Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

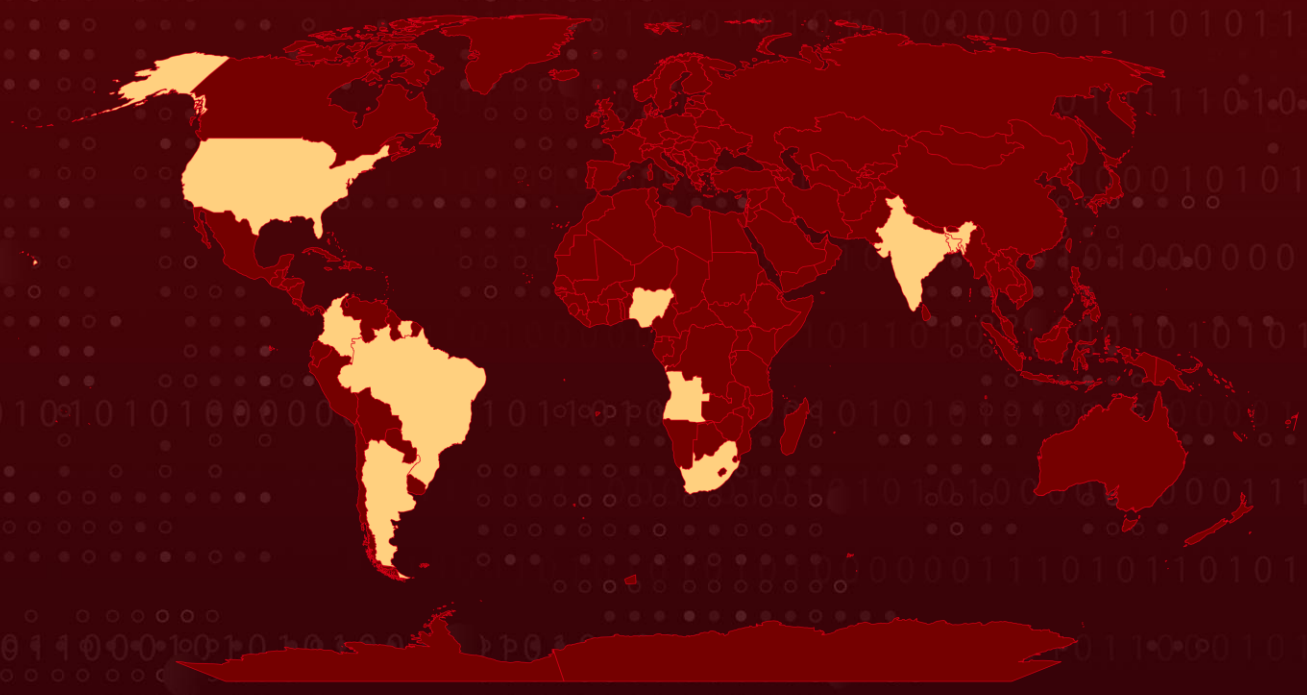
Socks5Systemz Proxy Botnet Infects 10,000 Systems

Date of Publication	Admiralty Code	TA Number
November 6, 2023	A1	TA2023446

Summary

Attack Began: October 2023
Malware: Socks5Systemz, PrivateLoader, Amadey
Affected Platform: Windows
Attack Region: India, Brazil, Colombia, South Africa, Bangladesh, Argentina, Angola, United States, Suriname, and Nigeria.
Attack: A sophisticated proxy botnet known as 'Socks5Systemz' has insidiously infiltrated over 10,000 computers by employing the 'PrivateLoader' and 'Amadey' malware loaders. The masterminds behind this botnet offer their services to subscribers willing to pay between $1 to $140 per day in cryptocurrency to gain access.

Attack Regions



Attack Details

#1 A proxy botnet named 'Socks5Systemz' has covertly infiltrated computers by leveraging the 'PrivateLoader' and 'Amadey' malware loaders. These loaders are commonly disseminated through various means such as phishing schemes, exploit kits, malvertising, and trojanized executables obtained from P2P networks. Currently, this botnet has compromised 10,000 devices.

#2 This malware effectively seizes control of infected computers, repurposing them as instruments for forwarding internet traffic and facilitating both malicious and anonymous activities. The operators of this botnet generate revenue by providing this service to subscribers, who are willing to pay between $1 to $140 per day in cryptocurrency for access. Proxy services empower users to rent a set of IP addresses for their internet use, granting them a level of online anonymity.

