Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

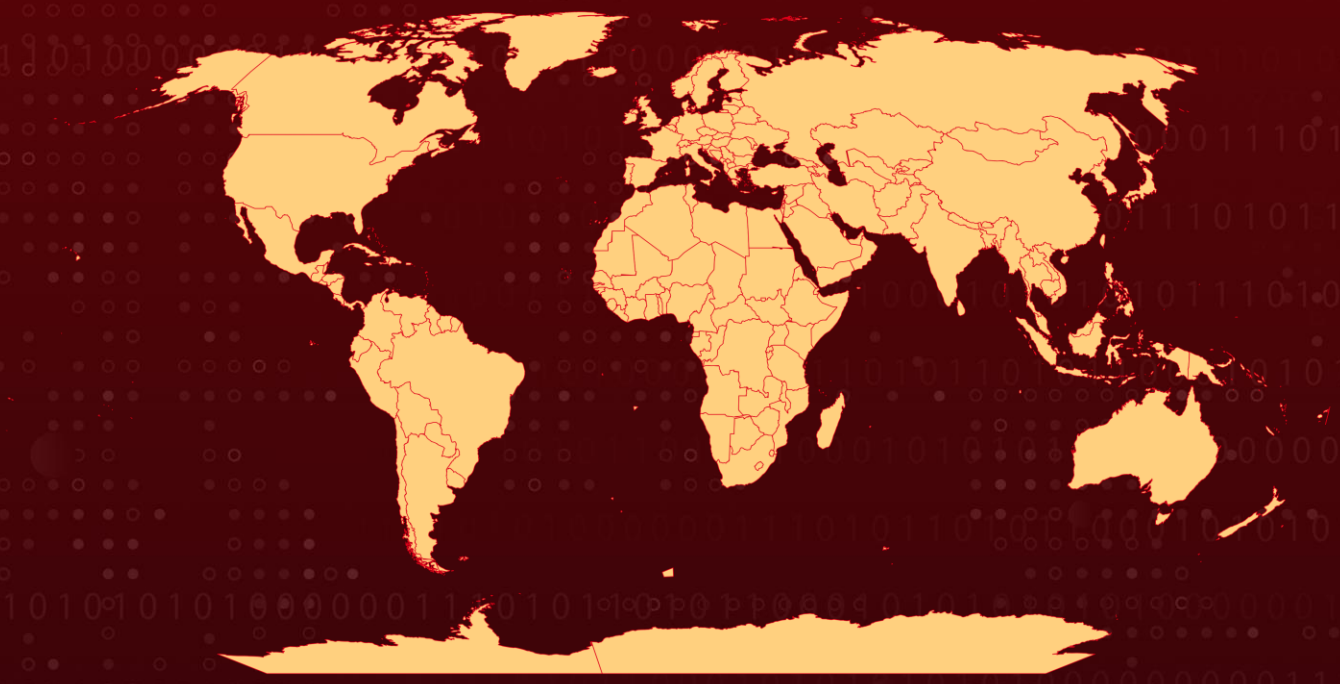
Windows SmartScreen Exploit Paves the Way for Phemedrone Stealer

Date of Publication	Last Update Date	Admiralty Code	TA Number
January 16, 2024	March 4, 2024	A1	TA2024017

Summary

Malware: Phemedrone Stealer
Attack Region: Worldwide
Attack: The Phemedrone stealer malware campaign exploits a vulnerability in Microsoft Defender SmartScreen. Phemedrone, an information-stealing malware, is designed to extract data from web browsers, and cryptocurrency wallets.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓

Attack Details

#1 The Phemedrone stealer malware campaign capitalizes on a vulnerability within Microsoft Defender SmartScreen. Phemedrone adeptly extracts data from web browsers, cryptocurrency wallets, and applications such as Discord, Steam and Telegram. Subsequently, the pilfered data is transmitted to the assailants for deployment in further nefarious activities or for sale to other malicious entities.

#2 This sophisticated malware not only captures screenshots but also compiles comprehensive system information, encompassing hardware details, geographical location, and operating system specifications. The ill-gotten data is dispatched to the attackers either through Telegram or their command-and-control (C&C) server. The Phemedrone stealer, earlier coded in C#, was actively maintained on both GitHub and Telegram, fast-forward to March 2024 a .NET variant has emerged.

