Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

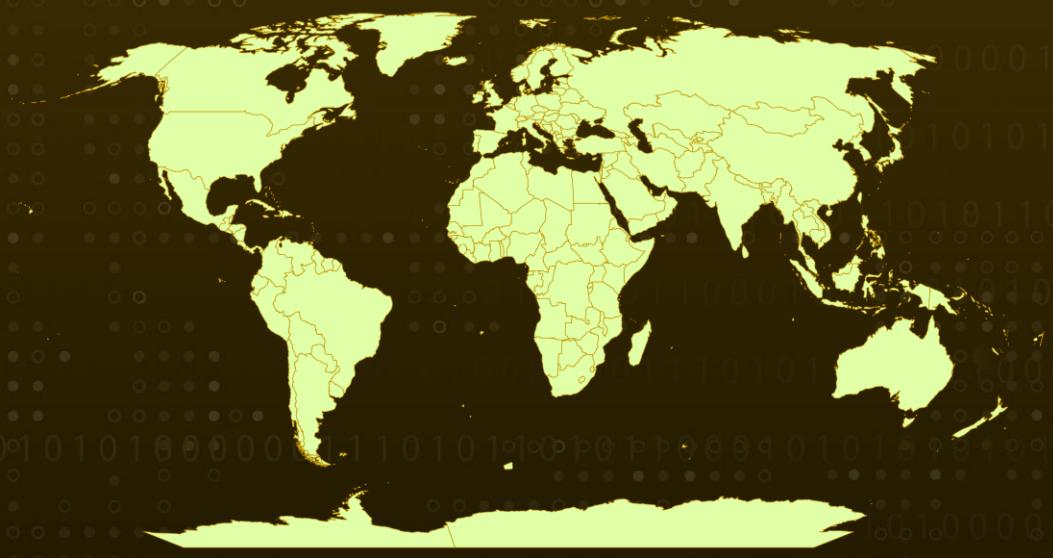
# Rilide Stealer Extension Targets Chromium-Based Browsers

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| April 14, 2023 | A1 | TA2023186 |

# Summary

**Attack Began:** February 2023
**Attack Region:** Worldwide
**Affected Browsers:** Google Chrome, Microsoft Edge, Brave, and Opera
**Malware:** Rilide Stealer
**Attack:** The Rilide Stealer Extension is a sophisticated malware that disguises itself as a benign Google Drive extension and targets Chromium-based browsers, carrying out various malicious activities such as injecting scripts and exfiltrating sensitive information.

## Attack Regions



# Attack Details

**#1** The Rilide Stealer Extension targets Chromium-based browsers using a Rust loader to install the extension. By mimicking benign Google Drive Extensions and exploiting built-in Chrome functionalities, the loader modifies LNK shortcut files to execute the malicious Rilide extension. The background script enables the extension to perform an XSS attack by removing the Content Security Policy directive for all requests, injecting designated scripts into targeted web pages and exfiltrating URLs and screenshots.

**#2** The Rilide Stealer has similarities to other stealer extensions for sale, but its source code closely resembles that used in the Aurora Stealer campaign.

# 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 websites.
- **Limit the number of extensions:** Install only the necessary extensions and remove the ones that you no longer use. This reduces the attack surface and makes it easier to keep track of any suspicious activity.
- **Monitor your browsing history:** Regularly check your browsing history and look for any unfamiliar websites or activities. If you notice anything suspicious, run a malware scan on your computer and consider uninstalling any suspicious extensions.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0001** Initial Access | **TA0003** Persistence | **TA0004** Privilege Escalation | **TA0005** Defense Evasion |
| **TA0009** Collection | **T1027** Obfuscated Files or Information | **T1036** Masquerading | **T1055** Process Injection |
| **T1113** Screen Capture | **T1114** Email Collection | **T1115** Clipboard Data | **T1134** Access Token Manipulation |
| **T1176** Browser Extensions | **T1547** Boot or Logon AutoStart Execution | **T1566** Phishing | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Domains | nvidia-graphics[.]top<br>nch-software[.]info<br>45[.]15[.]156[.]210<br>vceilinichego[.]ru<br>ashgrrwt[.]click |
| Wallet Address | bc1qkczacyp5jq29s5kaphth4asu8cv2y4u4gdgj7q<br>bc1qsjg8dqx6ga30h6szjd8dv2wg50ch50qrey4t7j<br>0xDBc1330056E2F5e2FB11FB3C96dE2c44B313eA8d<br>1KqequymujeNJuyB4gH7oJSFTB3En3Hf5n<br>LRYpzmnqBVozkbzJhTWndzYDPfjmNPyaLv<br>rUPTadzFN6LS662Z2d2AvNyqU1xwg2japJ<br>THiD8hFLiEyULVKLp3DSbBXQSbR3MQxm4X<br>D5asYfjtbTtFmFkrEwqVgbJKYv9YT7Tgjh |
| MD5 | 558104b26ccadec3d3eb2925113387a6<br>c28a180de1f80c8c98d0904e64142bef<br>1baaeedd1a26edf4fa79ded370e3d19a<br>0a4f321c903a7fbc59566918c12aca09<br>561797d7e5cf956e33735180d93be5b6<br>766d020e902b6470d0510e5c6cfcd6e8<br>d9cca3dd5bdaeb0466d52821b584602b<br>9e5f43b2dc1606e27fa0cfdfb4e363d2<br>740606987f4d588c89d0a5b68648e31e<br>1c54dd00bc7cc52b60ad4a46e2fb3a77 |

