Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

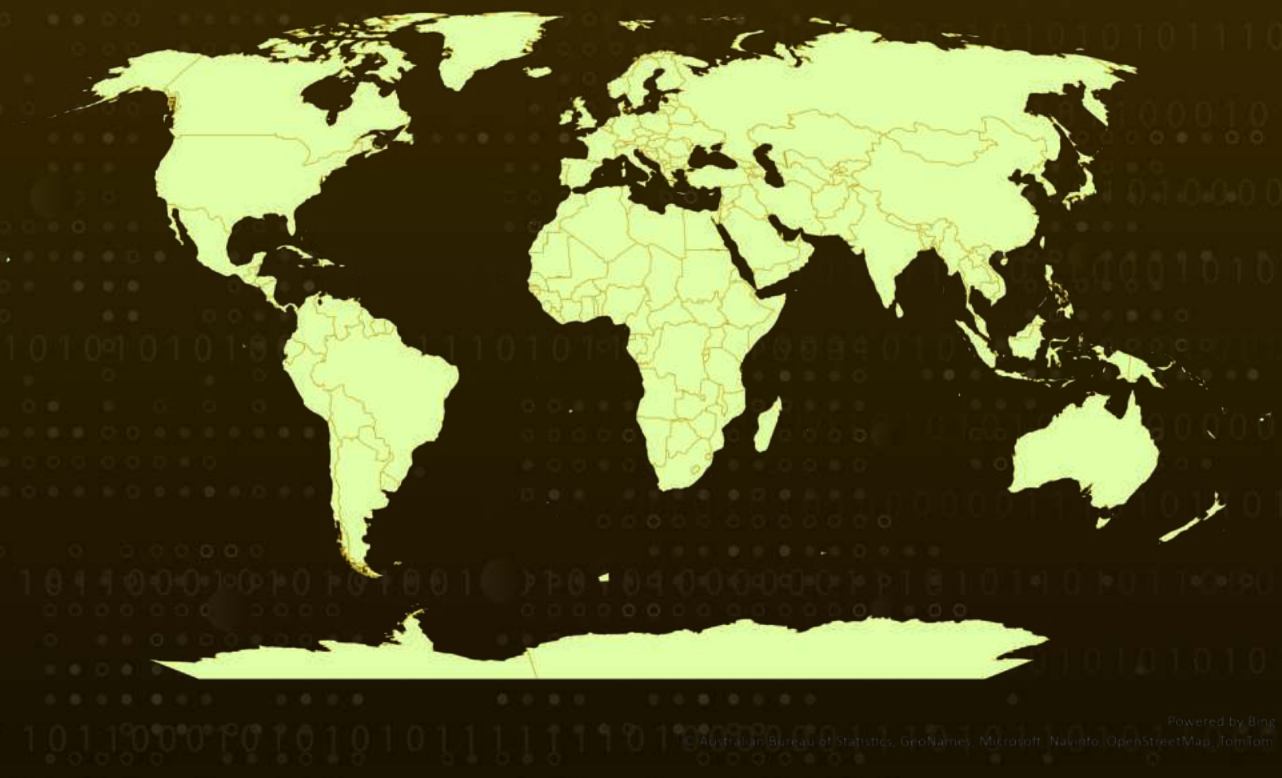
New Rilide Stealer Version Evades Chrome Manifest V3 Protections

Date of Publication	Admiralty Code	TA Number
August 4, 2023	A1	TA2023321

Summary

First appeared: April 5, 2023
Targeted Region: Worldwide
Affected Browsers: Google Chrome, Microsoft Edge, Brave, and Opera
Targeted Industries: Banking, Government, Cryptocurrency, Technology
Malware: Rilide Stealer
Attack: A new version of the Rilide Stealer malware, evading Chrome's security measures to target Chromium-based browsers in campaigns that exploit user trust through fake plugins and games, posing a significant threat to user data and Privacy.

Attack Regions



Attack Details

#1

A new version of the Rilide Stealer extension, designed to target popular Chromium-based browsers like Google Chrome, Microsoft Edge, Brave, and Opera. This updated malware employs new tactics to evade Google's Chrome Extension Manifest V3 protections, which aims to prevent the installation of malicious extensions on these browsers. The malware displays enhanced sophistication with modular design, code obfuscation, and new features like exfiltrating data to Telegram and interval-based screenshot captures.

#2

Multiple distinct campaigns utilizing the new Rilide variant have been identified. The first campaign focuses on corporate users, utilizing a PowerPoint phishing scheme and a counterfeit Palo Alto GlobalProtect plugin. The second campaign leverages Twitter to promote fake Play To Earn (P2E) games, which then distribute both Rilide and Redline Stealer malware.

