Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

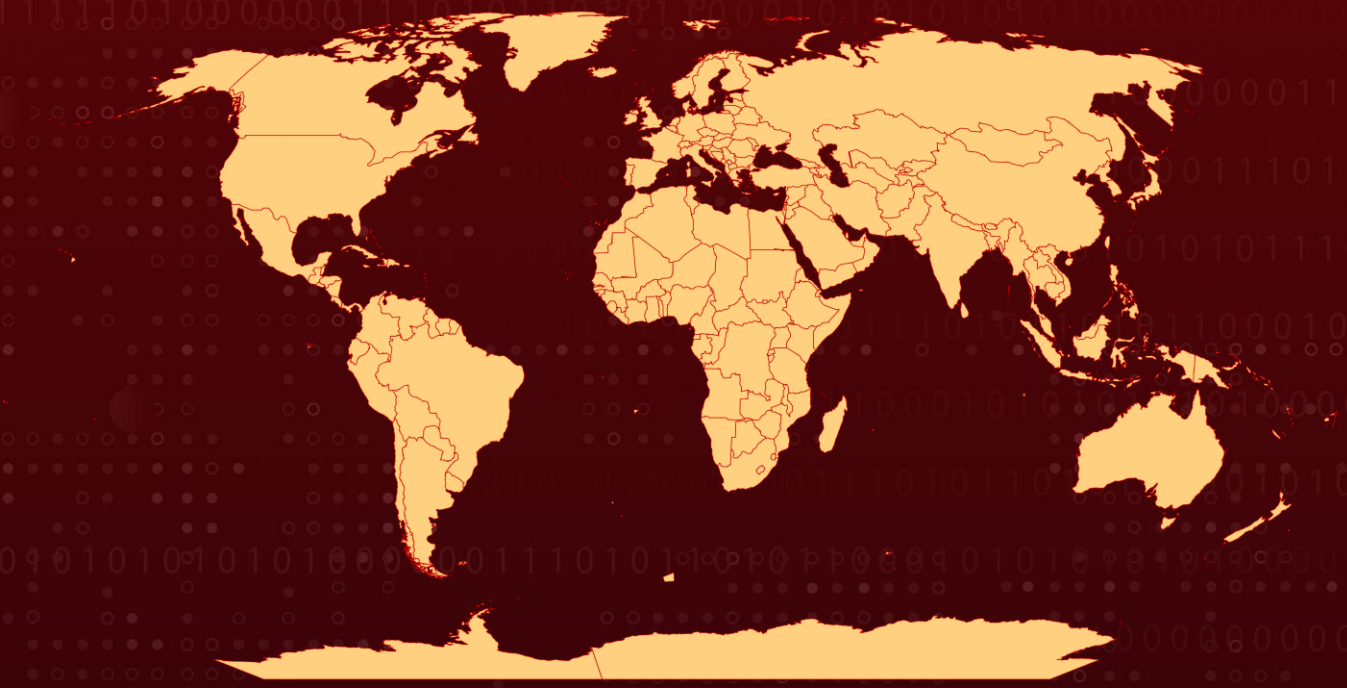
New Version of ViperSoftX Malware Targets Password Managers and Cryptocurrency Wallets

Date of Publication	Admiralty Code	TA Number
May 01, 2023	A1	TA2023205

Summary

First Appearance: February 14, 2020
Malware: ViperSoftX
Target Countries: Worldwide
Target Industries: Consumer and Enterprise
Affected Platforms: Chrome, Firefox, Edge, Brave, and Opera, as well as different password managers such as 1Password and KeePass, and various cryptocurrency wallets like Blockchain, Binance, Kraken, eToro, Coinbase, Gate.io, and Kucoin
Attack: ViperSoftX is an information-stealing malware primarily targeting cryptocurrencies, using sophisticated encryption techniques and monthly changes in command-and-control servers to evade detection.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-24055	KeePass Injection Vulnerability	KeePass 2.5x of before	✗	✗	✓

Attack Details

#1 The ViperSoftX malware is a type of information-stealing software that targets cryptocurrencies. It was first documented in November and its new updates include the use of DLL sideloading for its arrival and execution technique, a more sophisticated encryption method of byte remapping, and a monthly change in command-and-control (C&C) server.

#2 The malware arrives as a package of a carrier executable and a decryptor/loader DLL, typically downloaded from websites or torrents of illegal software solutions. The primary C&C servers for the second-stage download change on a monthly basis. The malware checks for virtualization strings and monitoring tools to check if the system is running a virtual machine, as well as for installed and active antivirus products.

#3 The use of byte remapping, a simple technique that requires the correct byte in the correct location, provides protection against forced decryption. The new version of ViperSoftX targets both the consumer and enterprise sectors, with Australia, Japan, the United States, India, Taiwan, Malaysia, France, and Italy accounting for over 50% of the detected activity.

