Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Raspberry Robin Expands Reach via WSF

Date of Publication	Admiralty Code	TA Number
April 11, 2024	A1	TA2024141

Summary

Active Since: September 2021
Malware: Raspberry Robin Worm
Attack Region: Worldwide
Attack: The Raspberry Robin malware campaign, active since March 2024, employs malicious Windows Script Files (WSFs) to disseminate its malware. These files, commonly employed for task automation within Windows environments, not only facilitate the spread of the malware but also serve as targets for exploitation by malicious actors.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The ongoing Raspberry Robin malware campaign, initiated in March 2024, employs a sophisticated approach to disseminate malicious software via Windows Script Files (WSFs). These files, commonly used by administrators and legitimate software to automate tasks within Windows environments, serve as conduits for the malware's propagation but are also exploited by malicious actors.

#2 The scripts themselves are intricately obfuscated and incorporate a variety of anti-analysis methodologies, making the malware elusive to detection mechanisms. Traditionally, Raspberry Robin was spread via removable media like USB drives. However, it has diversified its tactics to include social engineering and malvertising.

#3 Recent developments in its dissemination strategy involve the use of archive files distributed through web downloads. These Windows Script Files are distributed via malicious domains and subdomains controlled by the attackers.

#4 Functioning as a downloader, the script file exhibits similar evasion techniques to the Raspberry Robin DLL, employing a spectrum of anti-analysis and virtual machine (VM) detection mechanisms. The final payload remains dormant until the malware discerns that it is operating on a genuine end-user device rather than within a sandbox environment.

#5 Additionally, it includes safeguards to halt execution if certain conditions are met, such as the Windows operating system build number being lower than 17063, ensuring the effective deployment of its payload.

Recommendations

Monitor Network Traffic and Communication Channels: Implement network monitoring tools to detect unusual or suspicious activities associated with Raspberry Robin. Monitor communication channels like Jabber for signs of malicious activity.

Continuous Monitoring and Analysis: Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**T1204.002** Malicious File
T1053.005 Scheduled Task	**T1140** Deobfuscate/Decode Files or Information	**T1622** Debugger Evasion	**T1497** Virtualization/Sandbox Evasion
T1041 Exfiltration Over C2 Channel	**T1566** Phishing	**T1083** File and Directory Discovery	**T1027.009** Embedded Payloads
T1059 Command and Scripting Interpreter	**T1055** Process Injection	**T1007** System Service Discovery	**T1082** System Information Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	553b9eaa741adfb9073638e001d369441a802b406d3bca50436aea1df5b16da5, 4c87daaa84c41706156d37060360214798826229f5dedd6c46c821d879409509,

TYPE	VALUE
SHA256	4e93fb810189d3e1df1d0ef0f30642b8891e4140301a4aaaf5cb93955588734d, 0b369277901fff2ac52bf04e366318aa9018e7ea570779f476b2a0e676c9db83, ca6f46bdfd14021c102d4e4d95597a20bb9685628b4067b9ba85f18644ad6cdb, 98ad6aad996e4005389ea7e4782a4a082c1e83a8a20ad07bb3a3eed4047b3603, 9303b89abe2c0393e78991f74a90d9202a2f14dc267367277da7af705733eb32, 229c6b0dc9298a6868a24aad6cf3c8b08feb97f809f2d67fb6dc2e71ebee876b, 78ae67f650400ef6db9a85aa3d10ab7684f789e587ef33420a352a9b53916364, dd576545834e9c439491d62a8a6d9578a58693cef9f5cd2783fc80f49275dac8, fbdbe211e66792f3cefc50da6b3b88d82d497be1cd25f4654d4d122c0ed10a42, a3de553cae9671bd94aae75f76f8de2dd9abb41780d25f012debf7761a579ea9, 479d1cb582c03c679cb23ccb6b5dd1611822f59f311a6cdc82bd6eef5f53da14, d5dd3f1dd787746403843100c8dec9c70c20d8098071aafc5bfeef20b95fd93f, b4566c3cbfa193ad6dc7173d8b5d93734f06d940085110f6a2c7812524c2c236, 752ccebfcf2d63d44bf3073b2f30e83758aa0ae26d3bdca59de6e53e6d33b19e, a81176e32b8d73fbbd11d1a1da32789c8b18cf6aa79e1b4cae8ed031b7e9dbbf, 99d1e9839922063d3655583d541ac6908000222cd847c95c919a27c9d2b01301, 07b19580d9c5febb2b7d1da395022ca790372104bc99b35a8b18d506dfa2f9c0, 8921a869a93b4e9cec50b66b81793af67c2664aec5028c48738bae03f7026560, 981e56f56ab9c3dc81deed819ad3cd7367b8d44449a1ebbf1aad5033f2bd4547, 068f7a941ca655d71dd894c1564a24bbe9d67a6aa9e60b0692f558512e28c3a4, f2e1130b4baf1dc611fdde8029234348b4df69d5ebe32edc540e6fe1caaadd0a, de877115545a14417593fcf21d0ebf9b252940155e8fcdf152e5c6af54ffc84f, 4a0af8b333065d245b094964de709bb832fa630799106e711b38357236780924,