#3

The most recent campaign concentrates on stealing banking information from users in Australia and the UK, employing unique techniques for loading extensions and featuring crypto token phishing sites employing AngelDrainer scripts.

#4

This evolved version of Rilide has successfully adapted to the constraints of Chrome Extension Manifest V3, employing techniques such as inline events and Declarative Net Requests rules to execute remote code. The malware's code is also obfuscated, with a modular structure designed to evade detection.

#5

While the source code of Rilide has been leaked on underground forums, leading to potential developments by other malicious actors, the malware remains a potent example of the ongoing arms race between cybercriminals and cybersecurity measures.

Recommendations

Use a reputable browser extension manager: Download browser extensions only from reputable sources like Chrome Web Store or Firefox Add-ons and avoid downloading extensions from untrusted sources or third-party website.

Extension Control: Enforce strict extension whitelisting and periodically review to limit unauthorized installations of potential malware like Rilide.

Software Updates: Keep browsers and applications up to date with the latest patches to mitigate known vulnerabilities exploited by malware.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0003** Persistence	**TA0010** Exfiltration	**TA0042** Resource Development
TA0009 Collection	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0002** Execution
T1566 Phishing	**T1036** Masquerading	**T1176** Browser Extensions	**T1539** Steal Web Session Cookie
T1217 Browser Information Discovery	**T1113** Screen Capture	**T1547** Boot or Logon Autostart Execution	**T1059** Command and Scripting Interpreter
T1041 Exfiltration Over C2 Channel	**T1055** Process Injection	**T1090** Proxy	**T1027** Obfuscated Files or Information
T1059.001 PowerShell	**T1583.001** Domains	**T1583** Acquire Infrastructure	**T1608.006** SEO Poisoning
T1608 Stage Capabilities	**T1115** Clipboard Data		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	0f8c7037ba4cf9736a5ac22cde94b7ed, 0fb39568d9ba07e39f64d64510832a99, 172f5c41250ef3e84579645e5b1a22bc, 1c683f7e8ede935de16fe1af8d920b4e, 1de4b5ff5035d3df6ab27d12c83b18f5, 20d8abba528c323668911a7da1993336, 23fc39223b0225998a70a3cb2e05ad4b, 367300209532298c12b8678a1699b6ff, 403dd2a2a6163c07710fabc08f71bec8, 44cf3fe19f92cfac81d74ec366302104, 47c7a9d2010c0f1d1c20fec47339451b, 4a0e5fee91b361a09cd9d70e5f6ffb3d, 4aa44852969f4c603bf9e8e3799d6984, 59998a5c7c0f31adc47f3d05333ff8cc, 59e77f77b458eb0c390f90e2daa35504, 5a439a865ba82b35ef8eeacc1a778e0c, 5e8d7b2ea9c184a5a88edd0e507571ed, 614ce2b5df0dd74d1bc5b0bde55edd53, 63e9249d7950ca2e03c40a64a76a3951, 66e05bc7b8e8ccd31415e22272f03bd4, 678a0f6c5a0662b8f42fca2f6788e3c6, 79f586fe64498205b1aab8ece4b2e944, 7a60adb662556863752bd2ab1c25c727, 7ba207ff437a0df9b5a05a01c0d548b9, 7ca9216d43d51507d326a72c4d27056e, 8080ad6ea6102d445ea16169a990cb5e, 89d7bf4d70efaeb4e63eddd179df9829, 8b008a8f776b57060b5ce42b6ea2b8f6, 97a42807acd13205c1a2937850416439, 9f806a3d233ffbbb58cf82c3e769d6a5, a404c8f69888159b85aa2b069f0d0f90, a906698ebe07eac71494052bb82cd3f2, adbc8e285c7657615b2ebee344390952, ae249d95c6ac779246b8eea93730801f, b4867df506f38736c0f6ce56decad080, bb8315ba98e0cb251453d58cf2048f3b, bc9472ab59a9625003190b2dfcd1c502, bda2f43f6a08de8e0d41aa704a796eb1, c8805c7f4224c02b173f6beab132638c, ced4052c3d3d32e21df075d68b5a4494, cfe9ec19dd3991c45c76493d9598141b, d2b07b0e4142bbcb1457d51e25da416d, D504505d18408343a5f1225a0d0f3c1b,

