Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

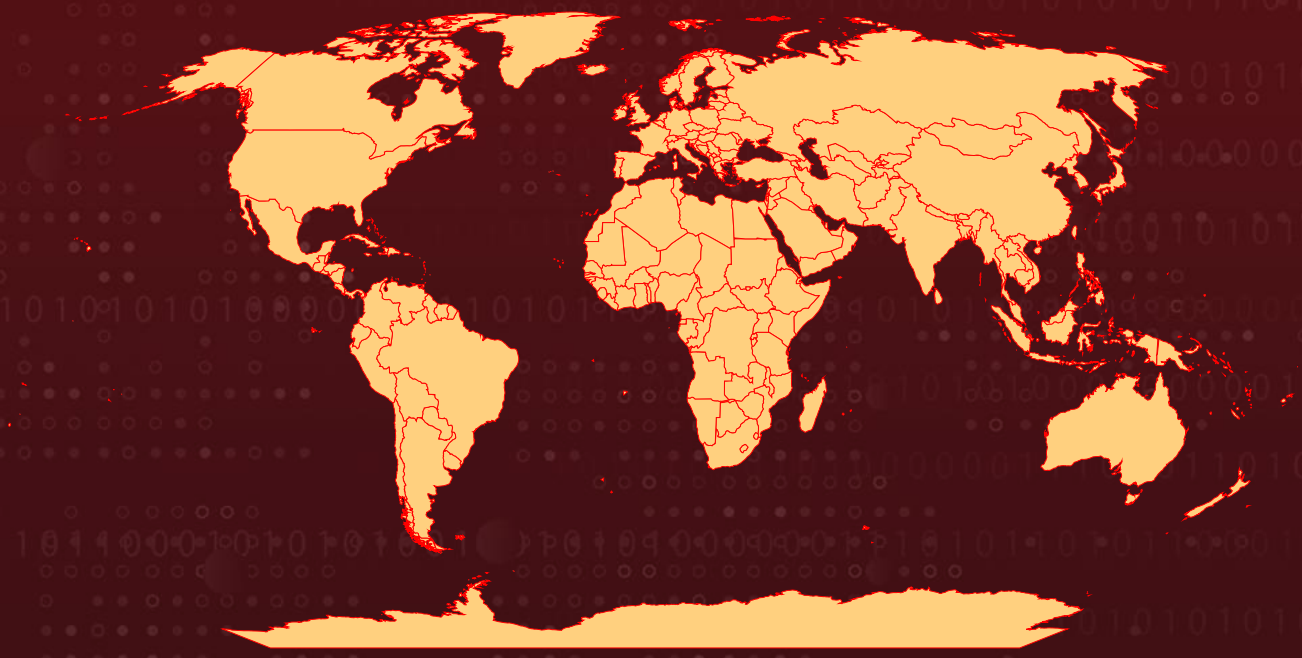
PS1Bot: The Modular Malware Lurking Behind Malvertising

Date of Publication	Admiralty Code	TA Number
August 18, 2025	A1	TA2025252

Summary

Attack Discovered: 2025
Targeted Countries: Worldwide
Malware: PS1Bot
Attack: PS1Bot is an ongoing malware campaign in 2025 that uses a multi-stage framework built in PowerShell and C#. Designed for stealth, it relies on in-memory execution to avoid leaving traces on disk while delivering follow-on payloads. Its modular architecture gives attackers a wide range of capabilities, from stealing information and logging keystrokes to conducting reconnaissance and maintaining persistence on infected systems. One of its most concerning features is an advanced stealer module, which uses embedded wordlists to identify files containing passwords and cryptocurrency wallet seed phrases, enabling attackers to exfiltrate highly sensitive data. With new variants appearing frequently, PS1Bot has proven to be a fast-evolving and highly active threat.

Attack Regions



Attack Details

#1

A new malware campaign active in 2025 has been exploiting malvertising schemes to lure victims into downloading a stealthy multi-stage framework written in PowerShell and C#. This evolving framework, dubbed PS1Bot, is designed to minimize detection by keeping most of its payloads in memory rather than writing them to disk. The campaign has been extremely active, with fresh samples appearing regularly, and it shows notable overlaps in both infrastructure and code with previously reported operations such as Skitnet.