Recommendations

Ensure that all your software, including operating systems, web browsers, and security software, is always updated to the latest version. This helps protect against known vulnerabilities that attackers could exploit to deliver malware like ViperSoftX.

Use strong, unique passwords for all your accounts and password managers, and consider using a password manager to generate and store these passwords securely. This can help protect against ViperSoftX's password-stealing capabilities.

Enabling multi-factor authentication (MFA) on all your accounts, particularly those with sensitive information like cryptocurrency wallets, can help protect against unauthorized access.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
TA0006 Credential Access	T1074.001 Local Data Staging	T1555 Credentials from Password Stores	T1027 Obfuscated Files or Information
T1074 Data Staged	T1140 Deobfuscate/Decode Files or Information	T1568 Dynamic Resolution	T1568.002 Domain Generation Algorithms
T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter	T1059.001 Power Shell	T1204 User Execution
T1204.002 Malicious File	T1562 Impair Defenses	T1562.006 Indicator Blocking	T1218 System Binary Proxy Execution
T1176 Browser Extensions	T1641 Data Manipulation	T1641.001 Transmitted Data Manipulation	T1321 Data Encoding
T1321.001 Standard Encoding	T1059.007 JavaScript	T1555 Credentials from Password Stores	T1555.005 Password Managers
T1574 Hijack Execution Flow	T1055 Process Injection	T1574.002 DLL Side-Loading	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	09620efdc1324f063aec6aa3d822c194f253d9393c5a7b4f7c8880b8fa260d2c 0d8e99281629352c68e5d1e462db3b003571fdc21149d6834bd2aa2d86ea03b9 2769ff525276045565a15fb959ae54a1ba294eb7903fa80a8656577d7dd5e76c 30a7ff659d267e9e201273087d4ced99f6eefe3078b40f38a1f6c5ff4e6d4fd3

TYPE	VALUE
SHA256	380697610810cdecaa497ad75b031106b486bc6c7da78add23885a963aab6dc0 3d19c605f3d4a84bd76190acd23838e4c9362fef3ec5c80bd049ee25bbafb862 416fad3d260add53a44052b726c1e911632012221c1e28942389ca0dd2902394 4c1021cd1863369e59e9087c34fee936281789e65cbbda464b0948aecb592807 516517135c39aee7b2aeecbfae063deb9b8869ca993f60120d7c5ee90ee90444 51c862efdb6b52c42dfe4f25c471c82c0368c0b9f8b194d07f9dcc4245b46394 5232a2a668c95ee6ab24cba79ed7bf4e9598a750020a2a88a2f352d2f667b7c5 5e9d9016bbb70c1b4b02f13d5a12e112250651a77bf5b89a92d124d0f8576cdb 66c98bb87c3bfc97e137ef3fc22e498ff1fb7368d82c2641db4998d090d31ef4 671756d73f9e8f35f9a71b102d474415aada55f1a846b0c20b73daf554d03173 696978b39b7afc97d4b7d6a3ab56b6b991fab9f9e511e722a2db5b8459679240 6a7ccf87978dad1a2d1a1a52100101fb330d966ff6cd990b1d04eb627ef4530c 6b23b6615b1287bf4ec20eab532921cabeb72e08af089782d5c827e48334ba36 6b8809f6f282778aeaa9634e1108f0776066d32e096526fa4c00cbba3dacc30e 6ca4b83ff71f42e15032e59a47b8275c298d28c2dcc646c4e4325b2243425235 8047b20dc50317fb38f7e805992b65eabad92362acd8ff728903da5a86e4f23d 83b8eca3bc4fe79fa47d918d34917344a2e179b0c4efc5c769b9f3a380a65247 85ecdeb135cf384cb82e62dea82baa7c01f56e88bdabb5784ee7401cd5537e69 8a2939ad4ee9cea394aba543b98076504cfdfafce76cecfb8fc88ade77bb6f59 8eff0c96aecd3f144a26699b8f3d6ec8d44b9ae4154417121f604d5297073cd8 96ddf314a4c6f10936622361416ac9b93b5cf4b61b148bfb42592d22a83f0634 a498168cdac52a10a25499a46e0d30db2db86c4dadd737bb6628c61a99810b79 aaf389bbbe02c31bf4605fcba51b1d5228337358cf66efafe979f782251b7fc5 b59dce85b24f078285d73553a05cd157c11d3495f399b753f21b3e7506bbe60f bb681757fc4dac5a64bf1b263e0ddd16db6e055d0efb2089ad04af5bba007d0a