| TYPE | VALUE |
| --- | --- |
| MD5 | d54fa225b07298ec34be872cd4ebf4ae<br>baee9ba0b94ea1e2b2e566fc8a615554<br>99dc4073f2fe91f48fd16bc65e7dcbc2<br>2cc204564b68c5a98b1ff68d861b66c5<br>646b9404a29febe9f3741797b79e300c<br>253f4319673673d2bf5285558a6903df<br>50e363409ba77b20fb6f0bce4eff7b1<br>c1f40584e4ac391d97218ce137a63fb3<br>ebce63fdc8ef245f117f06ada3ba0f6d<br>4abe60d2c3506f4767e163d135f89f92<br>b85c5659e946b5d7ad78410356288928<br>ff4e2df1a46d49862ab2a0af830a007e<br>c0e120778853f0a4865e006a07cd728a |
| SHA1 | add0d61399c8c47f8ac73dc83cc83dfa31cddeca<br>415d790b54ca8e374f37fdbb00090110b823ba18<br>ec6de82efa93e59da148f4d696efcfca851e051e<br>2449e4b27d778f6a4ffc00bb7b73926ac2c54e8a<br>0ead1d32ce6b15c4a90373fce58d1554035cd40f<br>39f546a4ec94e63e603e3c2481fecab2b5e8a475<br>61acdad59223a9eb0b392ccd085db1e49700d65<br>28ae2440c56350f65b607e4e99b67a2632db873b<br>05536aa80f8280ddc31be5c0ac3ca995f2190a0a<br>f689396c73055e99a06e002c39e3a74d3d402607<br>84db08e3dcbe40c7cbc998a77788f7303d4a2905<br>0cb1d9c2a3c8b776ef1e3ec1316fbf595ced7863<br>eafdc35b233600ef552b87e684faa3ab3396eae9<br>5012e783b2ee29cb40b04a10d1a40d0bfda683d9<br>a46586bfe22f4d84cd9174238740af275bf50c69<br>ffebf78a9692293a23f9a477ea8a79f7f6ef5aa2<br>a39d252e7927ae1adf518e6a3dd08f37e7ee7c26<br>70167e7e5d71fba7d92796324b488c0fb9727712<br>25f3fb6d2dab206a5e9b2c0ef26ec6d6a56c5767<br>b4b918a5898463dad1c7d823e0b3f828bac15aad<br>abaaa2644b1e84e8b39119988dd711572377c839<br>b1c100d5a99ae34ccb3654c7b7f8573376a44fd9<br>e049f56198c23d86e9083142bfe80042e21d4b8e |
| SHA256 | 0e31ff6406b03982581246b7dd60f3b96edcf0bd007b31766954df001fd68f69<br>e623984143e0dc6e35c79869ab1521c6714e588e8e648606496f8372ca0d8416<br>ebd72806abd354f3162eec0991d127f993a5dde1a0c719b47087c9ee0edefeaf<br>0f11aeecbde1f355d26c9d406dad80cb0ae8536aea31fdddaf915d4afd434f3f |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 8342b134cddeaf34ce05bafa9e860dacf6cd01b85fd00147d90a350516c055e5<br>4cc83be0fa496855d244050616ee2e86b044a9bc87bc5ca70b305986c1ba3bb8<br>55251c725e9f6f51b8db7a631b54dd85b1b59d644c3219e03ceffb0c49cd00a4<br>1b01c3e554700e1282c7fdd2dcb54314516ee1f0c5eef3560cdbabc1ba776293<br>a28c623d120a76dcfeef9504eaeefabac9d33f292576ccf012fa458b8d7bc6ef<br>8989f4244667626728c6c0083422ff714cb622c92c35a53f9cb1e9891f4528ff<br>170a13a7a8757336babe857804fa24b6cb20aaa9593b32546d7151f23095a510<br>bb57a504e0b821552344cecb3da9ecdd0d61817264617a4917d6f5e64a1df7e5<br>d70e933e10e667ae7ef6e68a625c447be8aabe9b29affdad999c969bd8769003<br>c8939f8d6237fcc17d486981a800b1e7e9974377de21d7e76677babe8ed536af<br>2e310391d77022bcc708c354140319718777ca35efdfb76d6c80cb9de8c8091e<br>4bbb0584eed0c082b5c43d3f259f37cf1a0b64eabb485e85090951a6566d98d4<br>9dca66f52f31dca921fb238bd36bfc1b1a59d3e4af7b071da9bc4c6bf294e402<br>4df0f18a7e05518bbe93758e751f1f462fef212cdc786c7217d50ddbda14efb5<br>ef20c929f5204b223b6e53dc406ea0bcd76d9e98c9ae4942037902883d4bb22a<br>e1ad66cc0244fc075e0aabe0fd19502d4c9617829b90aa210e74be1d915275d2<br>a7f0fdfdfdf1ef65799fd2114bf5c1e133a8b7635b498b334553fbb64b218a05<br>68278b40b59b1b0db2f814d2d864f0b9c2b4285f5795d22cabf60715f922989c<br>2f947644c7752ba014eae7971b247be60249a6088923c66ffe9886a7f5c5fe1c |

