Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

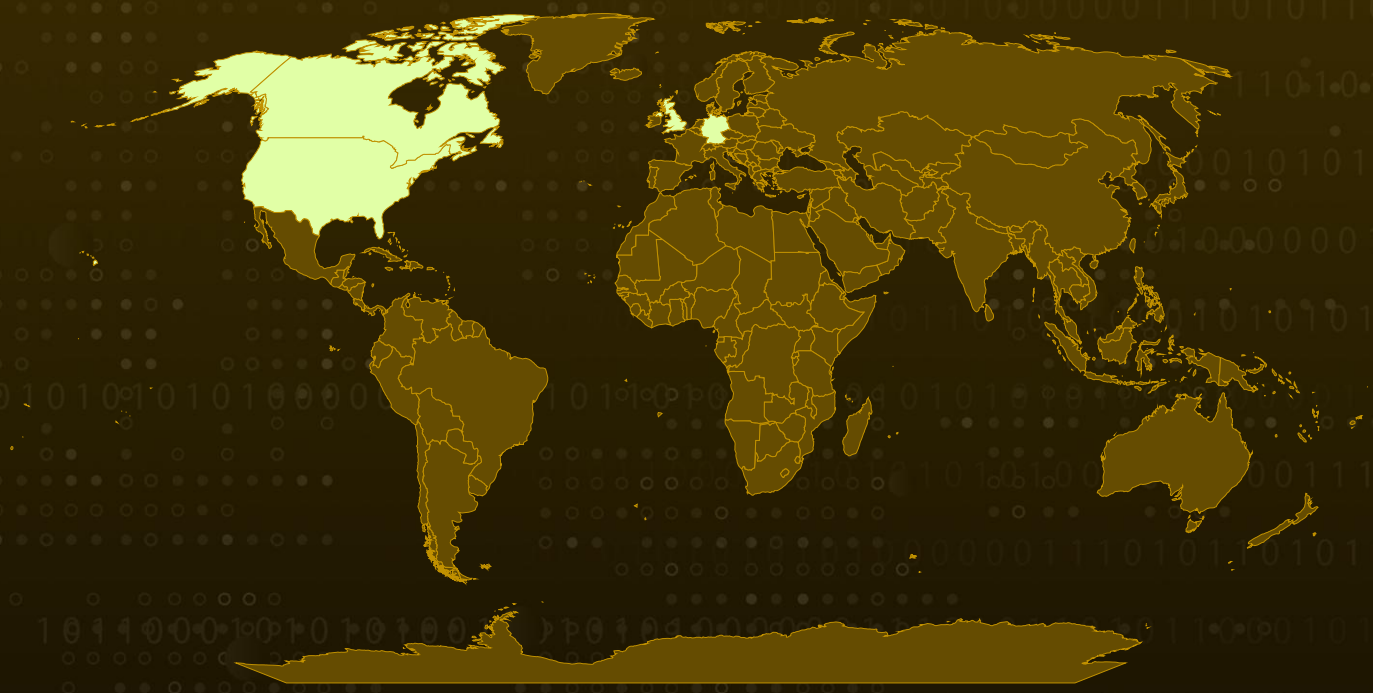
OBSCURE#BAT: The Deceptive Campaign Delivering r77 Without Triggering Alarms

Date of Publication	Admiralty Code	TA Number
March 18, 2025	A1	TA2025081

Summary

Malware: r77 Rootkit
Campaign: OBSCURE#BAT
Targeted Countries: United States, Canada, Germany, United Kingdom
Attack: OBSCURE#BAT is a stealthy malware campaign that exploits social engineering and deceptive downloads to infiltrate systems, primarily targeting English-speaking users. Once inside, it deploys r77, a powerful user-mode rootkit that manipulates system processes, hides files, and alters registry entries to remain undetected. With its deceptive tactics and deep system integration, OBSCURE#BAT poses a serious cybersecurity threat, making detection and removal exceptionally challenging.

Attack Regions



Attack Details

#1 A newly identified malware campaign, OBSCURE#BAT, has been spreading through deceptive file downloads and social engineering, tricking unsuspecting users into executing highly obfuscated code. The campaign appears to be aimed primarily at English-speaking individuals, as evidenced by its lure documents, filenames, and websites, all of which are in English.

#2 The infrastructure behind the attack suggests a strong focus on the United States, Canada, Germany, and the United Kingdom. Once the malware infiltrates a system, it deploys r77, a user-mode rootkit engineered to manipulate system processes, obscure files, and alter registry entries.