#3 In the most recent campaign, Phemedrone Stealer actively exploited CVE-2023-36025, a security bypass vulnerability within Windows SmartScreen. This loophole is manipulated by enticing users to click on a meticulously crafted Internet Shortcut (.URL) or a hyperlink leading to an Internet Shortcut file.

#4 The URL file initiates the download of a control panel item (.cpl) file from the attacker's control server, subsequently executing it and launching a malicious DLL payload via rundll32.exe. The DLL payload serves as a PowerShell loader, fetching a ZIP file from a GitHub repository containing the second-stage loader disguised as a PDF file.

#5 Upon infiltration into the compromised system, Phemedrone initializes its configuration, decryption of necessary components, and extraction of data from targeted applications, utilizing Telegram as the pipeline for data exfiltration. The threat actors exhibit a heightened level of adaptability, swiftly adjusting their attack chains to exploit newly disclosed vulnerabilities and maximize the extent of inflicted damage.

Recommendations

Keep Software and Systems Updated: Regularly update operating systems, antivirus software, and applications to patch known vulnerabilities. Ensure that security patches from Microsoft and other software vendors are promptly applied to mitigate the risk of exploitation.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration	T1059 Command and Scripting Interpreter
T1574.002 DLL Side-Loading	T1588.006 Vulnerabilities	T1055 Process Injection	T1059.001 PowerShell
T1083 File and Directory Discovery	T1082 System Information Discovery	T1211 Exploitation for Defense Evasion	T1105 Ingress Tool Transfer
T1659 Content Injection	T1566 Phishing	T1041 Exfiltration Over C2 Channel	T1018 Remote System Discovery
T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1053 Scheduled Task/Job	T1053.005 Scheduled Task
T1059.005 Visual Basic	T1543 Create or Modify System Process	T1012 Query Registry	T1590 Gather Victim Network Information
T1590.005 IP Addresses			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f32964087462ba3c96a87ee8387f89de8fa605f2f5bb84cb5f754cd736683f2d, 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f, c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66,

TYPE	VALUE
SHA256	a841cd16062702462fdffdd7eef9fc3d88cde65d19c8d5a384e33066d65f9424, 815b2125d6f0a5d99750614731aaad2c6936a1dc107a969408a88973f35064c0, ccd19ef6e81e936fc944ebafaefd2ad99ccd11dd15fbc7d3460726bb38237595, ea9b0dee3b7583ce60bba277e2189acb660284abf6b3b9273b6a60c85b0a5ce3, 9a96406ae06b703d827fffd1f1ced0781f89ca2af6d5041721e9fbd2647c8430, 22236e50b5f700f5606788dcd5ab1fb69ee092e8dffdd783ac3cab47f1f445ab, 1433efd142007ce809aff5b057810f5a1919ea1e3ff740ff0fcc2fc729226be5, ad513d2cba6cc82a50ee6531b275e937480d8fee20af2b4f41da5f88e408a4e9, 7c0a1e11610805bd187ef6e395c8fa31c1ae756962e26cdbff704ce54b9e678a, 4ae28a44c38edc516e449ddd269b5aa9924d549d763773dcd312b48fe6bb91ab, c9743e7ffb6f6978f08f86e970ddb82e24920d266b32bd242254fbf51abfe6ce, c3bfaa1f52abdbb673d83af67090112dfdfe9ea8ff7a613f62bd48bace205f75, 6bd8449de1e1bdd62a86284ed17266949654f758e00e10d8cd59ec4d233c32e5, 4446d5b475ce8aed5244da917ae42b6cb9744ffc4efd766af8e4dee7dd5a3e19, 70c23213096457df852b66443d9a632e66816e023fdf05a93b9087ffb753d916, 69941417f26c207f7cbbbe36ce8b4d976640a3d7f407d316932428e427f1980b, e2d19a23b19a07d35d16990e78c5cfaa3dd97b9ce92201f4db18a7da95fe6ff8, b7f53c507a1aa4254b66a883285e27b42d65ea4ea4206fe674e0d03738f52141, 4ae28a44c38edc516e449ddd269b5aa9924d549d763773dcd312b48fe6bb91ab, c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66, f24a8b3144e89b9bececfbf76add87ddefbd19a024a85692026e97f3a9911902, e64b185c149cb523d13cb46ea3911e2c0595b6f10ae86e6a14b15e8d45c0cdcb, cb58bf466675be9e11cfb404503cb122514f47b9708d033e381f28a60535812c, 80f88566fda41ebc1b4e35d89748a804740bba0d03049c33c536cffd5e0491e2,

