Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

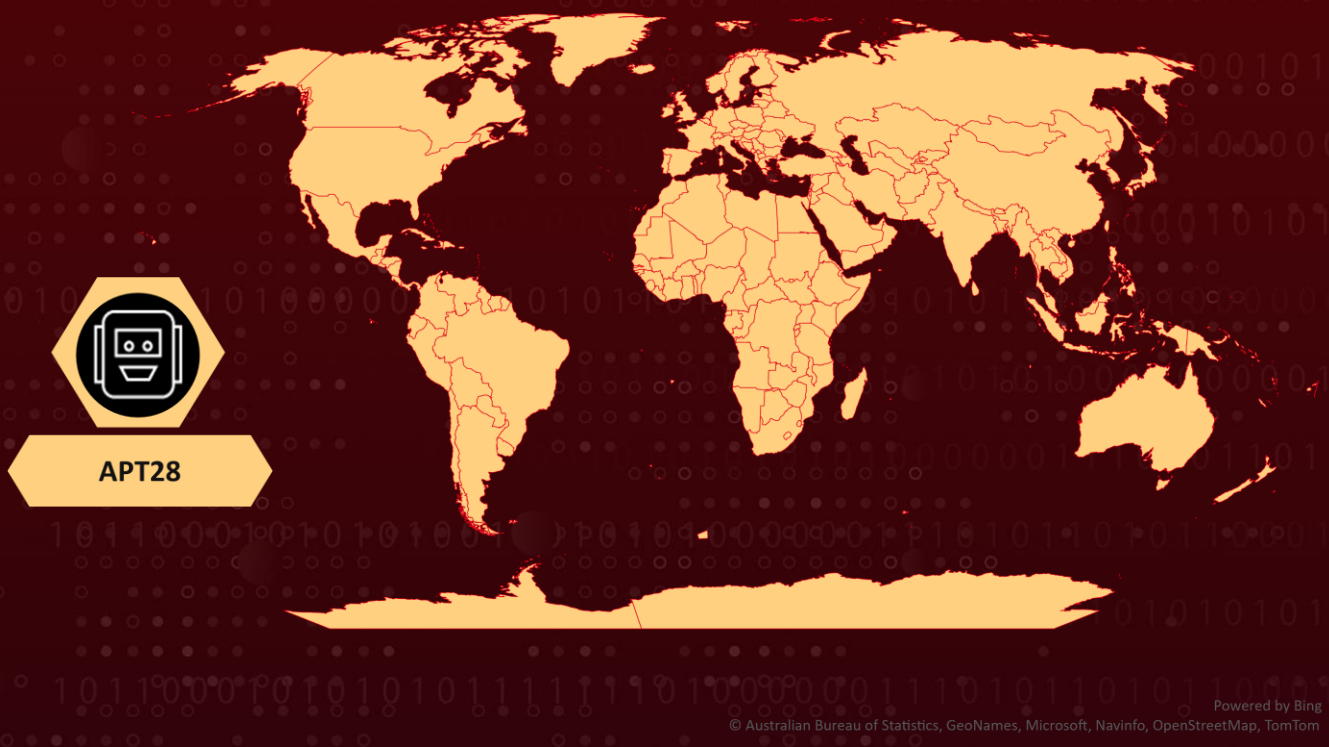
Cybercriminals Forge Alliances via Compromised Routers

Date of Publication	Admiralty Code	TA Number
May 3, 2024	A1	TA2024172

Summary

Attack Commenced: April 2022
Threat Actor: APT 28 (aka Pawn Storm, Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard, BlueDelta, TA422, Fighting Ursa, Blue Athena)
Attack Region: Worldwide
Targeted Industries: Aerospace, Defense, Education, Energy, Utilities, Governments, Hospitality, Manufacturing, Oil & Gas, Retail, Technology, Transportation
Attack: APT28 threat actors utilized compromised EdgeRouters to execute covert cyber operations, repurposing Ubiquiti EdgeRouter routers for a range of nefarious activities. With root access to compromised Ubiquiti EdgeRouters, they possess unrestricted control over Linux-based operating systems, allowing for the installation of tools and the concealment of their identities during malicious campaigns.

Attack Regions



Attack Details

#1 As early as 2022, APT28 operatives had used compromised EdgeRouters to conduct covert cyber operations. These compromised Ubiquiti EdgeRouter routers were repurposed for various malicious activities, including Secure Shell (SSH) brute forcing, distributing pharmaceutical spam, employing server message block (SMB) reflectors in NTLMv2 hash relay attacks, proxying stolen credentials on phishing sites, providing multifunctional proxy services, engaging in cryptocurrency mining, and sending out spear phishing emails.