TYPE	VALUE
MD5	ddddeb26f795fd7658720d5ae80a310d, df7d7dc978275f8c85ab8408abc8df95, e879d0f7540ce7b3365c7f79a461ec98, f1f97bcec87f298f3f533fbcb0de034e, f5dc1259e5300b8d4711ca7bf51c6e9f, f8653cd2a1c7cea7509abd6cd52078b3, fa3509f5adb6b3c8857194083af87edd, fc3afbea35d3844550af54a2506a5f64, fd59031e1c35e5fb1ecbaff6c64a31e8
SHA1	018caa6adbd983fd2e2ba46670196a41669b4cef, 027268c51892ca07c36b66ae31dbe33c2afeb789, 060ac379851786e61d081b1471ee15347185e56c, 10d3d6bf88bead7180e84a2b7acf3abc60e14e81, 16f46139147f5f6dcd521840951860c299982587, 173065e688b008e208d6ffd62ea2b5a15cf66552, 18ccba913df5b8867c6ef066f121fb8cd03a7518, 2700d7a6c6f5abdea5972c9d5a67603216870af4, 29dd8609c74cc54d60bab53c6e83a3cb641f8b4a, 2c98abcaea10d3abd307c68cbf95f3e4af40ec04, 3197073f18ce0432691d61f09302f949d3283e0b, 3976d181a1bdeaca94c072d672ee90750865ee96, 397a40a2f5047db13bf84bd7e6296c12dc317933, 3c6fcd01f513df3480930924bd82d2abdb19266a, 5174127b62bd3a1e983dd8a33e3efa5ec54471c8, 52a1ee4060e13790501163c78d3475be90f05584, 552b715702d8b4b0f035a92d5ab5bb1f0712ac32, 69fb5b178f369beaac85f02791fd8f85facdd20b, 70cae8f5f2d6573510f5f4400a8baba89e5bcd2f, 76fc50665aea80dca8844282804339b7351c3267, 8316ab2ee030c859d2952a0a0ee3fb8606b88816, 92a030999013b6835b39d2cce951fcb258107bc8, 92d4921b1fc15ae389a59b5df90614d7926f95e9, 937e03c89c33bbd5c7727c3f8e00aecdf22afa7f, 946ac4d655bc77624b912ad42431c8a692cac6a4, a1456ea8696c755d1d2c4d1f27661f9388f805b9, a1b9fd0577f6cc0ff87010a651ff123b8285289c, a25fccb0455f8e9d3751f5127dd6867aecb58b45, a468269647f3b9909f4df27b74711d56adaf87a4, aa7929ba89295c732398c63a574a49f035b9ca52, ace802a22a69b2d6fe305d407212c0919671f81a, b0c587068505fcbdb55d263dff03f3abbeeb0842, b27a56ee3262c4d87bae60c514ea7056a4ec7c6f, b3d59d7caab786cb92639a8c8bc17f73da26c788, c84a3774eea3c7c3069964fff500eb498a3e3fa0, cba87daff1cf961fe941489cfcc80f074f8d49ed,

TYPE	VALUE
SHA1	cc7949e9587b7f64049ab5b9b3603eb831f47808, ccbf7ed9d3c2b606b753359cb4b10caa2570a571, cde2d4b70d374fca96951a13f056f778258aeb45, d033569c97f382b21ce83439dae0cab5bd28e135, d85c34f3cd20d24fde93f0e60d677d2aa8c48591, dc7fa285da2034a00ed2c66cb86c37e1a4bbd679, dd4e7e8230e14685d73d142efb337e75cb2d3581, dd6e2e93d80d9b5df93e17e714aee41534f1158a, dd7f3feb98e4d84817a84a9fdfddaed3b2719303, ddb5e3e03655fa8dd8690aeb81db00da84bd2c8b, e3476f4fb588b23bdd625bdc75a98a16d1acb4bd, e4aaef90c4284e923679e92e970396f7ef989087, ea4d7f31e889585d1a2c77e2b2823a4ccbd765d2, f2348f98a71afcc241c6e3d5777b300e5602a4e5, f5a5d008a70e1c632d7cb72b2f255f3e500b43e4, f637104610e14e2260a792fd17775a83d2551a38
SHA256	008b7d803d8925c578168a2bd757dd4a0b26b32b2f810ce91e3f062e1ed5cd0c, 0778c7e2ec2dde55d2e88f31168a52d8e78ce5348ccab82c8e6b2c0f3bb0b3eb, 0fd8a4468d7d5370d1f67b01badb2e7e1aacb3e6cf1689cab4f678cc7868f520, 14405eee6b03c4de6fba6b68768a943120c092280e0763ee2672b7ffdf9358bc, 1ac5e7036f862b8d2a951b1be262b498f0c9213d4d2f500e9c5f06ac8e8179b2, 1c1a8d502871dbf22b404b6825b5219344a3d89ebb5da88380ba1ca158e2d92b, 1f62a8dc5e71b2826d0fe70588c4c4cbebb9518d3f1125807e6e6927b359458a, 2aac1089998e5e88fbdf539408be53570a4ed64a989885d1003bf73c723eea1d, 2b638291abc822a2bb5f94b196022cae4b064487a71a8e067f8d8a2fb3c7acc5, 35451261a9864614aaeb43cd8bfb8d166a483baaa4477c6e119ebcffffa0ba31, 3978acf99393c9538dedc22f97eb247bbcfe0791acead7f6c96d1079479286fd, 3aa913da9591d998a229acec529eb58b1fea14b403b92f56dde47a8425739473, 45d03f5d809664844d569d35431a147885d201ca151bda9bf66f282daec025a6, 461773a67e1a6228d0a8d02a45da72fc94ce0df97cd99aef33dcbf859d306a11,

