Mphasis
The Next Applied

Mysterious Threat Actor Used Chalubo Malware to Brick 600,000 Routers

Date: 03rd June 2024 | Severity: High

Summary

More than 600,000 small office/home office (SOHO) routers belonging to the same ISP were rendered inoperable in a single destructive event, Lumen Technologies reports.

Attack Vectors

The impacted router models, from ActionTec and Sagemcom, were confined to the ISP's autonomous system number (ASN), and were likely infected with Chalubo, a remote access trojan (RAT) that ensnares devices into a botnet.

The destructive incident occurred over a 72-hour period between October 25 and October 27, 2023, and impacted ActionTec T3200s, ActionTec T3260s, and Sagemcom F5380 router models.

The unique event, Lumen says, resulted in roughly 49% of the impacted ASNs modems being taken offline, with the affected devices having to be physically replaced. Overall, roughly 179,000 ActionTec and 480,000 Sagemcom routers might have been bricked. "We assess with high confidence that the malicious firmware update was a deliberate act intended to cause an outage, and though we expected to see a number of routers make and models affected across the internet, this event was confined to the single ASN," Lumen notes.

The threat actor responsible for the attack, Lumen says, likely chose Chalubo to deploy malicious firmware on the impacted routers to obfuscate attribution, but no evidence of overlaps between this incident and known nation-state actors, such as Volt Typhoon, has been found.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hashes	• 30584f13c0a9d0c86562c803de350432d5a0607a06b24481ad4d92cdf7288213 • 7bd723b5e4f7b3c645ac04e763dfc913060eaf6e136eecc4ee0653ad2056f3a0 • d7f3ecd8939ae8b170b641448ff12ade2163baad05ca6595547f8794b5ad013b • 36ea1b317b46c55ed01dd860131a7f6a216de71958520d7d558711e13693c9dc • 8e45daace21f135b54c515dbd5cf6e0bd28ae2515b9d724ad2d01a4bf10f93bd • bdef8e089ffa00794f40f14ad3cdb8f1629241a4ac313bef8fe3d38e08207e4c

	• 0f863f624da0d74094cb0f91cc226281 • 08dd3d407a74159c2de0f6be0956a79625bdeb2f913d04520d1f8f310d6a78fc • 21d9ae29551dcbe39de375bdf8ada5a47b0e2372 • b2e2193e49ee1240be30f5040dbb5e2c973cdfb02c3ea88ef4ffeda884de28c2 • 6c6609264e9e4b365e1bd7df187f4405a1df3f02 • 00550d5c2ed14a445ae13cff8eff32ba7a7dd502d145481bcd18161cf1df540d • ce68c3687aae08b796e3e57d97d4f333991b6eba804581ae66f46dbd6ec7dae7 • b9d31125782ca0f20162b9f86b034a34cdc6b3fe318ee990721dc7d7dae66d22 • 5b7874b18e8365e07624946a33518988aea4c72478a285a36047b4ba554a7576
Domain	• lighten[.]medyamol[.]com • lakusdvroa[.]com • checkqazxsw1[.]com • axon-stall[.]riddlecamera[.]net
URL	• http://193[[.]]201[[.]]224[[.]]238:8852/RTEGFN01/powerpc • http://mnbvcxzzz12[[.]]com:8852/RTEGF/powerpc • https://www[[.]]v5002[[.]]cn • http://efbthmoiuykmkjkjgt[[.]]com:8852/RTEGFN01/arm • http://91[[.]]211[[.]]88[[.]]225:8080/SASBCKXOWYALLCZXF • http://hackucdt[[.]]com:8852/test/res[[.]]dat • http://sainnguatc[[.]]com:8080/ASUHALUMNABTC • http://coreconf[[.]]net:8080/E2XRIEGSOAPU3Z5Q8 • http://185[[.]]189[[.]]240[[.]]13:8080/E2XRIEGSOAPU3Z5Q8/res[[.]]dat • http://efbthmoiuykmkjkjgt[[.]]com:8852/RTEGFN01/mips • http://poiuytyuiopkjfnf[[.]]com:8852/ASDFRE/x86_64 • http://coreconf[[.]]net:8080/E2XRIEGSOAPU3Z5Q8/mips • http://193[[.]]201[[.]]224[[.]]238:8852/RTEGFN01/mipsel • http://103[.]51[.]13[.]52:8852/test/res[.]dat • http://193[.]201[.]224[.]238:8852/GHJFFGND/mips64 • http://mnbvcxzzz12[.]com:8852/RTEGF/mips64
IP Address	• 2[.]59[.]222[.]102 • 104[.]233[.]167[.]63 • 103[.]117[.]145[.]106 • 2[.]59[.]223[.]226 • 2[.]59[.]223[.]253 • 38[.]54[.]27[.]204 • 45[.]116[.]160[.]100 • 216[.]118[.]241[.]204 • 103[.]84[.]84[.]250 • 116[.]213[.]39[.]3 • 103[.]244[.]2[.]218 • 104[.]233[.]167[.]62 • 141[.]193[.]159[.]10 • 116[.]213[.]39[.]2 • 103[.]244[.]2[.]170 • 45[.]10[.]90[.]89

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.securityweek.com/mysterious-threat-actor-uses-chalubo-malware-to-brick-600000-routers/
- https://www.wired.com/story/mysterious-hack-600000-routers-destroyed/
- https://www.forbes.com/sites/daveywinder/2024/06/02/hacker-bricks-600000-routers-in-just-72-hours/?sh=5ffd90906320