#3 It secures its foothold by embedding obfuscated scripts within the Windows Registry and configuring scheduled tasks to ensure it runs discreetly in the background. Additionally, it modifies registry keys to register a counterfeit driver, reinforcing its persistence and making removal far more challenging.

#4 What makes OBSCURE#BAT particularly insidious is its ability to remain hidden through API hooking, a technique that allows attackers to intercept and modify API calls within legitimate processes.

#5 This grants the malware the ability to mask its presence, hide files, and manipulate system functions while avoiding detection by conventional security tools. It can even erase traces of its activity, making forensic investigation and mitigation efforts exceedingly difficult.

#6 By combining social deception with advanced stealth mechanisms, OBSCURE#BAT poses a significant cybersecurity risk, allowing attackers to deeply embed themselves within targeted systems while evading traditional detection methods.

Recommendations

Enhance Endpoint & Network Security: Deploy advanced endpoint protection solutions that detect obfuscated malware like r77. Use behavior-based detection to identify unauthorized registry modifications, API hooking, and stealth persistence techniques. Regularly monitor system logs for signs of unauthorized process injections or hidden files.

Improve System Hardening & Access Controls: Disable unnecessary user-mode rootkit functionalities by enforcing strict access control policies. Restrict administrative privileges to prevent malware from making system-level modifications. Implement application whitelisting to block unauthorized execution of suspicious scripts and programs.

Zero Trust Architecture: Implement a Zero Trust security model, where all users and devices are continuously authenticated and verified, regardless of their location within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0011** Command and Control	**TA0010** Exfiltration	**TA0042** Resource Development
TA0040 Impact	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1071.001** Web Protocols
T1132 Data Encoding	**T1219** Remote Access Software	**T1014** Rootkit	**T1027** Obfuscated Files or Information
T1027.010 Command Obfuscation	**T1036** Masquerading	**T1112** Modify Registry	**T1140** Deobfuscate/Decode Files or Information
T1055 Process Injection	**T1620** Reflective Code Loading	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1059.003 Windows Command Shell	**T1204.002** Malicious File	**T1204** User Execution	**T1071** Application Layer Protocol
T1053.005 Scheduled Task	**T1053** Scheduled Task/Job	**T1583.008** Malvertising	**T1070.004** File Deletion

T1070 Indicator Removal	**T1106** Native API	**T1082** System Information Discovery	**T1518.001** Security Software Discovery
T1562 Impair Defenses	**T1562.001** Disable or Modify Tools	**T1102** Web Service	**T1574** Hijack Execution Flow

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	*[.]gl[.]at[.]ply[.]gg
File Names	sip.zip, Eternal2.6.zip, eternaltool-main.zip, Darius SS-2.rar, Darius1378910 project executor-1.rar, Test.exe, install.bat, Loader.bat, downloaded_file.bat, chiani.bat, TorServer.bat, AdobeUpdate.bat, nouaconi.bat, oni.bat, uacbypassv1.bat, CVerify.bat, cloudflare.bat, newest.bat, Mous Fix.bat, repair.bat, sus_bat.bat, 32ram1.2.bat, img.bat, Eternal2.6.bat, Loli.bat, Darius1378910 Project SS.bat, Bootstrapper.bat, test.bat,

TYPE	VALUE
File Names	Java_installer.bat, install_apache.bat, python_installer.bat, installer.bat, ChatGPT+.bat, share.bat, uacbypassoff3925.bat, uacon31025.bat, AsyncClient.exe, autoruns.exe, DefenderUpdate.exe, qexplorer32.exe, rem_edge.exe, rem_edgev6.exe, $nya-qX6Pb164, nya-dll32.dll, nya-dll64.dll
IPv4	88[.]222[.]244[.]187, 150[.]171[.]28[.]10, 195[.]211[.]190[.]61, 147[.]185[.]221[.]24, 138[.]197[.]66[.]62, 185[.]128[.]227[.]28, 100[.]28[.]201[.]155, 37[.]114[.]46[.]25
SHA256	e33e05d3182f46f65554fda2127d9d1d415a986b6c635485b323558a1821f56a, 5f7ee1c0fdb813fcf6d8a8e136940ad570bf544b1263c03d288a5ef1b90cf0f3, e5386db097dfc6bd1acde5302bc4b22309f151a478604713000bedb77484881d, 43cc98694575def427dd2adfb9fcb5e7018aedcda525b5e5f5877e3fd02775be, be725b2992385bdcbcf54c995ec1807275b761a019645f707498c958b36346ad, ff17477903ed742a4981f67515f1065689063703f86e0d38a1385e7b998084c5, 3367442f903d854aee965023734f25bfb4bca6c852d29dcb5774b9e64707ff4b, 47b28d3d1ab89e207f7d634b53622960931431dcbf73fc26875659a0c20bd70d, 504cc73800ed86c7627234a1d092efa14abcea667aa084191e34fff2a3edc167, 53d2b22b91f39305b436a08ef9280d4a8fa3bd038d834b1abeadb792f8e086a1,

