviluppare CVE-2020-15069

Individuazione del dispositivo (registrato a "TStark") utilizzato per sviluppare l'exploit CVE-2020-15069, collegato all'Università di Chengdu

31 AGO 2020

Sophos assiste un'organizzazione tibetana colpita da un cyberattacco cinese

Sophos e Volexity assistono un'organizzazione tibetana in esilio, colpita da strumenti individuati 10 giorni prima su un dispositivo controllato da TStark e altri malware collegati a diversi hacker cinesi

27 NOV 2020

Attacco zero-day contro Cyberoam (CVE-2020-29574)

I dispositivi Cyberoam vengono colpiti da un attacco zero-day che sfrutta CVE-2020-29574 per creare nuovi account di amministrazione

21 MAR 2022

Un ricercatore basato in Cina coperto da uno pseudonimo richiede il Bounty per CVE-2022-1040

Un ricercatore di sicurezza coperto da uno pseudonimo segnala un exploit zero-day (CVE-2022-1040) a Sophos nell'ambito del programma Bug Bounty, sostenendo di trovarsi in Giappone, ma comunicando da un indirizzo IP cinese. L'exploit include un bug che agisce tramite command injection in OpenSSL

24 MAR 2022

Un threat hunting retroattivo individua attacchi CVE-2022-1040 prima dell'invio dei bug

Un threat hunting retroattivo rivela la presenza di attacchi CVE-2022-1040 antecedenti all'invio di bug contro un'organizzazione tibetana in esilio e un ente governativo

2 APR 2022

Sophos segnala un bug di OpenSSL (CVE-2022-1292)

Sophos segnala un bug di OpenSSL, a cui viene assegnato il codice CVE-2022-1292

15 AGO 2022

Un impianto rivela un bootkit UEFI in fase di sviluppo su un dispositivo a Chengdu

Un bootkit UEFI in fase di sviluppo viene individuato su un dispositivo acquistato da un'organizzazione a Chengdu. Sophos crea rilevamenti per questo kit, ma non viene mai osservato in azione

16 SEP 2022

Primi attacchi covert channel (CVE-2022-3236)

Sophos e Microsoft identificano un dispositivo compromesso in un'organizzazione finanziaria, che risulta essere la prima istanza di un attacco covert channel (CVE-2022-3236)

17 MAG 2023

Individuati attacchi di hook del firmware sui dispositivi

Sophos individua una shell remota con un hook del firmware che consente la persistenza in un singolo dispositivo; viene installato utilizzando credenziali di amministrazione compromesse

27 NOV 2023

Gli attacchi eludono la patch CVE-2022-3236 sui firmware non aggiornati

Da analisi sulle attività sospette emerge che alcuni hacker riescono a eludere la patch CVE-2022-3236 con un attacco che funziona solo su versioni meno recenti dei firmware

Sophos X-Ops