#2 Cybercriminals lease out these compromised routers to other criminals and likely also offer them to commercial residential proxy providers. Internet routers remain prime targets for threat actors due to their relatively weak security oversight, lenient password policies, infrequent updates, and the potential use of robust operating systems capable of hosting malware such as cryptocurrency miners, proxies, distributed denial of service (DDoS) agents, malicious scripts, and web servers.

#3 Consumer-grade internet devices like Small Office/Home Office (SOHO) routers are also favored assets for criminal enterprises and espionage. With root access to compromised Ubiquiti EdgeRouters, APT28 threat actor have unrestricted control, enabling them to install tools and conceal their identities while executing malicious campaigns.

Recommendations

Check SSH Banner: Utilize the verbose option of your SSH command-line client to inspect the banner of your EdgeRouter device. Look for the presence of the "Debian" string and ensure that the OpenSSH version matches an official release number.

Verify GatewayPorts Configuration: Log in to your device via the web administration page to enable telnet temporarily. Then, log in via telnet and search for sshd_config files. Check if the GatewayPorts configuration option is set to "yes". If you do not recognize this setting, it could indicate compromise.

Verify Binary Hashes: Check your device's hashes of all sshd binaries. If any match with indicators of compromise (IOCs), it suggests a potential compromise.

Limit Internet Access to Administrative Interface: Consider restricting connections to the router's administrative interface from the Internet to minimize the attack surface.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0006 Credential Access
TA0011 Command and Control	TA0042 Resource Development	T1562 Impair Defenses	T1556 Modify Authentication Process
T1055 Process Injection	T1587 Develop Capabilities	T1584 Compromise Infrastructure	T1203 Exploitation for Client Execution
T1082 System Information Discovery	T1546 Event Triggered Execution	T1557 Adversary-in-the-Middle	T1059 Command and Scripting Interpreter
T1219 Remote Access Software	T1018 Remote System Discovery	T1041 Exfiltration Over C2 Channel	T1562.001 Disable or Modify Tools
T1588 Obtain Capabilities			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	95995686b9af8b56c3fed1dadccf8b2ed5f417bb4eb8947a406a6e943cca33c6, 85a4151d790ab32d5321c6e71748b2446032e1775aedd0168be25f76bf4fe93f, edefd297285090fe743f5c3b111bce54da40f43a32e15d8fa87b8a2c243f6d47,

TYPE	VALUE
SHA256	2847ae693533406defecb226bfe6d62dd36905ff07add4e773426bde83e85ddc, ef6fe4140001cb099968acd5772452859adbe7b57496389fbbf2342f9047b962, 944be9bb167a2f76fe2f539d3860bbf26301830c479bc68509af46e047993c8c, 104e3ea9a190ba039488f5200824fe883b98f6fe01d05a1b55e15ed2199c807a, 4a932ccc8a45db6897a11de118cdbf67062569112f1caa69793669c5c24be708, 17257ce42246b8c47f9ec639a6ffaca2bc14c21a22c4419bf468e3f1d491e330, 4d35ae9669db428b72b1aaadd21dbed44ad2fc678efc8110d89ff723e0497406, dfc86b375e974b3092bbff41eb24db3281fb4fc104f1043a7afbf95f85a2c1d5, f88d12332d2f58459f989c7c41b5381e8aed9c8c30c1d11373f0d1eb0b340b9a, a4a95807f1c5b200d5d94e3e811a7c4af2d0d9ca88ca4d7f9d02015574f4716f, 681a00df2e2cc680a4b68bdb6fe7d55c34d6d3fc35d462c78ebb659f9cb2cd60, e3ba85e0bc978013b145ebb4c2d583b33422da93787ab8fb2185b55478652d91, fed8c98fc754aff95f8538b5bebce558eb274256b0265d4482a675b74e93cc93, ad3fd3eb7a3a276ec0d384afb5b75fe7d9fc047bb0dab40f9d55870d4520c1f3, 0891588667da40da58ffaa8fedcddb0a9a172646ec12e6d0b9ce2acc2caa302b, bd0ea597f24bb72f8db34b6b6d2c0bc70eb53df9eae40cdb216a13521145ab03, 28aee94e9a3f6c4296663bb853a5af5817ae109f066c88b7a245316a9a1e4712, 2ae805b68d7408cc40ad058bc0b8b2b5c29d77760084a5230448e47cec1c43f4, 2f182a6cb72712c340c2adb43843cfccb5916d236485de1c62fb40c883570824, 53d687868fd7ab9e78aa09f696923bd3c057e4e50432d07210080474a8d879cb, 844cc1807cc5b628b7aa807ef3b682d051c8ad5427df3d3e36c7e7633bfc5768, c290ab5d8ce9fcaa91da3b488c93dee1a4d0581c1335f19cb48027a5a03fe525,

