Cronologia do Pacific Rim 2018-2024

4 DEZ 2018

Ataque Cloud Snooper

Novo rootkit e backdoor SSH, que mudam para recursos de rede, e primeiro uso de Traffic Signaling: Socket Filters ATT&CK (T1205.002) para acobertar o tráfego de comunicação C2.

2 ABR 2020

Ataque Asnarök (CVE-2020-12271)

Ataque Asnarök usa vulnerabilidade de injeção SQL (CVE-2020-12271) e ATT&CK T1059 para realizar um ataque em massa a dispositivos e implantar um cavalo de Troia.

24 ABR 2020

Dispositivo Asnarök identificado em Chengdu, China

Retrobusca encontra dispositivos em Chengdu aparentemente utilizados para testar exploits usados no Asnarök.

17 JUN 2020

Indicação do ataque (CVE-2020-15069)

Hackers iniciam o exploit CVE-2020-15069 encadeado à escalação de privilégio local para implantar um web shell em dispositivos que executam um portal da web voltado à WAN usando uma rede anonimizada.

9 JUL 2020

Implantação lançada no dispositivo do desenvolvedor do exploit

Após identificar com grande confiança um dispositivo usado pelo desenvolvedor do exploit, a Sophos lança uma implantação para coletar telemetria adicional.

14 JUL 2020

Identificado o dispositivo usado para desenvolver o CVE-2020-15069

Descoberta do dispositivo (registrado no "TStark") usado para desenvolver o exploit CVE-2020-15069 é vinculada a universidade em Chengdu.

31 AGO 2020

Sophos auxilia organização tibetana após ataque cibernético chinês

Sophos e Volexity auxiliam organização tibetana de exílio atacada por ferramentas encontradas 10 dias antes em um dispositivo TStark e outro malware vinculado a diversos hackers chineses.

27 NOV 2020

Ataque de dia zero Cyberoam (CVE-2020-29574)

Dispositivos Cyberoam atacados pela exploração de dia zero CVE-2020-29574 para criar novas contas de administrador.

21 MAR 2022

Supostos pesquisadores baseados na China pleiteiam recompensa pelo CVE-2022-1040

Supostos pesquisadores de segurança relatam um dia zero (CVE-2022-1040) à Sophos através de um programa de recompensa por bug, alegando vir do Japão, mas registrado usando um endereço IP chinês. Exploit inclui um bug de injeção de comando do OpenSSL.

24 MAR 2022

Retrobusca encontra ataques CVE-2022-1040 antes do envio do bug

Retrobusca revela ataques CVE-2022-1040 pré-datados ao envio do bug contra uma organização tibetana de exílio e uma agência governamental.

2 APR 2022

Sophos relata bug do OpenSSL (CVE-2022-1292)

Sophos relata um bug do OpenSSL, que é designado CVE-2022-1292.

15 AUG 2022

Implantação desvenda bootkit UEFI em desenvolvimento no dispositivo em Chengdu

Descoberto um bootkit UEFI em desenvolvimento em dispositivo adquirido por uma organização em Chengdu. Sophos cria detecções para o kit, mas nunca constata sua implantação.

16 SEP 2022

Primeiros ataques Covert Channels (CVE-2022-3236)

Sophos e Microsoft identificam um dispositivo comprometido em uma organização de serviços financeiros que é a primeira instância de um ataque Covert Channels (CVE-2022-3236).

17 MAI 2023

Descobertos ataques de gancho em firmware de dispositivo

Sophos descobre um shell remoto com um gancho de firmware que permite a persistência em um único dispositivo, instalado usando credenciais administrativas comprometidas.

27 NOV 2023

Ataques que ignoram o patch CVE-2022-3236 em firmware antigo

Análise de atividades suspeitas revela que os hackers ignoram o patch CVE-2022-3236 com um ataque que funciona apenas em versões de firmware antigas.

Sophos X-Ops