TYPE	VALUE
SHA256	812f646f94d6b6766698ce11de68bf49e9478272ad48113c4fe227735a0248a6, 2fc1750ac3ed97630a6088d1c4007065beaf44f50dfec1a068cea33537a53160, 08beb3900bbd4b4860e41b08b8585b7f3021676db3c07d9615d1a0aa92d3f0ce, 64c5b1ccc4023e0cdb1e7c880f00832b2a98bb9ce18f832e0c664b16726ea6fa, 28bc455cf1feeb0d9de0680ca8726bcf723b47bef43d3cb4180972aba7d30fa8, b55e88c542c9a90b4cba403d029f0c21aca5d3f001c47af7650269a227d9a982, 3f0fed4651179173f88b6be99eab1ab4f04f5eebe0f7eecdaff59b1e0c9fd6f6, 63ed9258e33164ee82be7d933377484b7ec7dc211a1119e4def4ac64d8d75c1f, 2dc987eb9844063e824ff6c27d64176c9fa8fcf974e835d5a06f6f022a05ea2b, 8fe220f1d81857cdd9d72d85a6d44d6e6e8bab59d6454877b27e6104bc3a2b01, 040a7f7f0304b486f82beac718abe7628fd1c514c22afa49d5540e652db9aabd, 0d35c51a0214117f1ad94428ccf789c8dd2376177192a86c4e7af9bd106affae, 83af28eb822624aa7d2434697ae1857ff7d5a27b8b1cbfbccc7ddabc4d6299e9, c2d4c676886a94f26fcadd5c381183ec93583b63b6acd43d48cff90c6a308bb2, 02e951d3e6644d21dd5b1d99f0a3b3111985bfe798a99a5b884419282c9c18c7, ff927726e3ef1a8d621696ec9f28925406f40d2eaa2580a8585bd8b1ab48a53e, f88fd72addccd83abeb8e1a946d6912d52a4a1c79452836a6b3bfe466e918ca4, 369053a465556ac48558b1d1fb44b4b8a99df362a0633bcce8215a54f3cf265b, c39f842302c80f925f47f35f0a033229e554a2e0128b2f98d93e1094ee32c074, 59e701743d78bcedc8ee825348c4fce930af88179ae22b34b6ec6fa4091059b5, 577277dee893b1a0fd6c84a0d52708dd198704b43ca25c6d8d62750f212db71e, 3c888db21bfb820731e08607497c3692bca4ccf396b91b11770fe1eccbc69e8a, db7b3ff26af8a6ea7d986c21db50c55e7b5a2f9ad3264f9f8b6a2c24044d5640,

TYPE	VALUE
SHA256	8d033a8d7987e9bd533054762d8c314a1e650df28cefe1d4d01b6516407c13f4, 1e45021c137a2a09002aa063c8b976ddc3b18a18aebb5847e80ee2c3799b92e9, a982ce60ad2a680ec6dba4e8eacaf9ddd5e6222731299ada6a8a5883465d865e, 2d83ee0241906ea366a01be95daaa243c164ff2c8de8adf8ba488ab770017ddc, fa2ffa1269f78db8a86ce4f91f1230d2a70cbec84d701207830fa012b24da762, a3a2c9e34fe8da242a348be59b77343394881c57ab02b2983f95b0358782524b, 65a920b94e4597c40bead51e48761453475de91706d311eac9d51be88adf28e7, f34a55f6df92d57cd54feca98f5f41c164f3236aafc8b22056b2facb88bb4ae1, 76f3685b21a7e4435a8d395b562f44b7a96912e75ad39af534d6b1e948416a2c, f345ea8bc11013cf26cf177fc320cec2ea95435462a8a866b154432f18c5a215, 7c2cc3f6d9fa535d79479717755e695ab23ba9be938a8e2e34255041c4040458, 7aef09c170f18016b091ebd0a9dfb3dba3bc291b75d86e0a30edf002f1a38a0f, f31e41692d87b580917e78ff8fd3d80ba673f52aee370b8c8fb8a428f765b901, 0b75220c914afcc34c52d1ff8c3602d365f5c4fe19d900d227a96c45b92a878f, 05a3b07352dec1cacee5cb460ca55b3ee79dd5a73e46761102e4f896609ae0d4, b449177e857bae35873170dd6f6d9b661b80c9873ab1c68e1298d1dd1564e277, 62db188559a316ba425a3351eda6b1ffc7d0823b6bc8ef8aa6342a0ff4c5e232, 9c718717bb9eee72daa6d9b378bf5a9671187436d6efd7e9859287e456f06cd6, 019b8250347f8012b4a82b65145625008eb515dc714f3f7c4a4da244cab217c1
Domains	chroococcoid[.]sbs, polyideism[.]sbs, ophthalmomyositis[.]sbs, quarrelers[.]sbs, counterboring[.]sbs, brittlebush[.]sbs, noematachograph[.]sbs, hemimetabolism[.]sbs,