TYPE	VALUE
SHA256	88f2d42bf225c930bc644f82bbd229e170d53dd1072e846e2883265a7ac33301, f6541b569787aa050c54ad85976ac5b729697a022be188b0040d37aa91e49ae2
IPv4	185[.]62[.]58[.]20, 185[.]62[.]58[.]141, 193[.]34[.]166[.]176, 193[.]34[.]166[.]206, 24[.]88[.]87[.]29, 32[.]143[.]50[.]222, 86[.]123[.]151[.]53, 172[.]114[.]170[.]18, 184[.]75[.]134[.]59, 185[.]227[.]137[.]200
Domains	moreover[.]lostgumball[.]com, li4858member[.]possessed[.]us, clientrun[.]compuinter[.]com, founderside[.]joseulloa[.]cl, packinstall[.]kozow[.]com, matbaiteahe[.]mooo[.]com, lalapoc[.]kozow[.]com, gneivaientga[.]ignorelist[.]com, antotehlant[.]theworkpc[.]com, onechoice[.]gleeze[.]com, mumucnc[.]kozow[.]com, enforcer[.]mywire[.]org, puffypuf[.]gleeze[.]com, speddot[.]seburn[.]net, terminal[.]looguy[.]com, vrrumover0[.]vrrum0[.]farted[.]net, trompadiom[.]tutotame[.]bigbox[.]info, gopremium[.]mooo[.]com, dfgtjytdfs[.]work[.]gd, xfgjgjkuykykgihguifdt[.]mywire[.]org, changepassword[.]giize[.]com, kjskrvmwerffssd[.]kozow[.]com, prekudinish[.]com, remalexation[.]name, macrofocafify[.]org, semiridinution-postepudency[.]com, underuvukent[.]com, minixetepate[.]biz,

TYPE	VALUE
Domains	antihicipate[.]com, interocakate[.]com, promexucate[.]com, inoluvary[.]com, recepatission[.]info, ultradomafy[.]net, emelenalike[.]com, subonuker[.]name, decumify[.]net

References

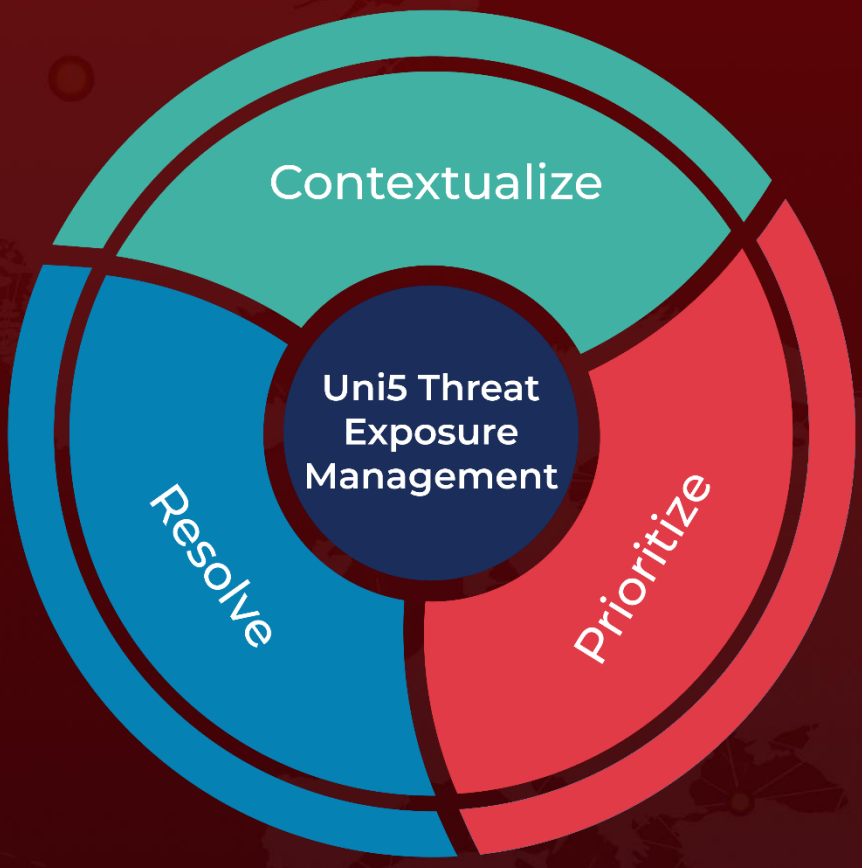
https://www.trendmicro.com/en_in/research/24/e/router-roulette.html

https://www.ic3.gov/Media/News/2024/240227.pdf

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 3, 2024 • 6:00 AM

© 2024 All Rights are Reserved by HivePro

More at www.hivepro.com