TYPE	VALUE
SHA256	d07a06783eb4fde909c0f4f09ec6f69a91820010b9327fc7fa318b199f1ca1e4 d5799651ab7bb5939136addde222255f81e090c3c127d05727b71b3b2cbc9860 f1e6821caa29aade550171d640ed5605556e7d074542eea5d5370168f2c09880 f310e01a9ed40b6563b88de23d560cf839079b503260eb86a7bc32160129170b f39386ba9605b7a1ac360a8460c4f5c5fc916d5c159ba3ba226545447cd7e4c7 fa31f03cfbb8ae682deab86660810ca244a718009cf4a24827699d679139067d 083837c37de9fce9e49257bc2b38dec11530b990b023fadc6f82a7cb00685fc0 0ca08b8044c466e286fb5ec2162a23fe35dda700019a1bc9f4528c777abb2a69 1b26d62c80689746de39869dfab8d8f05257bd16e46fe923344988802569be10 204a056399bbb7e1b4fcf2bdd8f463cf2d3ff21d9f7c5b745d74d62eb6184e88 22981d8cd10e0aeede5a2c5c209cf2d1a46b9eb54f85eca9f97d816b202d186b 2f936ccac29c88745093564858c4cb0cd6fed5bba997c3db71d7157f8c530be5 33fb5151edd9f921e0793575b5d1a5a24f75370455b3413405a2e66f02746e47 34ac92dfb29936f8af4e270da0d36b7cb4ffa743b115e2bfed23b0e127b38d0e 46a96def15c2dbd0825d008f11de605e912184aa40dbbe9295333a5d80ec45f9 515f32da068c171f1dd03472be04327d55cf6d2c5d40268fc1e61abb75e86616 53744ca02d82f1f966a3f882a17fbd424955991496b486e8dc4022e5a939c286 5b8b64cfba9e3771f586c5aa4f69fe210ecd1f037a6818cacf31cba543f1958d 6614299d5f9c1754a894597bd4fa894415d455df1dd4da6a96b717d2206b511a 6753eadd2cd36978630a31d9c9efbe12d09cf139916feee0d145b09ad18750f6 6c5d40b9484287b3a8eac469e0383b1309689e22d1726e36428e278cd883cc2f 6d18365010a19c4e74056d7a7c64d1046ef10a02ec7938fc936ac61898db5ed7 70c8cf961923f93aab18e771c2eb4a09683223129944cab26f75bff35449be8a 7176b56faa36c2275ff6728864d40eb92fbf956d0b6ae09907816811be94e22e 7516f43db52f494ce788ba514590d39cf26da53728388a26e400df4c944e1d18 7576ce1542ac29c8f5f7585d8c19b6a716242ef21f9b6a87c92718220544d467

TYPE	VALUE
SHA256	7890a7ae77a4ebeca05c344946d8a0a308e263ca88a8ca4530d6566bffa331b8 7a22bc09774dbd2d982596804f6eb767074019ce33cc5ffe8efa9c2e1972de86 80f0eed86e0499bbafbcb956e7f6f81b6a56dba56716082cf9ed280f35b355e8 90497bf6dc0724220a21694303c816cdc1f8c815f25c2cef5f2f53478d84752e 91a2a76932341c1e0df8f7b4058d87e69133cee839559f0146cccb42f1b14fea 95e6d8d692e7c7bc6e78389c4b8719ee05e6f71d6447aa016b5682496aef0385 978d83bcc3361c62d5974c33f56c2ab72618a13f9ccc0c37c6b1e824fe74e03e 983038dc5a3650de4f5ce46763a5c8e7e4441c5960e0c1f20f3ca9ff1561fefe a2f6ce37dd1c14fb789e1531e04fac2716e659fa5232295cd8b80b2994b93819 ad1b21536bf9892d070b72b0609970677ba45b9e53c05936dfb1a4f299930a84 b006d1043f97d47339ba1b6816d6c728207fe280a56d7fc10e5b7e7f0b969836 b3600c49c758f86e496d2b5efdbad239a218e74ca014c80f6bb7445f6fe7e4c6 b813b13d41fd4d824bd146ba9e7bead121362039ab79379ff15702c54476a703 bbaa007a1f4e3c62615e5886e4b91dc24545ed60232ec8290ec203f12a78d1d7 bd9b5b3ed93ec879a270a767e1beddc836ab5802fcb49e48cb154eb898389e49 c42a6b316558eed903c3c41b7da6120bf809e918da51119cbeea27f7047ab71d cc6bcb0f72789c7781550d0c184a1b94c5592f31e6459cc9754525232938a331 cf7b4af2c9497c97a2a9cb7f0e5818e76ccf534c3392d6b8d16be415d5a8ffbc d1556221a4bac69453c9bafaf7b7c753e3fd36aac171e3695c88265a22bd7889 d28910954ea84e6f8bad1f844333c3945416f6aeb8cb25e76bfee2319d029847 d7d4c5383a032e8090512f18a0e6387e2de78328c6fac8b6bcefc40a07cde212 d80a423aa16751868dd36d144a4a0e06335593c585187d77e2d00e913bbc95d1 dc0fe945dc3fcab4b4fa4ee9868c75d66719941b33189710dc5bf8b981f55ae8 dc58f7bd854e1537085324068f3a6e675831a5c4c441f9a2059cc7c40a59c61a e022dd5086aa6b1bc91489a3ed81a2143b8b78616d3285c00d6df4bc504f32fe