#2

The infection chain begins with victims receiving a compressed archive disguised with filenames consistent with SEO poisoning or malvertising campaigns. Inside, a single file named FULL DOCUMENT.js acts as the downloader, retrieving additional payloads from attacker-controlled servers. The JavaScript file embeds VBScript components and heavy obfuscation, which continue to evolve throughout 2025. Once executed, the script pulls down a JScript scriptlet that sets up the environment, writes a PowerShell script, and then constructs a C2 URL using the machine's drive serial number. From there, the malware enters a looping process regularly polling the attacker's server, sleeping between requests, and executing any received PowerShell code directly in memory.

#3

PS1Bot's modules cover a wide range of functions: detecting antivirus tools, stealing credentials and cryptocurrency wallets, capturing keystrokes, exfiltrating browser data, taking screenshots, and ensuring persistence across reboots. Each module logs activity, reporting back installation progress and runtime details to the operators. By dynamically loading and executing new PowerShell or C# assemblies, the malware can rapidly adapt deploying new features or updating its functionality at will. For example, one module captures screenshots by compiling a C# DLL on the fly, encoding the image, and sending it back to the C2 server before deleting traces locally. Another module, the "Grabber," systematically hunts for browser data, cryptocurrency wallets, MFA application data, and files containing potential wallet seed phrases.

#4

PS1Bot also gathers intelligence on the infected environment. Through modules like WMIComputerCSHARP. Persistence is maintained by dropping malicious shortcut files and PowerShell scripts into the Startup folder, ensuring that even after reboots the malware continues beaconing to its C2 infrastructure. Communication with the attacker relies heavily on dynamic URL construction, HTTP GET requests for logging and status updates, and HTTP POST requests for bulk data exfiltration. This architecture mirrors elements seen in related malware families such as AHK Bot, reinforcing suspicions that PS1Bot may share developers or at least code lineage with earlier threats.

Recommendations

Be cautious with downloads: Avoid opening unexpected files from ads, emails, or unfamiliar websites. Malvertising often disguises malicious downloads as legitimate documents or software.

Monitor PowerShell activity: Since PS1Bot relies heavily on PowerShell, organizations should enable PowerShell logging and monitor unusual script executions, especially those running from temporary folders or memory.

Protect sensitive data: Store passwords and cryptocurrency wallet keys in secure password managers or hardware wallets, not in plain text files or browser storage, where malware can easily steal them.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1113 Screen Capture	T1132 Data Encoding
T1132.001 Standard Encoding	T1056 Input Capture	T1056.001 Keylogging	T1082 System Information Discovery
T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1087 Account Discovery	T1083 File and Directory Discovery

T1552 Unsecured Credentials	**T1552.001** Credentials In Files	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1059.007 JavaScript	**T1059.005** Visual Basic	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder
T1027 Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1041** Exfiltration Over C2 Channel	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1518** Software Discovery	**T1047** Windows Management Instrumentation	**T1574** Hijack Execution Flow
T1574.001 DLL	**T1115** Clipboard Data	**T1608** Stage Capabilities	**T1608.006** SEO Poisoning
T1005 Data from Local System			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9304ff7136c030896973b0192c3ff02d47daaae9aa04db80a980df5c8eaffd91, 5c983b71d035b05aba30778804bd6a2db6a9e00b1e186083813cf6ae513f89f6, 943964e8eec89f1b8cb16c0cb813e0253529f47b60b2ecdef5afb4b0abd0d511, 7377c7e3daa3c0d3cfd941c6cb0e27271dd2acbc0737c472b609861b0bf44a5f, 14371c2993a31cdf39a8747a589e1eff365b7711a1d9fdfbc8b5273f397aa29e, 190f954bcca561f829b56b6e3dfce7a0d9206eab6628ee55a04d0c2c4a45c83a, b9caa844b3d72842f37a57dffc25df3fe1f6083f93295c2fbed0b0281c2652c3, a8020170bc2d83cc7cdf86e1b729a8874d287d1c5ba4d9515bf45b04a1558b7a, 368b1fb562d913222a06b6c4ec5c9aa060b1c223a8acbfd747167c75856b16b0,