TYPE	VALUE
SHA256	4a36cc607ca5c2acc536510fd1b0ddd43a9403dac168d2420d474611909ed9e6, 89caa1568fcff162086dae91e6bd34fd04facba50166ebff800d45a999d0be8b, 188c72f995ebd5e1e8d0e3b9d34eeeec2ec95d4d0fee30d2ea0f317ab1596eef, e326c1b9e61cca6823300158e55381c6951b09d2327a89a8d841539cad3b4df3, 4da33c7fe62f71962913d7b40ff76aff9f1586e57db707b3d6b88162c051f402, ff44e502bd5ea36e17b3fc39b480e65971b36002f27fb441e4acadd6bf604a20, b7980f64f892d70b1cd72a8c80f8319f50c3c410aba4e4bc63fd6494bcb4f313, 480fae3bdc2604cba846779dd7dced95b3ce036bdef629ded247771a2e4d5d58, 348aea633c99e5f6a0ac7b850961be0a145a35678e5bd074b4852f7a2419f518, 1c53dffcb4c474a2b08708609466e7d234d6d51139b6532af54fac5bb8d37415, b37ec923451dd15a0f68df0b392b0f1b243fe50c709de9e574ac14cf6fabdd53, f2814a4b3796fb44045c33b9d0d9972bf40478e5bc74b587486900c6cfa02f3d, 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f, 8b73d7aa8bb8db8a9ecbf9f713934fbbb5caf4745d7a61a6f34a100c4d84fd9d, 9b9ba722b314febfc44919551a03dde1539f115333183c2cb5e74b8e644ba5b3, 568b4b868b225f06bb34da0dc23603c9dedccc2b319353407c814983d5322563, 5ecad303475e180f8879871d8571d1a7eeb99e0b3c63cc77fdd02cb9b8c51211, d5b1214f1817a16b2bc8a76daa48c9a3c5af0e411cf4f0c17b0e364d437a454b, 5f0ff1fd6ca89a0ddd3178e023dea8f79ff3c3f3d8ff7900378eb014e83ed326, 40c6fa38e44e00d8cf113d0a079cd46f8b7654331f12e50d2af5a9f1ddc6d266, 3a34cd3a3221d83a1cca8913b2afbb5b780027d48b44d3ce15dfe4a402064871,

TYPE	VALUE
SHA256	38279fdad25c7972be9426cadb5ad5e3ee7e9761b0a41ed617945cb9a3713702, b7866dff1a56d27aa55caeeb55973fa76e30eedc1e3349fc3ddf5af810f23f72, 35630220b3ae942a4c3061981f9205a897ead5b58936747ffda871babce93d55, c969e6bd943c6476eb441a70f17788fc24de61a08cc2c53cec97b384f17e4cf6, db6fa8cecd6ad1647773914e0f1b07a85ef6e1171e610069feb42122adbfea29, 3f92262cdf4ed977b0c1137a5f011c67d665027b2e450867004c7e8409efc432, 1fdd63b4b1db9637871a4f574c746980977accf2a0f6c3ceaef82b6641a3e9e7, 97b467d4aabe790423c065f4fbb20f0e04a5af0002347c0e627726008cdd2aac, b3cf2db37a84c544b3ac466518d83b8b56c0f4e5da88b71ded00e20e3ff48c81, 031a346e370711ec09c56512f76bbce87fb2f2294f35e8d7b13c862e63e26a52, 4392360173d0f38bdd5c08a81ecd7703492532ba8b21ab9f9cfb4b068efcd82e, d1933d7741d2c5ff810f37ecc0fc2b04d4d6d7daf05450a9ffd29c35d2cb2c05, 3f26678afb3570932264d4414e61764998a6164d4516685287aa18e848e0a70d, 99fee366033c5699b2970c820f389ac3ca0ed1d19b17bda02fe57765a47bb5b4, 8873bffb719dfe5a4fdba98f04bb61c079eb678c93079851cd34ebadcc9e2e26, b31185a0d4d7d84a3beb7f81f545ddfb057d6047d022b69d9fa69aaba1fafca2, 95689e1b1e7abec1e0eed477c05c44867b06a1003c46829968e9851054174c3f, 8731e05790767c76250fff12cf1ecbf497889776be13aef569cc71f0aad97039, 5a9d4557fc72090010a587b6c20bf4cfb38134ba636c3f496e747eba9231910c, cfc09388265be4e0c64d627ae997ce9e38624ab45228971fea8ca761c4f6ed73, 7cefd001d84d72a8d9c078c4f24732d0944691b038fd3783fd805626eb4954cb, c62d1d7718106fd9ee3c8f256b6fb9866a5a996c9e0610758db3304914a443b5, 1fee8279856072c3036ca152ed062609f111d6c434d9ee8fe8ad6eb69f03c5d9,