TYPE	VALUE
SHA256	e4c705b6b93315d728d9ee5fd17734f3968620ecdc255955600f06eeefa252d8 e82cf0af68ec6ec4097d7bd0a5573af50aac191484e983bc9b298b30a7185aeb fd60eaf4d48f49ade5641aa928a30ac35721dbee52e69525132a9e3b1981eab7 ff03b15d57942f671b7c0b9cb978873b2314d13bf4f6603e7b26f3339fbe0c2a 0a0b5f64870c166c1fe246a7ac815f738e15dbc8481b985da862026f61c48282 3529336d0733bd2ee92acc8ed332f6c4eed36a8b0b272371ffdeb80117689b26 42018acd1660989d939814b2bdfaac086540f7a793b0d1b5b82ef72cd7dc2d6a 7c028a7a4eccd48049f0b66ab0211cccf136e56d2af8cd27cfb1c720a43993d0 88c46a74d0b7ba05e4641628f546cf29b322f1e0147b5bcb8439f3716f6da847 c73053fafaeff83d1cad7256aaa6ec7ad8e91ee5c2514c8b7b9de0307ae724a0 527982073113924b7e168b8fdd21beee42923510b58ca2ab444a4a6a4619f78a
URLs	http://ahoravideo-schnellvpn[.]xyz http://chatgigi2[.]com http://arrowlchat[.]com http://static-cdn-349[.]net

Patch Links

https://sourceforge.net/p/keepass/discussion/329220/thread/a146e5cf6b/

References

https://www.trendmicro.com/en_us/research/23/d/vipersoftx-updates-encryption-steals-data.html

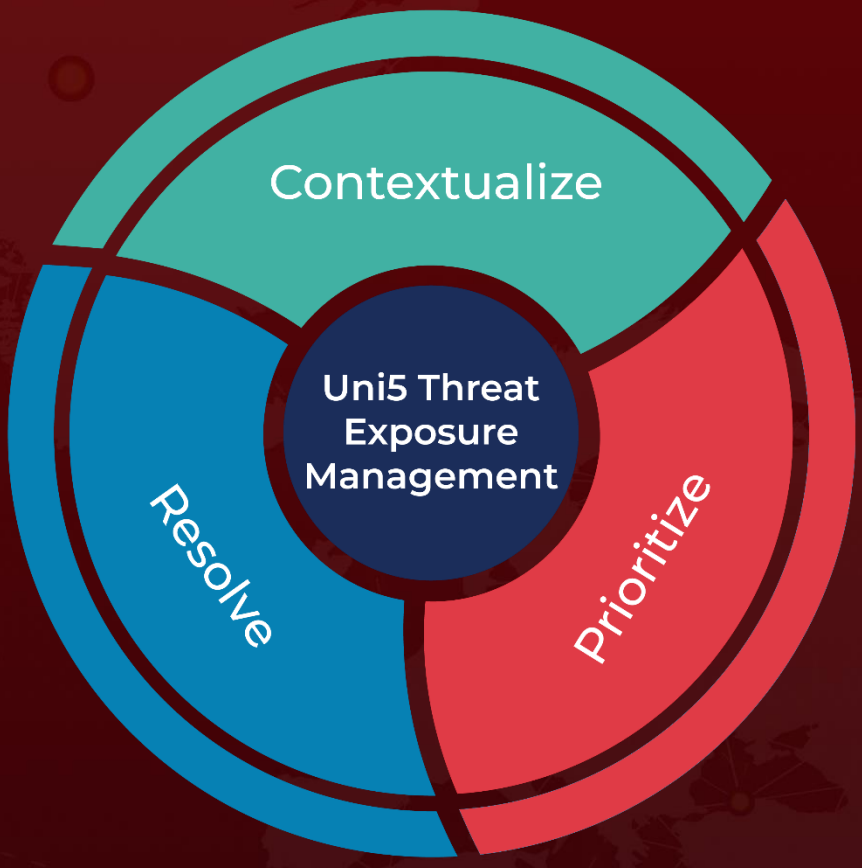
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/d/vipersoftx-updates-encryption-steals-data/IOCs_ViperSoftX-updates-encryption-steals-data.txt

https://www.bleepingcomputer.com/news/security/vipersoftx-info-stealing-malware-now-targets-password-managers/

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

May 01, 2023 • 4:30 AM

More at www.hivepro.com