TYPE	VALUE
SHA256	844be559debddec75f460faa912490dab6ea400fe325e59b91df250c1e1ad4fc, fb46ff16bf658aeb5f3a19559ae6afc10dd2ae108b8ae23457011d6dc5a4b560, f553759453259559ce7c4321898e83c9a3bddd14758aecbd1567634ca4ea8d86, f3b652503b20261b2f83d43efc1cc20c655b68a339805714dd95ed14f659d4be, f180a6e4a5ec5b6eaf82c2bb31ff041a66699387483e9eb489613dbc1bacfe1b, eddad50d490349749c5104c3394fae49dfd6e9070ba0000c139dd8e24e2a06ba, ea0dbc5ca8e96d8940337c5d19574498a4b398847049e62af14f1d98346638b2, e4cce18562fddc70c71a8969141c56adeb56032196f05e10524374c1eb398d7d, e2864bd791df7e060b43598f04be86c839e9907a1fa9c3614205b5139542d8c1, dcbc1a43e1ee9d4c4c5a426ce862b151973545111f69f5b1c036e46e801acc82, db82442d83c116211531f104b77adc5c45cf531315cafbd8f6e1f9c5dec6c0d4, d92c28680af30136dfd52852eddc07e5197afe039d84f5b2255b14ae8e15ac02, c08d8e742a34e9dc610ed5276e5cd0dcad4f6139a03dda07d9292d50ffd47d39, be4fadb015d35092f3ee59938a3e68c671de8c075f04e90fd819b61c383d4501, 9b8cae953c8f3dcb8e9e09d387d217fea8fdf07c5e3001813a26d83af7fcb4cc, 8f2541e5c425e6353ba1170079b238632acb21498415861c1fd27a8615a86336, 879b9ba401a3b8b580980ea31050a35dd849ad3b6e00338cb81d106bbc02963f, 7e658c7c9a1be6ebd7af0150fa6fa289d59822b4e771167e13bede5c9a622448, 7c2a3a41217da8a2a7d4b72bb5f0c5f45e2b7c6518526101f64b534070651dfc, 794d1ff3b3fe275b49138f82b0cc597c35e1fc0a91be3136729598d97f1086ff, 72c5f9a11f126b4d1b79ac81bd03787622f2109560ceefa762ea0c3a9e1a5e7b, 5f75a50ae9f6252d1f0f135726f4a605f4148ee36c9d36c4b2d3fa6404e03b10, 5322f5eeb9e789fe63a89ce7852c24593b8b2b6233d855a1646116c14bb8e88e,

TYPE	VALUE
SHA256	40f0a201e85e6cf32c48a0cfc496a55a4bb87e8c13174e6c583de9bf7ed70590, 3e88e710043b3cc9bf1af3b373828e9ef023aba5d697a82a9a568ae9e45cc544, 346ec63bddad6b1889d6647ed43dcd71432f687ba8642b726ac67f08e415d77e, 30a17c5c65fe87d961aea290e97e8aa09a03c20d257e22d8ac63f5a7b67c0c6b, 2da6d8fa510e66ae79bab6b12849b123bb9b88d23de3b0b383e7f48f9e9cff69, 2bc694a9a6fc03043472f6fb88d3eeda31722facf5659aa7eddb13c29a8fb754, 1f51f00b06d5c0358b662af01db9690d1eb379b33b1bf7a161ba2b6fe53d6574, 18d93547b1f14b452b7ad053a1a93122864d810d82a48ecc391d6d6b44ffd661, 0ae3e6a8af0d7657f820986291dab1f071007de4197214c976893eb78e8e200f, 0a20a60ef5151f8adaf9dcd819f970d9aff20d8eb8f905fba55ccc0e91c446be, 033f50893be3bb35ec8cc358d6d7fc764d327b00158617f8deac08a60e5f6883, 019ba14b03b42a1d3f3496659573e8ba9440340ea16166c3e294164f9bb8f3ef, d0c8c833e2de4f7d0d92febc6a9845cf2a2438013a9362cefe0878897bd322a4, 682f7884b06695a44f19077eb5cd21f1823347b070c8a3773bacebfc0439b8b8, 54cb466d399ce2d3fd24b1b800e276100c3272522ff84dab4bb1de73e5eaecde, ff22090e3e7d9dac05879802bd0312d282c8a9a44b3c9a7c6afd4b07c05624a2, fea5df5596be7448e2531cc352bd5a361e128bc6b15e1ac2ca9abe12927dfb83, f83d936e48bc89338ea9d639f39cf36c3ecad1e59551f18e2b6d8d5af6cf403b, eb673d5c936238eed457bfe41ad02f2081f3ef42dd5f3935a0bb11394574c60d, e060a451a4f310d4e4bc05a63b9027896b3126642182d8b176119b975689f217, c3dce9c45b659118211b573a802ecac94dede201d59b2a5dced29d68b7a82f3b, c1fe08defd1651508b32ffe38892b52a519570f78e457467ccacb6fae46b2439, bb276b2dd3726f3a712e0904ef87d41d133cd36a72ecb97da8cefc6ba0d33a30,