TYPE	VALUE
SHA1	482b3ae10d6b70c1faf55a9b3abd14bdc1b198b18d089a0aea6aa6ac6fd7ace1, 48346d8f46efca68f354f0833c3cfc9e8931d5b655ec434725fcdffb03069460, 533576b2f435591fe51d0e09d479154fac13a6440c619085dc0a11ada0f69e12, 54920cdfbc9403da38058b90bfb19a1af5caff2ca4584209d13e0f90b64c3b2c, 5f6e10bdfe78f855105843c67ff6ec69801caba328a8b1681425b06e359f888c, 687e9fc52445b8045fccc308c30713395bdfba08dac83fc85355a5c94b2bbbde, 6a83ee64b323082bf8827deb6297d4d3895f346ff83e9d9d4d125e976df5e503, 6aa388c50c8c184901db02eae71b1ec3d9e0ab9e636d22419f64a83c8b2c94b0, 6e9c56301605aeeb0efcbbfbf10008dba7a8b99963f02256d1b28fbc30df7907, 6f68fdf8c77b6deb44427322f82a6476a631ec6e4cdb0b18421bf5a0c895435e, 718b9adb3cd2f68c41234870242e312cac6beb00444ed4e21dca5f21b6fbecb9, 7465e22c5544ff885472e36dd60beec5039c68c4728d804fea240bc36e8f6794, 7dde5fe5377eaa43af2896f0aab7a6875ac88a34d0391c39d0979c3cf2861723, 7f0a71e2443cef0beaeea10a78fbbdb3a612be6c4be206acf7c13849d593fad7, 83fff7424342575d8ab6a9bd8eba71490e75a87ea825c8a84bb16945613467e1, 8caaafe787c9e3d59486ec129b4259764641999b0f1de6b5b46d3773e96442c8, a4ebe88f43d782b30fd83e1fb79b26674827cc03db4aeb77540243c303b51a6a, a7e24ead72e9bd2d74be36c201e348d5c5aa29c1c0c4e972677ce12602a74158, aa76e48528f473b171b98bfc4d4e4d839a98c255e78382dc6f020e36ed00ea5b, abae2f164e073e7aab2822b507de10e731cc1b396809728452e98be6618c149f, abe1c395c9db7df35611caf30fff0a18f23726505b2b51e4dce6547896ee6f76, ac4ae2bb49343ed24c2ae0d531cde04c3186dc4263a2352f2c2ac78812bb5c05,