TYPE	VALUE
SHA256	3e103d47994d5cb6f198147cb050ddae313e14dbb16de677b7e4d3b0816e0530, 9750e572ed0c71431f53409e3020e7b4f8b88bb2937971031969f1b8a4bcd5ba, ebb5175dc49675fca8793153ef73eb04d3e391669837426415a78c311e8bffad, 37862819b86590b3c52a10b2cd8406696a55829e9f4d3b1082bbef5d930aed11, 29b7e31d89a8c9ec5c99fa5bd9d2562fc770ea42cf530622b5f9655a2e4469a2, 5b1b6e7eaad23c4d4be1ab8ba824bc64ba8e4a7eed125827efb2f7d97bc269ab, d1546aebc8e5787ed91b3cb9a2dbf43603438361c3b7db31d619ce3aaac109a6, 08037bcd11dd6cb47f2234f6d322997b1a0f42fc456434fb1191bd4e79cf662e, 4401571684fb386d81b34b0ecf7fa6452728c2016e12e772c8354f1ed7ec6e20, 26cc1c8139f9c595715327bd6ef258f9f1d8d2b005502919818f0c611cddcbd7, 0df623b4e710fd97a84d364d383ddbeee36beb19316b06437fe80dd9be295540, 73f21e4c51e183cdcaa7e5df01b0c3738f01ad7fe0f98198c60c7d519c5e9c73, 59c0dc33006e007304c0d407d5b138c1f9c0ecaf2bf53acf094cd49474e72676, 7abd9df84ba376dd79ca84a22be1e46e0cd3a7fc90e8fa45848d53cce0a05725, 9d0c23542a94064c3372c2ac13ac150904e9ae97666465437b9388789f56976f, 9a2251cd0659f32759f589124a0aec75a046d3137fcb3138dacd87c087d38768, 65cd2776426e19b902d87a88179d10789d3ba1f226a52821bb81df872f0bcdbe, 252eb46ece2f4c53e1943d61c64a39729beedc250aa2aeccecdb7b2d2222804a, 4e402c4ea4aea068e6be7278dad760824e046895f572ecb34d9bcac8646c1f61, 097ee22514e22938f10c32a70ffe6aea00d8a85fb71e595dc34aa2699ab2c5a0, d67b4d1d78725a4f9542ed450d9316133d42d10a4c40358e271700271aaf5b94, f3f43ba0527be4cee9db86b29677ac9a4b069fee5c1bbe7c0712183a421b9a5f, ca811fc768eab9c2b42314b5f41f4125789be4eed40a61b13af06c8362be55f7,