#3 Essentially, these services obscure a user's online presence, making it appear as if their internet traffic originates from conventional IP addresses while concealing their actual source. In the case of the PrivateLoader and Amadey malware loaders, all distributed samples execute a file named 'previewer.exe,' responsible for establishing persistence and injecting the proxy bot into the computer's memory.

#4 The payload of the proxy bot comprises a 300 KB 32-bit DLL. It utilizes a domain generation algorithm (DGA) system to establish connections with its command and control (C2) server, transmitting profiling information about the compromised system. After parsing the connect command fields, the bot initiates a session with the backconnect server via port 1074/TCP, employing a custom binary protocol.

#5 Since the beginning of October, there have been 10,000 distinct communication attempts over port 1074/TCP with the identified backconnect servers, indicating an equal number of victims. The geographical distribution of these victims is widespread and random, spanning the entire globe. However, India, the United States, Brazil, Colombia, South Africa, Argentina, and Nigeria exhibit the highest infection rates.

Recommendations

Port monitoring and filtering: Implement port monitoring and filtering mechanisms, specifically targeting port 1074/TCP, to detect and block unauthorized communication attempts with backconnect servers.

Monitor network traffic: Implement intrusion detection systems and continuously monitor network traffic for unusual patterns to promptly detect and respond to any suspicious or malicious activity, which may indicate the presence of a proxy botnet.

Behavioral Anomaly Detection: Implement advanced behavioral anomaly detection systems to identify deviations from normal user and system behavior. These systems should be capable of flagging activities like frequent and unusual execution of commands.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0009** Collection
TA0011 Command and Control	**T1203** Exploitation for Client Execution	**T1059** Command and Scripting Interpreter	**T1105** Ingress Tool Transfer
T1027 Obfuscated Files or Information	**T1543.003** Windows Service	**T1055** Process Injection	**T1584.005** Botnet
T1571 Non-Standard Port	**T1040** Network Sniffing	**T1047** Windows Management Instrumentation	**T1005** Data from Local System

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	C:\ProgramData\ContentDWSvc\ContentDWSvc.exe
Domains	bddns[.]cc, datasheet[.]fun

TYPE	VALUE
IPv4	109.230.199[.]181, 185.141.63[.]172, 193.242.211[.]141, 212.8.242[.]211, 109.236.85[.]145, 190.2.135[.]77, 151.80.38[.]159, 217.23.6[.]51, 217.23.9[.]168, 37.187.122[.]227, 51.159.66[.]125, 109.236.88[.]134, 109.236.81[.]104, 176.31.254[.]229, 185.141.63[.]2, 185.141.63[.]4, 185.141.63[.]84, 185.141.63[.]85, 188.165.192[.]126, 188.165.192[.]18, 188.165.195[.]130, 195.154.174[.]130, 195.154.176[.]206, 195.154.176[.]209, 195.154.178[.]238, 195.154.188[.]211, 195.154.235[.]51, 195.154.241[.]165, 195.154.242[.]37, 195.154.243[.]38, 195.154.251[.]21, 195.154.251[.]99, 195.154.252[.]221, 195.154.253[.]49, 37.187.142[.]187, 37.187.143[.]172, 37.187.148[.]204, 62.210.204[.]131, 88.80.145[.]110, 88.80.145[.]142, 88.80.147[.]200, 88.80.147[.]205, 88.80.147[.]36, 88.80.148[.]219, 88.80.148[.]33, 88.80.148[.]8, 91.121.171[.]208,