TYPE	VALUE
SHA256	ba8565d459cbcc972bbca96122881e85f5736f4e7b56383853190c95d0334b5d, a439f188be62856f9dc6668d11c691c031c1cb5a9574a5cab5cfc1856c7c7676, 9063336b99527f9f46b1d1f1d0db44143b30f478cc708e217525c58cde5fddcd, 8b10e9c4e8c475fb7357e97205a0e3c8857908dba93846f7c771e06726db99fa, 79b898274b1af26ac29f8bd23887244bb3766968b46d5e1012cc4485c6291ce9, 70fb59ac30b0fa16fec656cca60bc743a32ce6222e9fbdc1896bb2afad3eb868, 6f0bc6d96340807bab7a76d132444dc3ba21d99a4c825bcd07363e8d1340cc85, 63f6bb98a3e3256f528734f1deda5524d97ef3540fb2a06624c92716ba1456fd, 519a389d0d183fa5cae0390ce8cc2716247b8f50332de8e4fc8bee5026c8ba70, 51267fbd6aa2d09fd1ecd4c9f52557aa85f3f5af0c60223aea55acb562df9aa8, 4304a7028616787990476ceb92ce98842c8e049278ad9e4afa24a1fcf1dad782, 20217810aed81399374fec1f556b1537fa35b6499133f65e08eeda324a72680f, 31e9ea58c807633dbcc680303f1f741e2a6e58747e040e98db133e076c6cbbed, 11e0596f453ccf8f30ba8177e7df50517e364326585d1cefb4c59de277b0f6aa, ef83368caf9c9d53b4cb74b76a96e7092097e35da214ba946a146580443d0792, b6180699e895945d6178a61fd8228576629ed0fa03de54d78e7ee16f271f1522, 2be90feea3580358a7ab90d744b7c3028c8e7694863672a8a30f021b284cc94a, 0368bf651d5ce7e58305dd300a428d12e6a64d456a4805e845cb1985196bb5fc, ccf58b300ec2a7d491cbd492373ccf5175056f55d4843889ad15c3f0b2db815f, cc8e4c0c2e126938b827acfcec306dc9811d4aaf00934d397e3841fd6352f4d1, 7bf9be59db4c55f5b372576b7baaa25cff2716d2f7e24db1b98724a0e0927ecb, 28a4eff21c27f9e3b0e7b5383abb407e0a3d69bfc1d094ddd4f0b5c18425c523, e1070a6b5a406ce70cf1d1655169a4ec36fb69114c3064f00d28cc01cedfb0e8,

