Zeitleiste von Pacific Rim 2018–2024

4. DEZ. 2018

Cloud-Snooper-Angriff

Neuartige SSH Backdoor und Rootkit, Pivoting zu Cloud-Assets und erstmalige Verwendung von Traffic Signaling: Socket Filters ATT&CK (T1205.002) zum Verbergen des C2-Kommunikationsverkehrs

22. APR. 2020

Asnarök-Angriff (CVE-2020-12271)

Asnarök-Angriff verwendet SQL-Injection-Schwachstelle (CVE-2020-12271) und ATT&CK T1059, um Massenangriffe auf Geräte durchzuführen und Trojaner bereitzustellen

24. APR. 2020

Asnarök-Gerät im chinesischen Chengdu identifiziert

Retrohunt findet ein Gerät in Chengdu, das anscheinend zum Testen von in Asnarök verwendeten Exploits eingesetzt wird

17. JUN. 2020

Bookmark-Angriff (CVE-2020-15069)

Angreifer beginnen, CVE-2020-15069 in Kombination mit einer lokalen Rechteausweitung auszunutzen, um über ein Anonymisierungsnetzwerk eine Webshell auf Geräten bereitzustellen, auf denen ein WAN-basiertes Webportal ausgeführt wird

9. JUL. 2020

Implant auf Gerät von Exploit-Entwickler bereitgestellt

Nach Identifizierung eines mit hoher Sicherheit von einem Exploit-Entwickler verwendeten Geräts installiert Sophos ein Implant, um zusätzliche Telemetriedaten zu sammeln

14. JUL. 2020

Gerät zur Entwicklung von CVE-2020-15069 identifiziert

Aufdeckung eines Geräts (registriert bei „Tstark"), das zur Entwicklung des CVE-2020-15069-Exploits im Zusammenhang mit der Universität in Chengdu verwendet wurde

31. AUG. 2020

Sophos hilft nach chinesischem Cyberangriff auf tibetische Organisation

Sophos und Volexity unterstützen tibetische Exilorganisation bei Angriffen mit Tools, die 10 Tage zuvor auf einem TStark-Gerät gefunden wurden, und anderer Malware, die mit mehreren chinesischen Akteuren in Verbindung steht

27. NOV. 2020

Zero-Day-Angriff (CVE-2020-29574) auf Cyberoam

Cyberoam-Geräte werden von Zero-Day Exploit CVE-2020-29574 ins Visier genommen, um neue Administratorkonten zu erstellen

21. MÄR. 2022

Ein pseudonymer chinesischer Forscher fordert CVE-2022-1040-Kopfgeld

Ein pseudonymer Sicherheitsforscher meldet Sophos eine Zero-Day-Schwachstelle (CVE-2022-1040) über das Bug-Bounty-Programm und behauptet, in Japan ansässig zu sein. Tatsächlich erfolgt die Meldung jedoch über eine chinesische IP-Adresse. Exploit enthält einen OpenSSL Command Injection Bug

24. MÄR. 2022

Retrohunt findet CVE-2022-1040-Angriffe vor Bug-Einreichung

Retrohunt enthüllt CVE-2022-1040-Angriffe vor Bug-Einreichung gegen tibetische Exilorganisation und eine Regierungsbehörde

2. APR. 2022

Sophos meldet OpenSSL Bug (CVE-2022-1292)

Sophos meldet OpenSSL Bug, dem die Nummer CVE-2022-1292 zugewiesen wird

15. AUG. 2022

Implant enttarnt in Entwicklung befindliches UEFI Bootkit auf Gerät in Chengdu

Ein in der Entwicklung befindliches UEFI-Bootkit wird auf einem Gerät entdeckt, das von einem Unternehmen in Chengdu erworben wurde. Sophos erstellt Erkennungen für das Kit, dessen Bereitstellung wird jedoch nie beobachtet

16. SEP. 2022

Erste Angriffe über verdeckte Kanäle (CVE-2022-3236)

Sophos und Microsoft identifizieren ein kompromittiertes Gerät bei einem Finanzdienstleister. Hierbei handelt es sich um den ersten Fall eines Angriffs über verdeckte Kanäle (CVE-2022-3236)

17. MAI 2023

Geräte-Firmware-Hook-Angriffe erkannt

Sophos erkennt eine Remote Shell mit einem Firmware Hook, der die Persistenz auf einem einzelnen Gerät ermöglicht und mit kompromittierten Admin-Zugangsdaten installiert wird

27. NOV. 2023

Angreifer umgehen CVE-2022-3236-Patches auf älterer Firmware

Analysen verdächtiger Aktivitäten zeigen, dass Angreifer den CVE-2022-3236-Patch mit einer Angriffsmethode umgehen, die nur auf älteren Firmware-Versionen funktioniert

Sophos X-Ops