TYPE	VALUE
IPv4	91.92.111[.]131, 91.92.111[.]132, 91.92.111[.]133, 91.121.30[.]185, 94.23.58[.]173, 217.23.5[.]14
SHA256	fee88318e738b160cae22f6c0f16c634fd16dbf11b9fb93df5d380b6427ac18f, dc262539467bf34e5059686955d6567efadd8e21c76be51eba94737d8c326720, 78efcbb0c6eb6a4c76c036adc65154b8ff028849f79d508e45babfb527cb7cfe, 5b45926c91fe46b12dadd3dae6afa2cf76f91a8fed7c3aefdad7f8c1faa03919, 189af501e84dddc5af3f7a66dcdc5095d22570abad100575ade261698d199bf3, 2987dc6ea8908c9e80ee5cd15ae4b91d15c48d1d31f7dbc79e01864475f33247, 3222778fd2f0717284dedbbda7298abf17105881147832e7a1cdbddc24747b0a, d99188eb6d65ecfeb7586bfb3566766fd1c68f659fbc57c7ce2bf1580452fd69, eaaf1823c34ea385dc3fa483a071b9a5f6122c8ab347b83da00a887ade466a0b, d2eafbfcd0dc07d49081b9b8324b549b08eb7aefd87ca6175046a9dd11b1d350, 5b3b41fcfe12f7bf5f933d8dbd5d881a3c5391ffb0a71fc313ac456afe8d7510, 2acfc97589dfb9f01a4ad9919b6bd73b38f391343b2e952e7dec8bfb8318bf51, 09f3fa5267026b2a7a698517d21dec97594cf2623388b13f0091e09ecba85ee9, 34a818f4223d32179c774e5cc707410d448d4e72fff148c293f453179642c8e6, 5c52f631330f6099fdf038af2e7fc2bc7956e561fe9db5fbde0e8c1fb1951323, 99c4c0abd02e05ce83b85184d4f49853674b63d1e402e5068992aabdd35109f8, 116db67b886d33dc3ce3892471ea70b652539fe3436aefbc6d4771cd72748bf1, 1ba2ae706f2e9b938f96b1d9baa63e302eb0b93c370d6a9b8c555065f90123dd, 903ee5d2fb1341754c10acba60faf45fdde7dec94b5c82e3d990a9e7a5a7cd7f, 8093be2f5aabcfdb73bf1e6a73161e37d2f702868f974387a032d4e0489516ee,

TYPE	VALUE
SHA256	75a741eb4e59010b49520e85c949c610ddec55cd89ea954178a12e6b45551483, ee5ce35a68761315dc14c27af6cb25128952bbde67a699b5c69cb21081a3bd75, 9b914a04a6b4acb86915551f54a471fd3fc5edda4f8b948416db38808fa291bf, 8be1d9004e4ffad4035fa973d6d6508835762adf097a7f4362039b11b5d41122, 25e34355c90e9b96478a3a316c4b3280f3254e3677bc9c10e8146efbaaf29c39, 449d46143fac008f3c90ea25156bf2e1f3492c7e55e11a45670b98c076924f34, 48429a97039eef7473041955fdd403f4d6ae72332cc7f9ede56986167920cd65, 973b44c741b1e12417e6a99a806b519b1fb2a1095d2931c154d10a92fabcb01b, 65faccff1bd94971f57d4ab74662a11e0de5e9b84c64db56c2290b419c2ad59b, 759e28b5e743ef6368816dafb62507ba7133cdbb38853e21ff98964aa3c0d454, 1357aed783ad4b524540bcf99d980eaeac3aa21357b696b32c412ee44b925eab, ebca811f9da30028f61da7eb4e4d842eec9558a0c0b9e6c172c70095cbc8f4b9, 37f72d7cc30ac6952775a5972e510e0f2e0163b11ac7dea1e4dc0449dd8e633a, 3476601196502ae5aacb48ab2a6b0b1089100c0761f563c2cdb86861bc18798d, 6cccc777cf4eeebb2a17f4d13732f5dfeb0f6dbf50e6b96c743f101c481a44b6, 8dabf008e15a4822e0a34b1a998ce3522194128dffbab0401320c6fd21fa97df, c02e920086d41efee570ff2aa367640d63394f1ef86bffb1ced03aafa9bebf4b, 8458c1237cd94a1446468c7d615df01af8ef3ffc14c1033efeb61118bf4bd3b4, 3b5d15ed72a7aaf60ee447fade02e82e333e09c84ccd7ceca3b3594702da0c52, 70b3d99e5a06e20095f2919783b8afd9077e5a9a6aed92236605d69bcf424316, 2f255e9658e381d9c02499c30dcb07af2c7f5691fd6e5afd8ef35f3d284429f7, cb346f5850a116273a9a6fc0430d99e2b2d3a1f92a1742242499d67728efba1d, 779bc4fda3638f8adfba674f096475dc4e663fb45c962b5120b9c285dac87fe2,