TYPE	VALUE
SHA256	780ea1c97bbfe745628415aa0049c9febfcf56857a3482e910289ff229e6b7f5, c35ec5aea53b2591e7ee8cf89da86c7a44ca1f333b206c8f33b078c8ddbe4fa9, b9866a44469d7855d114ddfc1b9bdad347ddec6dfcd5c4878367580e40be87df, 107afca60912befade2b9867167135da0a8658e6eb515330b064a9db73a562ac, 1c0f9d45e5fd0858eed93c36d9fb2ed8fd30a3fc9f0a58c1fa5c38bc32a9cf07, 21a56e1b10037c794a7eac52d71b063b76b0ff2e92af507d2f8d9f87402b721c, 2616e7157017331e10f932ae45bccdde091c724aca5496b069b17fd42f952a4b, 42fe9d401dd68ddfde23e89a7a4c08125dc0aa121cdfe930589798a92b4262cf, 5980798820124788c99dbbfa6da0e3a1b8bd5e8f18804a2a0bee6d0bc119c685, 705b51c3ccd0bd375a65fa1e80acfef80709b50b2a7d54b487309f49e9a92f11, 76e60c2bad2d4ff20845dc9b4fc969fda6be34531ead2e53568b917fc815ae36, 7b89423831873906aa3f28507d1adbcca92b37dbb8a9be4f2d753ebc31467f33, 7c5f964dda057e8f5bc7f81204bfb3f607191e7250cc60eb0c0fd69ee83f62c2, 84147b1bd16218d165b5fc6b72040a69f10fdc9c654ca056e997cec18638b4ff, 87d493b325177b038f068819b9efbdaf7596e252cc0cdc421b831226e9e20500, 89b0f2496b6200d93e1734bf586bcf67473e0437a3301403e6708f58ade9cbe6, abfb7c3c3ea828bf85874c596cac17770668abb28734cbeec67dc8c958afd340, b3c7b3bf625fdce478c0e5def4ab43f8d9e427dfacac7d37f143b3aae0050118, bccd81dc5e2c8eafbf8062561b40f77d63c9f498bd20723d9cd68e1526171b79, c09dffd32f233b9d65fe73432cfa29c1de9ea56cfd2f42b985f5e0cccfc0aa4f, c2a0e65177b941424183f97329fa78bd28696aa928e3a26b7a58088e44e3e4f6, e3c943ad9ff6a43c88b7d977f207b85c8c2cfd0c69d582e748cf58419d5bc188, f74fac3e5f7ebb092668dc16a9542799ccacc55412cfc6750d0f100b44eef898,