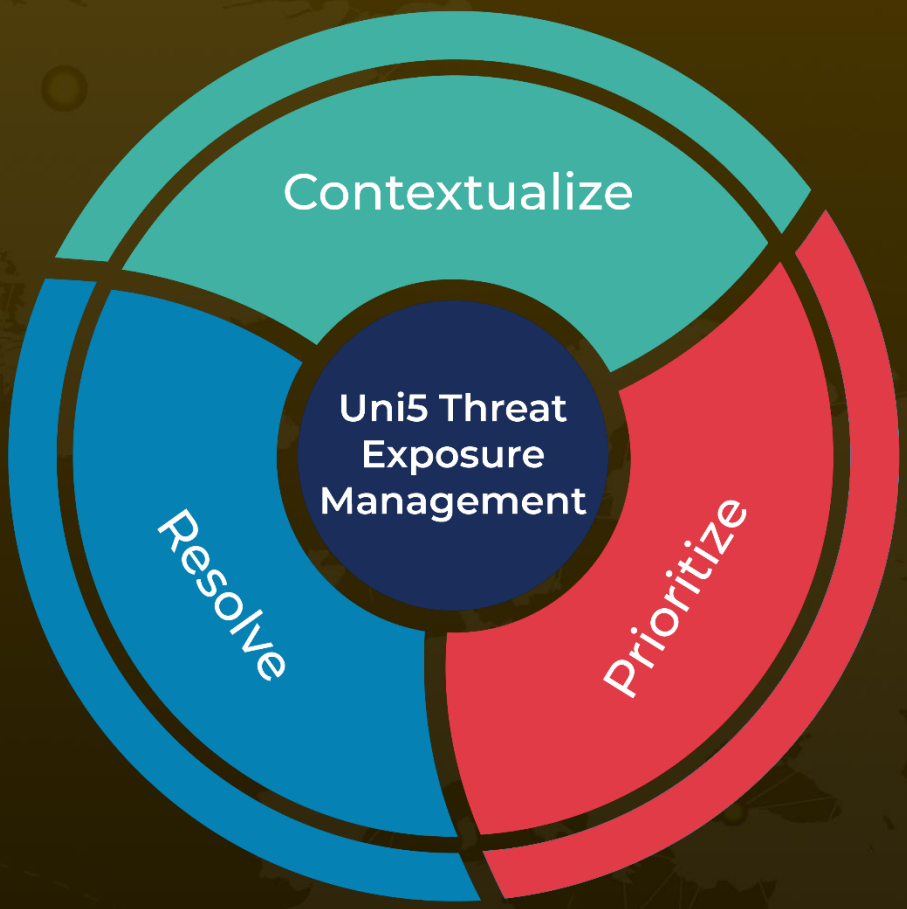
# References


https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/rilide-a-new-malicious-browser-extension-for-stealing-cryptocurrencies/

# 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 14, 2023 • 3:30 AM**



More at www.hivepro.com