TYPE	VALUE
Domains	spendthriftiness[.]sbs, misalienate[.]sbs, smartville[.]sbs, refractorily[.]sbs, syllabication[.]sbs, uninsolvent[.]sbs, mammaterijekasumy[.]sbs, dechlorinatingdermatropic[.]sbs, axiologies[.]sbs, okruzihealdsburg[.]sbs, halsalkalindivvies[.]sbs, squeezably[.]sbs, contretemps[.]sbs, indulgement[.]sbs, viandelarkishness[.]sbs, cunyguddlefrodina[.]sbs, audiovisuals[.]sbs, perrputtnomi[.]sbs, azoospermia[.]sbs, metriconetimeagley[.]sbs, dundeelieflydeflect[.]sbs, juniorstwosometogt[.]sbs, nametagsweatseyelike[.]sbs, glubeulaufuggy[.]sbs, bootedpindusvalenba[.]sbs, rockerstalbertcerate[.]sbs, biltongpumpsiecrumrod[.]sbs, jossesdialykreamer[.]sbs, ingressfloor-walker[.]sbs, freamingrafttwoway[.]sbs, craighleserapic[.]sbs

Note: Refer here for the comprehensive list of Raspberry Robin IOCs (Indicators of Compromise).

References

https://threatresearch.ext.hp.com/raspberry-robin-now-spreading-through-windows-script-files/

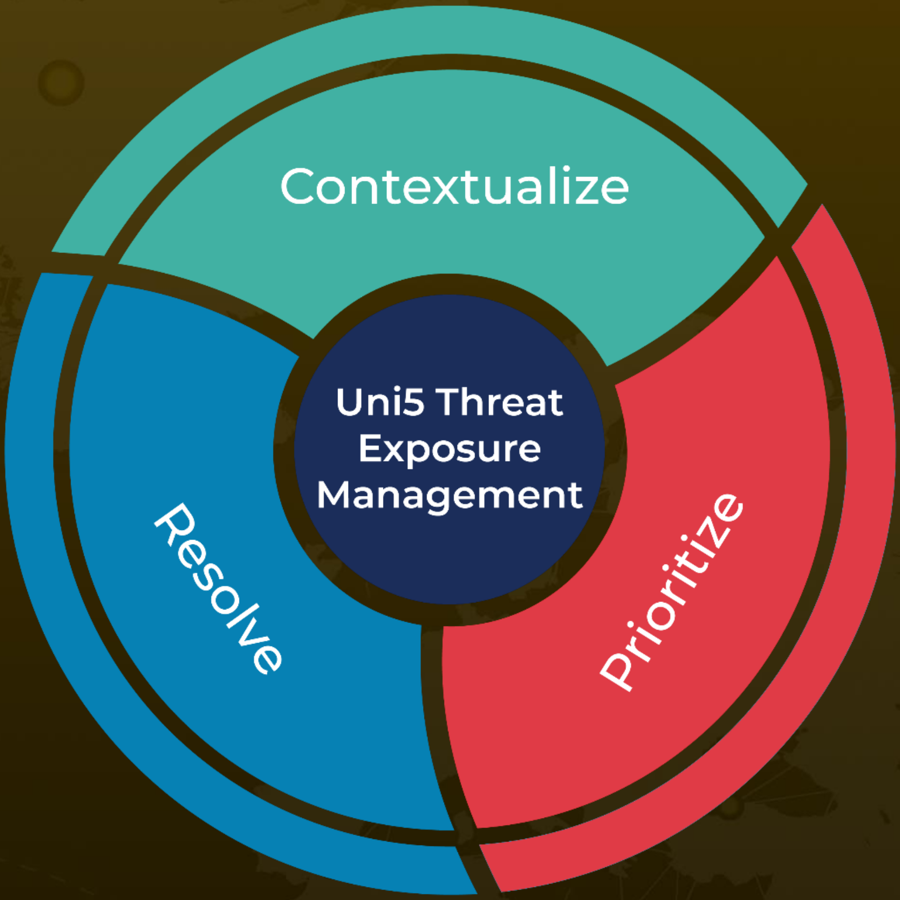
https://www.hivepro.com/threat-advisory/raspberry-robin-worm-infects-multiple-windows-network-devices/

https://github.com/hpthreatresearch/iocs/tree/main/raspberryrobin

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

April 11, 2024 • 5:30 AM

More at www.hivepro.com