TYPE	VALUE
SHA256	882f21a0cc459a7bd4ce58988bc64a247b209873c20588893733cdd167156e9f, 56e19a889098729742b165d8e496eea3a4e25bc8918fa4b39dd265df472020d6, 9cde7d0276e36d93a904e718a8556eee0a796867f3f3374dcdaf69601694efe6, 62a764ce80a9b36516220bdfee931bb0924ea4ceb2a876a46e6fcb37a5b89c1a, 4966b71d315bae779a6e99782f868ed38d449ab801381068e67dbb2bb65adde4, db1f7d38c4b9f6e6290e10eb22c53079470193540ac95e3c14e8fe1be2179b1c, d4f3ec0f1a86c35afd65978c83a18a3ad44f3b3fe3187e79131ab69043368f4a, 7edf0c3a805516332246ad912dfb54e8386aedda46978d52a96a0a5d3b4581f8, ea3127063dbc8f1515424cda85fb4decb95898e2dfe81bc240ffcf183e2c6cd2, ed06c02a3353005d07a7b1c20ed54acb84447ae241aa7697f669fcc27f1f52af, 49263d326c6fd96b0aa0e125f73c13be73fa68208e5b3d552f8297c456a28378, e4c74b33bf933feb83c9dc2cf34b3cff78ed9439e4998aee1752de34530b68de, 3dcf9f12ea99bae5197ec46384779361b6a315a996af886c845dcb83f8569411, 9904422c4abe22f0cbb40893aa17f3ccb4ef40a3120333dbf9710e0a31930560, ab61ca0ffd4903334d4d35629654a5e7ddbf7981578f8c55bc9a114184b6b3b7, 0f9e01f100f9cd8db400504d5994f5c8232c318578bb33b807710289d9ef480c, 08ed769b18f1f3eca36f072f6b296061114022bae51e6d3baeaef46014647162, cace4237aba39368fcf37803e0f28fdeaad6a99cc6e80503f730b1970bf437b9, 1b9033d03ceea48f759324f56e1c63e25ff7293894ab78deabda4f1c7f25d6b5, 950c2390aff0efa320d0ef651a1e22d68549d9dd966372bb3545e4419448502f, bd442f310cd4f0877153d4c5e30f972d99cd0187639ae891f038c32b50596820, 8e2bd38da4c106d07fa03ea2d9a3d472ce1e2d4fe004770b400595e36dc8cd18, 0ad35643f11aa64a0de00e2cece01757e251e1fe04d915ac2a697485da5cefc1,

TYPE	VALUE
SHA256	ed832791b94069c53a30c649632819c5c8ffa28cfab5a7c2b8b7c27c54f8ac31, 2b80f861472785297ca0640bf2d4bbb2e1368b1399210d0f5611d5280afd5309, da54dc88b7a473a0ff63f04efc0df313f999115c81f9c9129ac8c94608e33043, c5ec6a46584584988be1366d29cb8d3c3e5e865d6ea958544ef2f14fc1fac422, 5702a7aacf503744df00a600dec212db82ea1e815c778f932682b15476f700a9, 9a289049bbeef81ee7b62c68ac930dec51d0b324bebf876eaf23d4d914cc5bea, fb33a0615fea2eaa9ca908d07cebe8ed0d5d7630166eae85ddb6864019dde7be, 8821798e2abdae6bdc11d95968f1945173091e9720021f239b1cad21fd878154, c9227413f759cbb2e4cd79a668ab3c6778039f0a6cf27e17d3881cb17f1b5853, f4bcd511195454d82e1e4fca47392147407b869a8ec04f6535349806bfae4976, a33cc3be8b09b9aea9409f00f3576dbd2b9466854ba38b0c21000bcf25c81c26, eebdeac6e6bca0a720c047291a85dbb4e0c17f18af0e20b8a0c645360ae66626, 4b3c15c249b6b526de64374cf74406abf2d16e0a579da26825028abad9e200d8, ec1ba0d1d568269539bf13058247b3a2ba2fa7c86bc9811a44fd68193eef1780, eb76cba8d70e45912e9e76ff2c12a2954511a95bb3a0066200a9a3f39ce066f8, 46a2a63da434d0ac34a632274f843624ed3b8cb2ee32208506746bd467340e71, 36854edf126247498cd112fe13528cfc704ebe60f4b806d79919f28a5b52a0ab, 7cf968a9307034d3ac5e467e6b9ca2e22d454648f473a47ed10a0ed589dec261, 566b7c859360f82c5b2bf28b0f3e33ec440395fdb4170141eb02952e8e6dd1f0, c62b294ae3209354bdb59db74b6b6a22482fe9625965285ed450ea688ff20f9b, 2595dc056e7c9a879c282ebd6cb7cf2142a1ed3dd51eb6c5fa0464d2888edf98, 967139f9b4870d88b7e3ba65a9a39989bd34b3b42c0b09d7d625dff838cdb79a, 98543e76fbba4b53ba07efaf545fe4a941037e32368aab66b8f34e95fab1baad,