TYPE	VALUE
SHA256	f9a2c3d1b3244b0f38601e26f36d46b8d93b7b3df5e6fd1703e7c5afed8375b9, ef9456ada1d93e7cfc1750be1afd68807d532b6e893edd5ad79f016affd29dd0, 048b2bafb871b586e895a0749ca74a6ebf47d1901b35730097c7a981d868772e, 1e437075ff88f4ab33447a14683a9304dcb0bdb6cc52f2cff065f404a949e3fb, 1fe0138168469fb6d3f0f07f848499057d8990879d7ae2cddcd9345faa335dc7, 34804cb36531f1871c0a51e5163bfd639b97c7fe4d1604295c326e08e1afadd9, 36c3affc545476d2c5db29fcf9129849706ae41bd54894b7eb5dfe8c6b670b4b, 41c8b2709640428746aca1e842d99db237a91f9cf948396303c8b73e90b785a0, 45ba535ccd969263b74ddc571efe3ae023fba2b9567ac272967f92e799c7f83c, 48eb1c7586732005ab6da8644e550c7aa75fa382d1cc27e82ed43ca953604078, 49f323dbe82ec8452b8e205bc7aa0925bc9f48f2b4ebf66e3c54a9e3b08d5be5, 4dbd1bf6a07b97cb14cd4e2d78d09bc3561f225b64f99dc40774959e6bd9de21, 58b4d06da885b9e373516b560d4e8ea87a7281f19bebf547100950e41511d67e, 5afbfd477f803d1b0de651c1a16ffb7c698ba4033258276b8e19bfa749b3ffb5, 70da9f738fcc760986e0ed4f76f84800d3a038f672c64683a1d5323043da76e9, 7270dfd6bd579283f4f2cb5654de644491d29812109ae51a71886241cb824395, 90a81e6dd69c7f01bbd6bf74e259a1374bfe362bd23445532cf8d044b9739f8b, 9b3a0f109f96dbc74f65cf464cdc92760c1aaec1cda55d5bf39e6359bebbfedf, 9cc1657fa9f056a7b34009c71d376f9af41e3b2505e0e3ecca536c806c5eeda4, a2cca39a4bcd12b6213334d7bc7cfced07636d24a760b7a8e39f05b85bf86caf, af339fc0bc2ac4f7618021c9560586164d55c8aa5fa1d1ac740e30739c0ff425, b432adc819e6b5b65004956929dc843cf4cee3ff6dc54687d50268d36ba6a81f, b82710fc1422c5d94c68999e4fa9f90bf49ec7927636eb12be5933ef0690f354, b9f5dc18641151bf70bab31f2acd3409bc149ca8ff9fcb4edd8e20c0311157bd,

TYPE	VALUE
SHA256	ba3aed3af58569b8bf6bafbd360aa73bc777e81ee2783b7b0dcb956ea6b82df0, c025ff463278744795798abc7ed404f38cf167a447cbd4c0fde7f9a4b2dd0ccc, c52f4f652442ff142c00989e919f43387fb4779964fadc458ec80886727e55be, cab6a14f345a6a8404160825d91240ba24c6dccaca6b90da096f05406fcb4935, cd875cd6c18697b401e0ed103e1d9a5f2d047ec22fa2b772fe3c4dfec6952151, ecb7133e5c2338a74f1f9e836edcb9218a82dcfc83c85cec8f49903246783e48, f010ec8d2ab7b702870ee029aec16c0fdfe64a40f872f36dcb94ae7bc62a4638, f1414ace7527119aa69ea6c18de4d3ae073a306c9c3d63cd1d279059a5077bc4, f5d72181c6b7b8054244a40e6ade96fbb2d6968a132fddee082846b8ca4dc102, f966b7fa2ad4efc87cebb2fe2ac1fcbb21ef22b945dbd44aea9706791537b671, fab53f1bceaeedb7f84a031346a0ef840328cd28aeb984e34f2434a9d3475237, fdb7373fdcdb59b744e5b4e8369a2ba1c210449aa63dccde3f3546c790701804, ff2933aa3eb4b43ad93e798feec1d3699ce7b75497ed893942e742b3d2514b67, 33621b2d12a898e4a78b7e5e1dc59506a9fe3b0fb4fe2ff33c32795ea5b312a6, 01a94f7403e9e8cbe1cab08c4a1730e79e129d4c24193100292f69ed0d1979a9, a3730e2dbcaf2bd3dea2c57c945175480577fe00ed5ece7a16f53fc2b2a36869, 04b6a4c58ff8db639125a8277e7a3e8fb00100dd88f299896e24ac0fca928460, 9a5685effadb8c63cea8b14115402ad3cfe721984b68726f8afd4f4b38e00a8b, d2a9a3fdf016e9f0f32671d2dfdfe5fa6f66541822d6c0278ccf8ce9eba94db8, 291700be999ed8d361e9418a3375353c384999afc42271affa7ecc395f137fc0, ec513db1dcd045444fb7282f382786d91ed3357d254797afacec8b7bab1f5070, b5a97bc726b26c05d76eb6c51505d1e3fe18eeb7177e2be25854e6d84bda7a02, 6669f4a455f5c71667f5f8b0e0d627f1398e15112e08277205a883487c189603, 5c569c68ec4085607b7c23854105a9255dd4290c8ed43f1d95141f77db4e4781,

