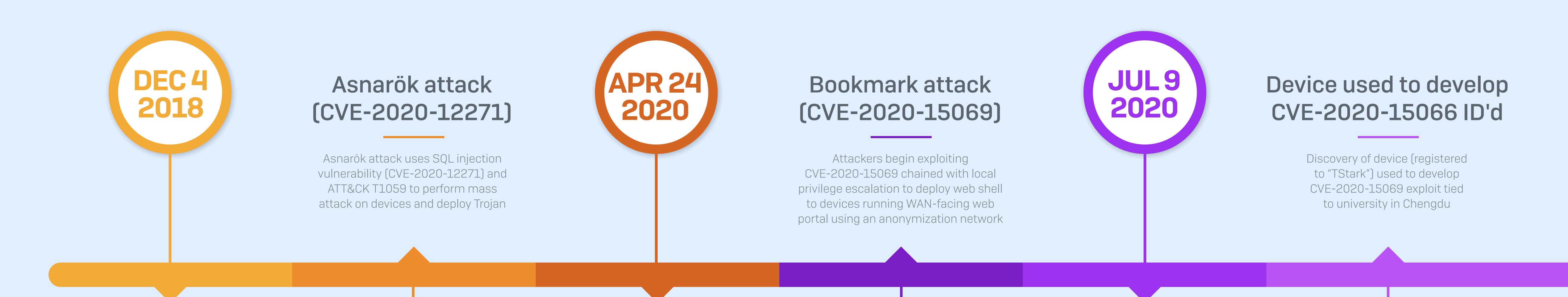
# Pacific Rim Timeline 2018-2024



**Cloud Snooper attack** 

Asnarök device ID'd in Chengdu, China

Implant deployed on exploit developer's device

Novel SSH backdoor and rootkit, pivot to cloud assets, and first use of the Traffic Signaling: Socket Filters ATT&CK (T1205.002) to conceal C2 communication traffic



Retrohunt finds device in Chengdu apparently used to test exploits used in Asnarök



After identifying with high confidence a device used by exploit developer, Sophos deploys implant to collect additional telemetry





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

> Cyberoam devices targeted with zero-day exploiting CVE-2020-29574 to create new administrator accounts



**Retrohunt finds** CVE-2022-1040 attacks before bug submission

Retrohunt reveals CVE-2022-1040 attacks predating bug submission against Tibetan exile organization and a government agency

**MAR 24** 

2022



Implant uncovers in-development UEFI bootkit on device in Chengdu

> An in-development UEFI bootkit is discovered on a device purchased by an organization in Chengdu. Sophos creates detections for the kit, but it is

## Sophos assists after Chinese cyberattack on **Tibetan organization**

Sophos and Volexity assist Tibetan exile organization targeted with tools found 10 days earlier on TStark device and other malware tied to multiple Chinese actors



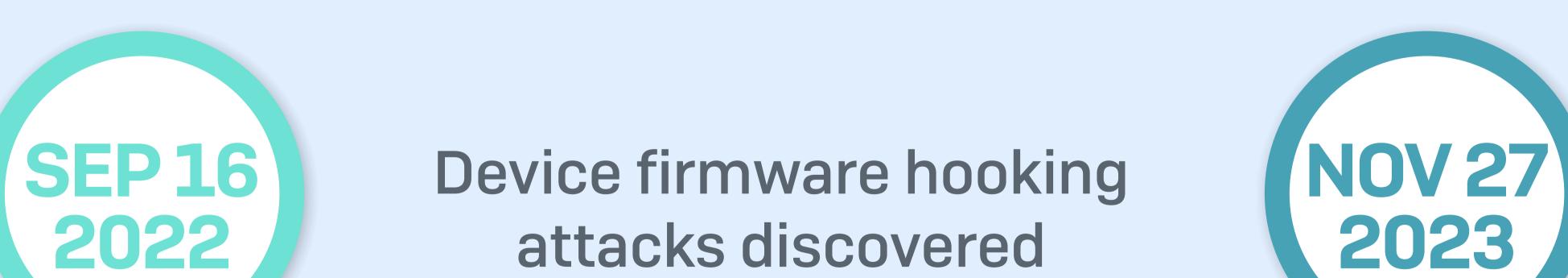
**Pseudonymous China-based** researcher claims **CVE-2022-1040** bounty

> Pseudonymous security researcher reports a zero-day (CVE-2022-1040) to Sophos through bug bounty program, claiming to be in Japan but filing from Chinese IP address. Exploit includes an OpenSSL command injection bug

## Sophos reports OpenSSL bug (CVE-2022-1292)

Sophos reports OpenSSL bug, which is assigned CVE-2022-1292







#### **Device firmware hooking** attacks discovered

Sophos discovers a remote shell with a firmware hook allowing persistence on a single device, installed using compromised administrative credentials

**MAY 17** 

2023



Sophos and Microsoft identify a compromised device at a financial services organization that is the first instance of a Covert Channels attack (CVE-2022-3236)

Attacks bypassing **CVE-2022-3236** patch on older firmware

Analysis of suspicious activity reveals attackers bypassing CVE-2022-3236 patch with attack that only works on older firmware versions