TYPE	VALUE
SHA256	7a1f79bbee9a99a34125266bcda1a9619768045bea3d913481654bff3484cf9c, f7b78b5ca9a5491ad51dd7b98fd04495134de1fa0b9c475bca4a5357453f2e09, 53a4d8aa480279be8c287814dc2e1766f6b74d49b7a26b7f2d39eb4e01bf874c, a0f7a1f6ff7060e3ad4076998e96727a144c2864c6850819302790fc2c0eac79, 9d1d2b72b84b8a546114d0578e65173b26f7b87c1725d7a611880ada0b018779, 3d39d813b0ef99f82822c651980ba4f3dd3b2580cefeacd53f6722e1def3a48b, 4ee81cb5288a5941cc37114c8bec7287ac5abf5587152ffa367c46207b58d0a4, 4dd94ed92e97e9c8bf5ebd8e6083c417dfb4ac920a44673e65c88b77fea14ab9, 52b443e6c8c88a269c859ed7cb1210bfd4ac2b3a20f49c8716904828ebbfaa4c, 6cd12ca930abada4cfd30c4244e99a19699732832fad9b6b8f980c94d75189dd, d97b3523922ed89de611d2eb0dcd48b4bf19792657016ee4751545dd0c2f8a72, aab02cb9ba573ddc586376e4da538348042b85ae60fdcf4584b54c61c1fd4261, 3c8dcee34183d3c759f2a949aa37efa9d877fcd77ed90959aaa0ffc80076cddc, f432784cfabfc472903c27c8bc7ceeabd9d1c8e1e426e829fd2b2a1b567e6b1d, 3c75421d04636ab0c6224f708e477f708fb4f368688fd5f9ae50cf3ac610a49f, 1e2c99bb70ad10f763d912a5e508347791e12377e913c06045ee1aa49bc05daa, 2e6e0d8fe020acaff59e3c2c829ad6bb2d7b5b8e493948c004f99df5536b0357, 7a0a711fcb31932b7153274aa501ae0aa6f98b68642a3643370b5afe13e842f6, 42c3892e410fddd167d60b5ffffd8ba833f020b062272c4d94082ed828736a64, 49b33dad6320244156edae280845752e6359dc9776c328eddbc9e37aaaf5c25a, 505e269439241067ae3c00b0dc3cc40131eb7e1f0cc444fd9ee75baab03aa53f, a70d71ad3b1284fc4ddbd47b8d210a6d9b7f9acae6c2b23d40287283d6d2de54, 98e2d6e09ba9cb55b9127d1cbf38e4e176b57dbf9e2fa03e397d140c60764582,

TYPE	VALUE
SHA256	0cb17b09ef57b9db9a2bcdd554d34714b538f5429aef7a40ec476abea126dc1d, 893fa53d6bdc8119d80992ff000c547c5e38eed122fe2576f060e88ded398dd1, 26156443dcbf7d8b4a9cdc4ba751b75010e29da99a307f97ef294285c84a98ba, ed7bff0d2725651d085a06e1cb88d379e3eb511a9a733ae3e419b764c34b1bcb, 56cd278e566cd4d3b6d525e948e8a84a32a5cf4b2774d75f772d8271898a688a, 8a6a2e1250af57505a41c67315da1240002b3359d23b1f24d343567d2699536d, f14b2b101a0c3286379d08196639b6d0fab3fea087d67dc0055b3e1324ca9bc1, 760c2cc6a7358a0a60f8652fc8022517d63a623d12cace40a8cd500edebc7191, 64503745802796c734b5c3b6e62a5ba2b40fde46fe5a3ea1e8f7b37b49b2df92, 131d1dc92442a44ed507de20c901581097ee70761e03805a065f59dabca54ad0, 24d523b3c6e96b088a7c013135fa5b9af34c3f79c77d43f325712201f0ed76a3, be32a134ad05875030589acd7f066e0f84a9fa2083ed4f368075b6fc5cd54b75, ccc3f58337ae5ab5919e7b6f84e9fa8049bbacb8ede98f53375fbc5dd6020a85, 56a28cc812c4bc9390585f7df1b8379dacb3a80e1ef8854b482521c45dc4cacf, e4d7674f35fbcde4122d4964416f1dcf78bbd8b876e0af090ce04293e51ae949, 96bf34b5bc11543e62bce7d8f81f10c08b0b570d1e9daabcf5de8a3384aa9aa6, 454b0ba2f890f8f4f487a4aa519bf471d7ed0c80fa273b196e52a7775e003a0e
URLs	hxxps[://]raw[.]githubusercontent[.]com/nateeintanan2527/Joyce_Data/main/DATA3[.]txt, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1175808264479449138/DocuSign3[.]url?ex=656c93c7&is=655a1ec7&hm=6e8b316f2112cfaf27bc8cf35089098e4a0f2d16054e8d199c13588c31b2e383&, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1177255995156742144/DocuSign4[.]url?ex=6571d815&is=655f6315&hm=f9e208714ffc862f97cb6363fb887f11fda0020802a020a56a571c4195114854&, hxxps[://]shorturl[.]at/ixEZ7,