TYPE	VALUE
SHA256	8e7241ba98618ccb4ca015f3673704a8df9cd8de5aa2e8a287e565479755567b, c75d16ef197ddc7241abc712ccb7981ca7817f5761f9f8f986fd8b9fb7036256, e899206a07b322cb69f659a112fd508911bd92be40cfcef4773fcf8b43ce93f9, b5e59c233b825cceaf03b8e902ebdc4d608a3c3d0ee35a092ef8c17fcb48e6f7, cd58d6d9065c112293f15ae8bbd2002e88f258e8bee38297903d1ca9025d05a6, d0141a341f816d3493919524be6e025ccbb04f114a7789d982d35b40b0f7ba63, 244e511e0699fe0b6722244dbe66026597bdf5b4369c9c66f846a3f49b438341, 8a1b2bee78a30f2f119a37a0e024b47fb21572f6f7e02444302889fc1bd75686, ee726c64a82244cb65a6a0a768e5fe7032cb5d0897296418ce91f3b561726586, a8cd019b2e762ac277a282eac9dc4507ab1fd81d47b37d0d404469a95f0be4a3, c1c5e24991986565840385439 7a6b62593ee6ab99f4a20ea8ae1e03f1fac5e71, 411f6444889d5bdba73cf7735f29a8fa971f80cb9d0464c8475d304bf22e94d5, 7abafcb21b1f7fd4c07b54c3ca99912caaacfc0e8e7330631d62247faede6ada, 0e415f71530b9d65e9804d8bc3fb12f53d26e6c27919db32c8a2924e437ecaa7, 253ed51910d7835eafb1a21814f45520809ee6420c0a882b1c2d64487542652a, 5bba8e7b6f31b3bdd2db9562b327e5e464867aeb436c268957ecee9690db181d, 6bf52b79adbd2b79118700810b8437e2ec2e5e19d599e4e068c8f6f0d76ffc1a, c64a9e869ad8b210338e462db7bbb9de8c1288a9de3cecc9437666d75821429c, ca4e3ab9ea7b85ba81e0141fee19c67d91832155a11c0b378e58749010ff243b, f41538620ce33c25984032ddcfa339bd1e0dd6b4e7c97688dd7bebb310837716, 05d79a474dfe20fbb433806e215d78b31cf8574cd955588fb15cadbf720bf3c7, 07b8120b557816182ea185e9d20b61445601c20c874761c41c4ab9a12d596886, 453b93029be22447b4bf2925991f72a1b063c753c85e230e44ee1ab382b338ea,

TYPE	VALUE
SHA256	90588fa7721cc3a381ec2353299beeb9918766ee38cfbf95bac45e15ef84d81c, dab22465284356186a3de1ea470f2721e0ac18a84a072ae7dd83f06ca3efb25b, ee2385867241917960d21cc66b9c58aab8a62d2b203f725458771b3ee7794c80, 1b3e8dc1f493b8e9bd8cbe1aa948acef8e6aac41f480bff76075327dbe66652b, 3f97a1c386e14a44e7eb259858adec0bb1546fe59d3199595cb6c3d4d1988470, de5022893af502a25ae5f37cfa80783df798d578bb5d69facfd631055cd0f2b5, 809f4ffef71ab43d692d4fececf1dfefffb0854ae1f15486960b1c198c47c69f, 64c6bfb31a340464a99acb4c51680070e470ca649ff29f5db26954bf13963b26, 330a579ba3bb727a8c98079d127d6341c2ae8321f164c0b2050ed7d1dee4b588, b6fb6849c14dddef78c58c62878d3c67f85f81c663a3614992eda616cf36f25c, 1e63e374ec0b11f361a1b051e4d123e3a2a10404ba81cfff912cbd4c96187297, 94a7a0ad7ba79bccbdbfd542269b20fae67df35e05537106e91aed6f2553d088, e95d9c7b29714bb4c880c3417707b2f3da9ad52f65bcf288baa27dd2c8a54c9a
IPv4	109[.]120[.]179[.]170, 131[.]174[.]164[.]238, 147[.]45[.]45[.]168, 181[.]174[.]164[.]117, 181[.]174[.]164[.]12, 181[.]174[.]164[.]170, 181[.]174[.]164[.]180, 181[.]174[.]164[.]2, 181[.]174[.]164[.]201, 181[.]174[.]164[.]238, 181[.]174[.]164[.]47, 213[.]176[.]113[.]168, 5[.]252[.]153[.]94, 77[.]110[.]116[.]227, 181[.]174[.]164[.]161, 62[.]60[.]178[.]24