TYPE	VALUE
SHA256	af9c847cc0a204e969a0fab93ae676b06222892afc5271186604e348852bad37, 80af77dc9c38a3bbfb68fa66635bb3f202d72dc093305d1218bb85811ce018c9, 52634530f53dfce289317b2c4057811136fbbe873211d01e150ac32a94dd0f4a, 68a0f5040dcf9b7881d1557cad827275271027906f830f6ee90e5521a00b72e4, 3b86b107b36aa1224df2e46419f2652682c67f99222011fd63f7ab3ed43ab1d5, b2bcbc0fb471660632b6589fa96656f935f72ad5308e9b659b2e59acaf820e02, 7aa0d53bc4a08e7b61aa283c39beccf7364afc2174ffc958b3c5fd2d56dd9554, ee481ae34be52da5d9f2e8dbfab3bdd228a7fdfa9fff308e98b7691d3eb9d0fa, 28dc3771dc4aa5d8a19ba732479f3719c276e62cffd0fe8ade6159a1fd3ba880, 35bff2270daa66d092afaf7e6cfa3210790e1d17dd77e0af94b361dbf632b571, c9aa237a2a30b901d52d0074731b5ac57f70322f1fde81f6794588c17d6bb268, 612fbfebfdcc12d6eaa20f22835a1a360a747c043ae1058070d4a71ef20a59da, 0877653f6a24639bb02b547c94f670597c3c0cd96df910a2ac891eaeaa9cc5f3, 159057ba35f3454424a4901866de6de286bd11715e975d4d124d33b2e83055c7, 28bdd3e3c182a8e9a5082a4677df2f2116c8973d4ecdae023cf9fd3489b9f012, 7c684a112461478a8ed1f3885628d0235bc20081c11c55ff96cc98454e096944, 2acd42ad45f8dbb3866b537e6135672daa48921eb00668b657243b666991c4ad, 625e590fd62a1c8b4c85bc9f551188de0627c5d43b234408ce57139f4ea0b7c0, 160165d2e7f332b29b5980c27c044de2804552469ec70458df6e77dfd254765e, b6b68cdac6cdb3956dc8b7c11454e4f493fbd9157f902ffd2539545d6f7315c7, 62f035a79382bf50e9959fcb272c19d5aac64a7409deebf7c8e9b597f3954db4, b2528cb39295490b53428a98fefafde2d5f32c957b268f528b66756ad8ab6896, e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,

TYPE	VALUE
SHA256	431435e3a7a8e38458cd2a2c1e97c6b3aec993e9dfc3de5cc665ac57c21bf528, a79e4199ba0dac6948dea075c26cec05de18d3217a25000a3c7a0fcb45ba1b02, 1bb63cb3d89389f426f4cb5350e38fbd0c49ce1851f6311c5e5d246200f29de8, 96aa71f70d16e2784488fad332ac65287f33d059cde4cd2858b0dab85340ba0d, c1d0981485f8afea96d8c0ce85cb9888c96418387b8c43103b113ba283f8c59d, c7d9a5ffa94eecfbf5c22781750e404c6e50ba12459e3071670783598839cfdf, cf3f8d4d3ee1a8eff414a221767ede4c73424bb62d6a090ad3f65ea55ff22fa4, d4b46254b03f3800038cc93f226bc7b5897c34fcac0d16210f45731b57d4f86a, dd0396754df3aca8a482242eebfa92db7433781ebdd679507e329e34d4065c98, 04dbc65a0ec0a3d95aeec8161816352a22ce74c19fcd002f631879e990c2d468, fc6a52fa9d578565e4b6c47be3a4f0358a01ace3ed601c0eb88e46dd88203ebf, 6cd9bdc704701ab3618be8546e471f335431929a96d10bc59f66872b144770ce, 9ba76c05333a17c734b4b6174e68222f689f298ef48fe5dd03d25da7e01904f5, f6e19e1c17291b9b4b2436d561d8373cf8a18841b5c4393205845bcc6ba31616, 9b7cfe2a7f46aad42c8aeb5fcb668f2286b24fcd0241ad7c1b1b3d00856c2b18, 903391cc79136eb1efdca469686b96fd04faf257d87796dde594c500ab226150, 7f970ee9b2fef5c77db4cdb7fe536377e165e056aa056299624a224ef8e0cba9, c4df50417827b20cafc1e724948d576cd1b90636e5d68d577856824cb9ceb328, 8713dd146895b8262e5096e49399dbdf4dc796d37a532912c0ebbb46de059eaf, efc09d4380483145573ac4f1a2b4fe308e9bd4378bffbc44efd00739d2e055a7, f3d48bb2dc545f0864d8b85d93aea9c2b9a55f0fc9c7435f1dee000802a261da, 53b9c02ee582bf97385beb39ee140c49f73c557ccecf3bf44c795899083a3519, 5906fe2b69a5874697b84882df732f77dd3160221d0746f9688e9aa9b8e0af31,