TYPE	VALUE
URLs	file[://]51[.]79[.]185[.]145/pdf/data4[.]zip/pdf4[.]cpl, hxxp[://]51[.]79[.]185[.]145/pdf/kay[.]zip/kay[.]cpl, hxxp[://]51[.]79[.]185[.]145/pdf/data2[.]zip/pdf2[.]cpl, hxxp[://]51[.]79[.]185[.]145/pdf/, hxxps[://]shorturl[.]at/flEK5, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1167767477921513512/SecureDocuSign_pdf[.]url?ex=654f5336&is=653cde36&hm=08ea24126262ff865a1ab0c79f20e41e9e53896d9cda8e0c374c077f5a500b00&, hxxps[://]shorturl[.]at/vzAD2, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1170627585105997854/DocuSign2[.]url?ex=6559bae5&is=654745e5&hm=ab8a5d275414768c20bd9a8a0e434c4b8fe7c0bd8006c3b5f69cc80b7fe57cb1&, hxxps[://]shorturl[.]at/bsuCR, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1170627584627855481/DocuSign1[.]url, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1170627584627855481/DocuSign1[.]url?ex=6559bae5&is=654745e5&hm=acf93c3a4f79068689d20d197ac297533dc28d94bb93f4ec1021c7c258c8dbda&, file[://]51[.]79[.]185[.]145/pdf/data1[.]zip/pdf1[.]cpl, file[://]51[.]79[.]185[.]145/pdf/data2[.]zip/pdf2[.]cpl, hxxps[://]shorturl[.]at/flEK5, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1167767477921513512/SecureDocuSign_pdf[.]url?ex=654f5336&is=653cde36&hm=08ea24126262ff865a1ab0c79f20e41e9e53896d9cda8e0c374c077f5a500b00&, file[://]51[.]79[.]185[.]145/pdf/data[.]zip/docusign_pdf[.]cpl, hxxps[://]shorturl[.]at/clpIO, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1171355007245893653/DocuSignDocument[.]url?ex=655c605c&is=6549eb5c&hm=2aeb65239a890e6b070957136681600ca33584e578816faeab471a5e11004538&, file[://]51[.]79[.]185[.]145/pdf/data3[.]zip/pdf3[.]cpl, hxxps[://]shorturl[.]at/eqxU0, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1175808264479449138/DocuSign3[.]url?ex=656c93c7&is=655a1ec7&hm=6e8b316f2112cfaf27bc8cf35089098e4a0f2d16054e8d199c13588c31b2e383&, file[://]51[.]79[.]185[.]145/pdf/kay[.]zip/kay[.]cpl, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1177255994775064717/kay[.]url?ex=6571d815&is=655f6315&hm=5edd3e4b0cc773a06fe9f1a8177f99239a105079f23eb7707c225be4867160df&,