TYPE	VALUE
SHA256	71f6c61bc2314ab899d3e79ffe0cf9434106ae29f760a5e076dbf826a7dfda7e, 4847e2d370b72b717e85f289bf9daf22a39906fa99cedc8cda584a775ba571fb, 0cebb8519e93f4177b4ab6d82f59643de9940ac6acdd284c3c1f23019f203120, ae1b4b92fd179336c88340771c8c16492b6b3f80030735d770dafeef2558861a, 43ec23f5477e218b33003603458503d469804ab5a05ee97541402a2b7255627a, 23416440ae258c4a472c5c3c07bf7659190168277f8483dcd84d24fbcb83bbd4, 78ab98c5b5ead97ff7d245b9603bb5edc4d59d379e492049a3a958a8e48cb945, 1fa58cb939e9b5d0f7f0d5c78b437f62f182b5d3658e59729fda2f28eb8746da, 29122127b97c0810a564fe16d87faaa9c931e0e48ecd63271af86385a652baca, ae9aad29ad8bf58206a14b791b0ab0c842d745495762bf3fe092ce3be1f7fb0e, dc0cb777651c14ef9e44cad759ce2a9688872e56d241352e23a3ab3443b03f07, 15f4e20fb7971cbd61a7ba4f6ca0582286ff7ca332c17b7c5eef0c023f40bab0, 1f8ceb6cd9e01bfe384378c5ea66de52674e188103f5e438a6029680c0b3180f, 2e00197cd4b002cf65fc588be7c31b0b6c46f320885eddd6b7d71c8d2f98b36b, 3f321b0d86d3af5f72c328b445c07c9c423b47ee3faa89bd413fdd5486019a0f, 2d41e76e3200255d7a11e43c6b826bef6a91cabf451c66b3b36d6826cd56fb46, eb5dfd6a133128a5d2c7183940639ead5e3aa33aa5ba581ce8d91ee113e4931f, 8466c3b28b913e7e965b083b8a3174fbe12b76ed5e9f7d4d929a51cb660e326b, b1ed4acd9128d49b5a619e8607cac13b33a8743e717a937c9ee9e6d963375867, af766ba5f46115470242fa6033f4f4ba85c82b6d5a001ebfee8482e51d793e1d

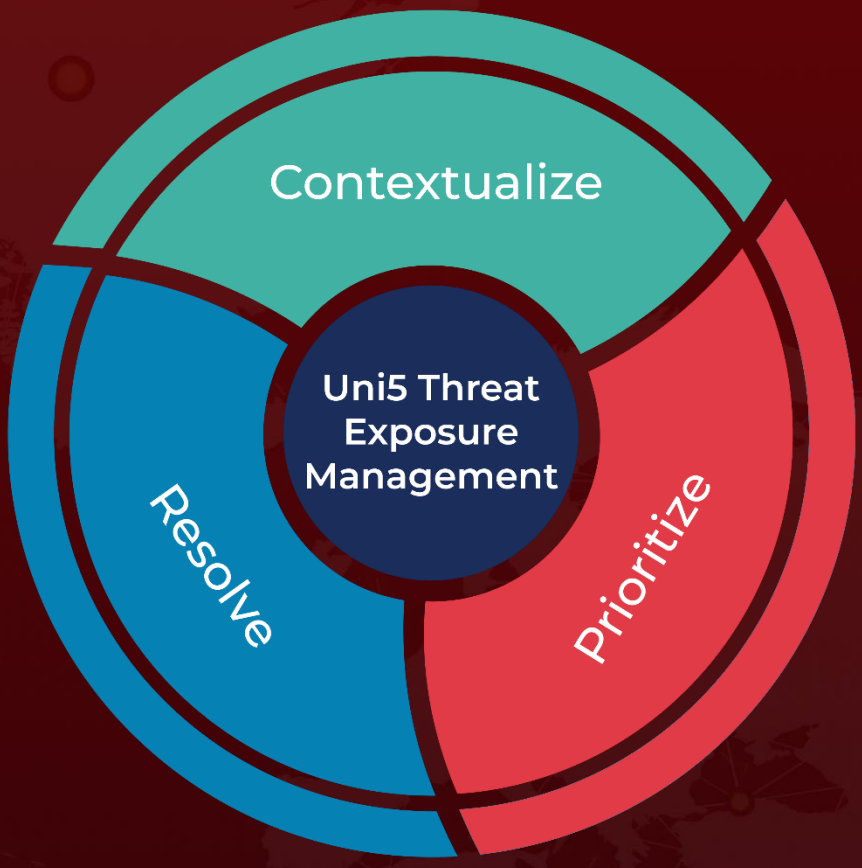
References

https://www.bitsight.com/blog/unveiling-socks5systemz-rise-new-proxy-service-privateloader-and-amadey

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

November 6, 2023 • 3:00 AM

More at www.hivepro.com