TYPE	VALUE
SHA256	f41051697b220757f3612ecd00749b952ce7bcaadd9dc782d79ef0338e45c3b6, c7bdcebe60356900dc4b4f8bc8b75acc1536df33ae7a1049bfa27192b8c62d0a, 48b7aae41c1f229dadd80e7635a142175cba75d03d54f08952269720c5f2735b, e0c27d9a377e5f18ae850d1d0ef1d69934934cabdb95172e21fe0e36807243c8, bde4436aac1e27fe22b134cadc1e19dd954d350a5619c3593efac659ab1bbefd, 0abecc48522a2aa66c798e817f0412dc71df2875b8908255208642fe019ab9d3, 1bad202e452b1d1f8b365e946c446f889b2479a6198a17a3dea1d6a4e5d12052, 8004df38975733770a7e2a0c71d284bc3439eb7ee74077f950ad7c0baf2512aa
URLs	hxxps[:]//cooinbase[.]net, hxxps[:]//eloquent-chebakia-e2667a.netlify[.]app, hxxps[:]//dashing-cassata-b94dd5.netlify[.]app, hxxp[:]//45.88.186[.]152[:]55553, hxxps[:]//klck[.]ai, hxxps[:]//kick[.]am, hxxp[:]//klck[.]pw, hxxps[:]//twitch.co[.]com, hxxps[:]//twltch[.]lol, hxxp[:]//twitch[.]cx, hxxps[:]//twitch[.]team, hxxps[:]//twltch[.]uno, hxxps[:]//rumble[.]tube, hxxps[:]//pnwthrive[.]com, hxxp[:]//cooinbase[.]net, hxxp[:]//tiktoklive[.]studio, hxxp[:]//secure-login-bing[.]com, hxxp[:]//char0nbaby[.]online, hxxp[:]//hyqyj[.]xyz, hxxp[:]//smallmonster[.]net

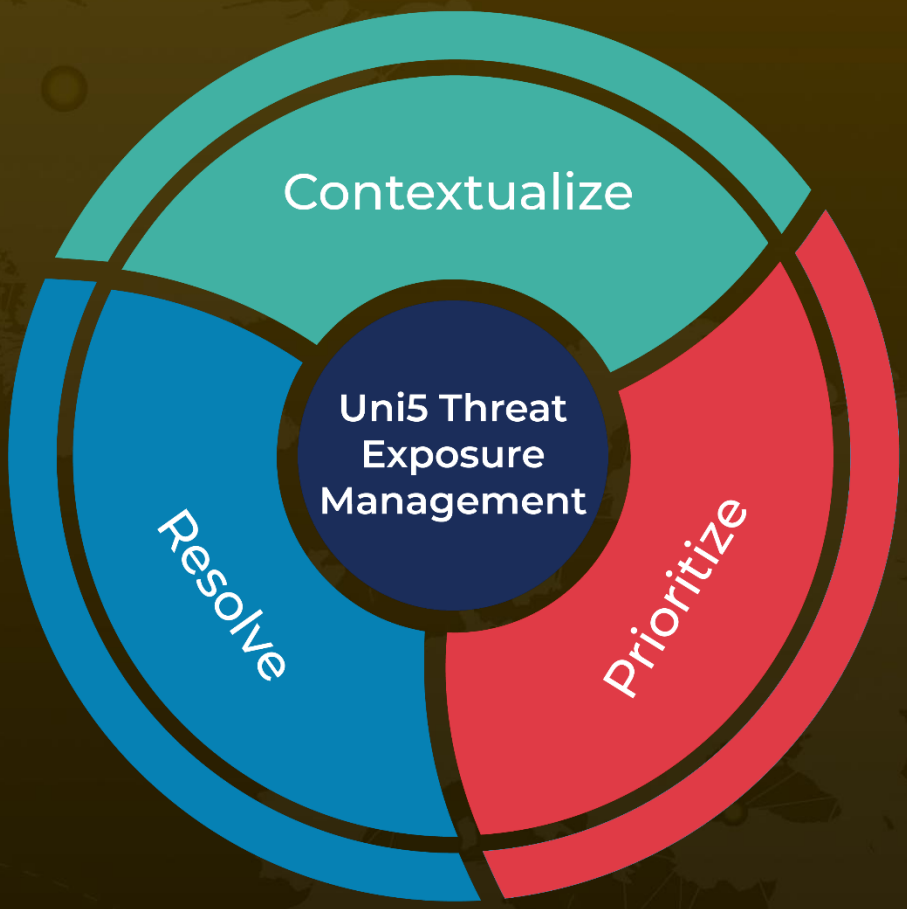
References

https://www.securonix.com/blog/analyzing-obscurebat-threat-actors-lure-victims-into-executing-malicious-batch-scripts-to-deploy-stealthy-rootkits/

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

March 18, 2025 • 3:30 AM

More at www.hivepro.com