TYPE	VALUE
URLs	hxxps[://]shorturl[.]at/dMY69, hxxps[://]cdn[.]discordapp[.]com/attachments/853270434422456330/1184415259717533726/My_Photo_Album[.]url, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1177255995156742144/DocuSign4[.]url?ex=6571d815&is=655f6315&hm=f9e208714ffc862f97cb6363fb887f11fda0020802a020a56a571c4195114854&, hxxps[://]shorturl[.]at/ixEZ7, hxxps[://]cdn[.]discordapp[.]com/attachments/853270434422456330/1183676616564547624/image_reported[.]url?ex=658933c1&is=6576bec1&hm=b60477e0a798182a1dc0ea65def7305b111ce06a398667a1c567b3f9afd253b2&, file[://]51[.]79[.]185[.]145/pdf/data2[.]zip/pdf2[.]cpl, hxxps[://]shorturl[.]at/oORV9, file[://]51[.]79[.]185[.]145/pdf/data3[.]zip/pdf3[.]cpl, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1172211288303206400/DocuSign3[.]url?ex=655f7dd5&is=654d08d5&hm=26a68927b4c05c243d910f3a5ebcf2c6ec43bcb7f460acd45891b3b21b308cdc&, hxxps[://]cdn[.]discordapp[.]com/attachments/853270434422456330/1176802586481922098/image_reported[.]url, hxxps[://]shorturl[.]at/gnL15, hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1170627585680609280/DocuSign3[.]url, hxxps[://]shorturl[.]at/dKOR6, hxxps[://]github[.]com/nateeintanan2527/Joyce_Data[.]git, hxxps[://]github[.]com/nateeintanan2527/Data_Document[.]git, hxxps[://]raw[.]githubusercontent[.]com/nateeintanan2527/Joyce_Data, hxxps[://]raw[.]githubusercontent[.]com/nateeintanan2527/Data_Document
IPv4	51[.]79[.]185[.]145

Patch Details

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025

References

https://www.trendmicro.com/en_us/research/24/a/cve-2023-36025-exploited-for-defense-evasion-in-phemedrone-steal.html

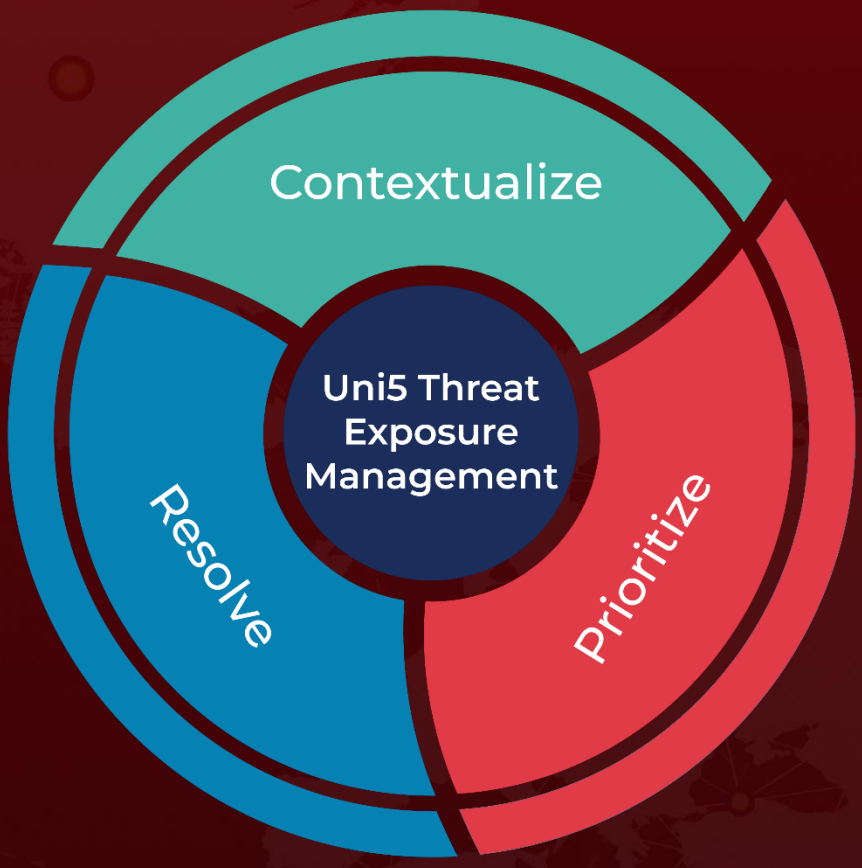
https://www.hivepro.com/threat-advisory/microsofts-november-2023-patch-tuesday-addresses-five-zero-day-vulnerabilities/

https://www.splunk.com/en_us/blog/security/unveiling-phemedrone-stealer-threat-analysis-and-detections.html

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

January 16, 2024 . 4:00 AM

More at www.hivepro.com