TYPE	VALUE
URLs	hxxp[:]//213[.]176[.]113[.]168/pgq, hxxp[:]//181[.]174[.]164[.]201/mhx, hxxp[:]//181[.]174[.]164[.]12/kyc, hxxp[:]//62[.]60[.]178[.]24/vag, hxxp[:]//181[.]174[.]164[.]170/zso, hxxp[:]//77[.]110[.]116[.]227/kax, hxxp[:]//147[.]45[.]45[.]168/san, hxxp[:]//181[.]174[.]164[.]2/sdvpqcm, hxxp[:]//181[.]174[.]164[.]238/hgv

References

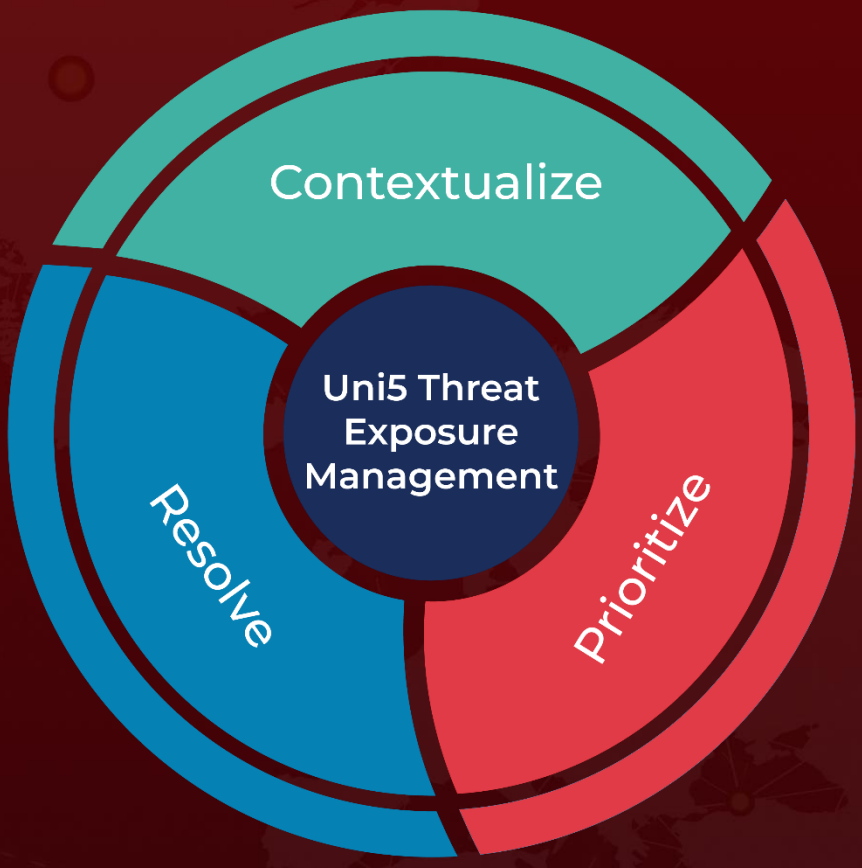
https://blog.talosintelligence.com/ps1bot-malvertising-campaign/

https://hivepro.com/threat-advisory/ta866-new-financially-motivated-threat-actor-targeting-us-and-germany-organizations/

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

August 18, 2025 • 6:30 AM

More at www.hivepro.com