Androxgh0st Malware Compromises Servers Worldwide for Botnet Attack

Date: 24th April 2024 | Severity: High

Summary

Veriti Research has discovered a surge in attacks from operators of the Androxgh0st malware family, uncovering over 600 servers compromised primarily in the U.S., India and Taiwan.

Attack Vectors

- The adversary behind Androxgh0st had their C2 server exposed, which could allow for a counterstrike by revealing the impacted targets. Further research revealed that Androxgh0st operators are exploiting multiple CVEs, including CVE-2021-3129 and CVE-2024-1709 to deploy a web shell on vulnerable servers, granting remote control capabilities. Moreover, evidence suggests active web shells associated with CVE-2019-2725.
- Androxgh0st operators prefer exploiting Laravel applications to steal credentials for cloud-based services like AWS, SendGrid, and Twilio. They exploit vulnerabilities in Apache web servers and PHP frameworks, deploying webshells for persistence.
- However. their recent focus seems to be building botnets to exploit more systems. Recently, the FBI and CISA issued a joint Cybersecurity Advisory (CSA) advisory, warning about Androxgh0st constructing a botnet to carry out credential theft and establish backdoor access.

Indicator of compromise

INDICATOR TYPE	INDICATORS
URLs	• http://45.137.155.55/libsystem[.]so • http://45.137.155.55/kinsing • http://45.137.155.55/ap[.]sh • http://31.210.20.120/ldr[.]sh • http://195.19.192.28/kinsing • http://195.19.192.28/libsystem[.]so • http://202.28.229.174/sys[.]x86_64 • http://195.19.192.28/ap[.]sh

	• http://194.145.227.21/sysrv • http://194.145.227.21/ldr[.]sh • http://185.191.32.198/ap[.]sh • nervous-hodgkin-5c3bb4.netlify.app • http://heuristic-hermann-392016.netlify.app • amazing-nightingale-3617e1.netlify.app
File Hash	• 1489c404a110149b66476e0f41317770f0291da64a0d4b39f28900ccaf4d30f2 • 240fe01d9fcce5aae311e906b8311a1975f8c1431b83618f3d11aeaff10aede3 • 428340a0695393a0cec55513e700a479e252d9b034f27f80a29da3ac99afa459
IPs	• 128.14.134[.]134 • 128.14.134[.]170 • 128.90.161[.]152 • 128.90.166[.]247 • 128.90.166[.]31 • 139.59.126[.]50 • 143.198.62[.]76 • 155.138.14[2].87 • 157.119.20[0].185 • 157.230.21[2].97 • 161.35.188[.]242 • 185.191.32[.]198 • 185.225.17[.]102 • 192.53.170[.]243 • 194.145.22[7].21 • 195.19.192[.]28

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.hackread.com/androxgh0st-malware-servers-botnets-attacks/?web_view=true
- https://www.scmagazine.com/brief/androxgh0st-malware-ramps-up-global-attacks
- https://www.fortiguard.com/outbreak-alert/androxgh0st-malware