TYPE	VALUE
SHA256	ad32f29f994a9d4eeceb39afeaa2a1dbda4f17931668d64026c225c738518cfd, ae5da62daf678fc0555f739c116f58fd26c5400257367dcd0f777997615a4b23, aed0c82e40f51089ef8c08df53404d61a591db8f14f07a9ef38aeeef8f4e15a8, b6043858d8b28b397ce364417a59167bb1afb32b5c8fcf0be428362af7952e27, ba1d0a41bf1bfacf41e667857cbd24b9834631613de44124b95357cd5c7637c3, c23846b1ec00890c3fda2b600b29b2fb717de6fa54b8c9bebe825aa4e0a7f2cc, cab8e0569f69efe0214dea05461cba63c3abb9c255f17e2ae48e904dfce500fd, cca6dda21c62f2665eccdec2edff5e6dfa6260a217c02709b21b3e14670ca3b7, d4ae1e54da50c3dbf7c201a42537f42fc307c5ce7700ad32aceb60f69ed7d779, d755c580cc88b6a5028e843aeda3e3a50c8f025ef1dcf66027c0c1b671024d36, dea7f22216fcd2a3355b231d57dec37164c85faf3e9279beae6cdb153051a48a, dfc0c60526e78d58f055ddace6cb91227958a0c5b413c88d00be175f084bd5da, dfff032e311776b3d62f70856a6d29ca8267beee614f756301b7f891c6325485, e39d0974b403b547b07282237f356061754375d1b70dacf731d8fa2add15d856, e669e3509aa8d6a425b61e77993b23f832071ba2f7def373af57417f661eb431, e89971bfb8375d748cc233157537856c5598fcd513ed42e862261a99843f40d0, e8a791965f8534b33736a0786ebeb0975002f3a03c31aefe2e4a64a1d4c70a34, f2931eb819db38895ccc016a6b04b90bb1456931164f2b7e15f4bc0c95fbd997, f6e81b0d239268ce0c9bb6ba7dbe09fb67ffa273a85fdfe656b14b5ea9a94568
Domains	blackfox.lol, eaougheofhuoaez.top, edd2ed2.online, ext-panel.website, extension-login.com, extensionsupdate.com, faugzeazdezgzgfm.top,

TYPE	VALUE
Domains	frz-panel.su, getvoyagebox.org, io-web.cc, lsadksajpenal.su, nightpredators.com, proyectopatentadomxapostol.com, pupkalazalupka.com, riotrevelry.com, silent-scale.com, tes123123t.com, web-lox.com

References

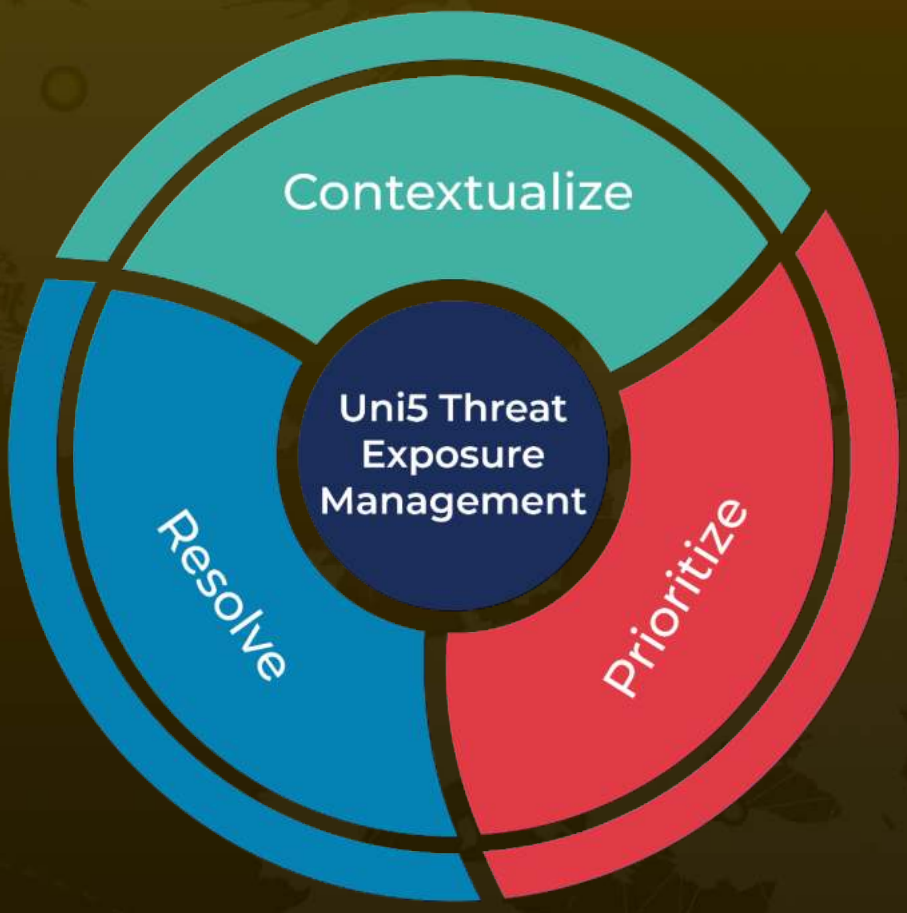
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/new-rilide-stealer-version-targets-banking-data-and-works-around-google-chrome-manifest-v3/

https://www.hivepro.com/rilide-stealer-extension-targets-chromium-based-browsers/

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 4, 2023 • 6:40 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com