Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Realst Infostealer Hides Behind Phony Blockchain Games

Date of Publication	Admiralty Code	TA Number
July 26, 2023	A1	TA2023313

Summary

First Seen: July 2023
Malware: Realst Infostealer
Targeted Industry: Cryptocurrency, Gaming
Attack Region: Worldwide
Affected OS: Windows and macOS
Affected Browsers: Firefox, Chrome, Opera, Brave, and Vivaldi
Attack: Multiple counterfeit blockchain games are being exploited to infiltrate both Windows and macOS systems with a sophisticated infostealer developed in Rust, known as realst. This malicious software demonstrates the capability to siphon funds from cryptocurrency wallets and steal stored passwords and sensitive browser data.

Attack Regions

Attack Details

#1 During the beginning of this month, a Rust-based infostealer, known as "Realst," was distributed through malicious websites, cleverly disguised as fake blockchain games. These counterfeit games boast enticing titles such as Brawl Earth, WildWorld, Dawnland, Destruction, Evolion, Pearl, Olymp of Reptiles, and SaintLegend.

#2 Each variant of the fake game has a dedicated website and associated Twitter and Discord accounts aimed at deceiving potential victims. Certain versions of this malware are disseminated via a .pkg installer containing a malevolent Mach-O file and three related scripts. Furthermore, it has come to light that some samples of Realst have already targeted Apple's upcoming OS release, macOS 14 Sonoma.

#3 Most variants try to acquire the user's password by employing osascript and AppleScript spoofing techniques, while also conducting basic verification to ensure that the host device is not a virtual machine. The critical aspect of all these infostealers lies in their ability to gain access to and extract browser data, cryptocurrency wallets, a screenshot of the Desktop, and keychain databases. The gathered data is then stored in a folder named "data"

Recommendations

Use FileVault: Ensure robust data protection by **enabling FileVault**, Apple's in-built disk encryption feature. It safeguards your entire startup disk, including the keychain, ensuring data security.

Exercise caution when installing third-party apps: Stick to trusted sources and thoroughly review app permissions. Unauthorized or poorly vetted apps may gain access to your keychain data, compromising your security.

Implement regular backup: procedures and store the backups offline or on a separate network to safeguard your data against potential info stealer attacks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0010** Exfiltration	**T1059** Command and Scripting Interpreter	**T1562** Impair Defenses
T1048 Exfiltration Over Alternative Protocol	**T1048.003** Exfiltration Over Unencrypted Non-C2 Protocol	**T1070** Indicator Removal	**T1070.004** File Deletion
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1553** Subvert Trust Controls	**T1620** Reflective Code Loading
T1566 Phishing	**T1033** System Owner/User Discovery	**T1555** Credentials from Password Stores	**T1555.001** Keychain

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	77.91.84[.]110, 167.172.103[.]83
SHA1	44aa30ca902a22520b52789b81add44e15e74a50, 713cdae1bc6c68c06d3b9cc18171b5de43957f98, 859e5b3d534c8282d168ebe40c127576dc0b9c70, 8d60062ad8a29b4e88c7b9ec3b649aa30476001f, 963f55a93523c001fdec52ff33ff232e020135e5, 89e1cfc0fa65e4369279b78a26837e6259d4800c, 144665cb2e5d65c88579aa4391cebbc116842536, 56a0b37302829d5fb116d8aa5700dcc3af00dc34, 5da136f267dc70447d420b28dee729d32fdf437f, 6cb07664ef882f7cb98f017b0fbdffe4946e9161, b10b37f3b1ce7aa6dacd4402fcfdb97ba92e1508, b898723602c96ecd04176bd13e6c21dbea82e6de, faf6b11a137bf7ae0ffcab411b02e0c0905260b6, 091f960fe4317696fb30abc3b36d2c8a7eef4b65,

TYPE	VALUE
SHA1	0eeb66a08ca067f168779be8b22da25f90fe4f51, 88880772b0f8723020e0feb2bb179dc71e482072, 6ee0d99e3a56a72c60f3da790268286cd1e7a3ab, 60a747b3e8a25b885ccd16945ba1a238a66e4439, 8054b51a51c8c8f21fe4c51322ef36a9fa02b570, b8ac89eed011c0a4e5f4973acbee888323ec80f0, efccafe8cf2a7d63f82c69882195a565fbd60720, 39060bb82061c5d426d4a7bad66e07888b05b354, b1aac3888403f4597d9cf14b505f572b2fe7d485, d890822af137df48a91f4ba47a27272dcacc9920, 630b23a57d2d8e6d8e25c346173191af6273c3ab, 087b3bf372928279d547fb6bb0ab656717fa8c4b, 0a2a853251fe28333761cc6f9c4518807354dd27, 13bdb3823b8555d846f17bdf381f9568b9a81d26, 29a7eefff22156a72577ed920eaf9b903e9f164a, 2d89ffbadddd62483bc2be33e296ce4e6036c45b, 4e5a59a515981fb97bdb272e3e4acb7118e4e6b2, 9719fd9415d438722f94877c55c9495708c64fee, c205d4ba044f2d69500f10a46c31aaf068e32c44, c716a02e3bc8603fcf0bb8d63fc4f7e3afab471d, dadfbd13b7bd0e9b6d87ebae30bc48c2eeae0eb3, 09e8672af5e18ce99ad8ae608cdc0fa229f121f0, 112b5637c8cbb7d2e216d89f969515809e1dc66d, 154909cdd261130b0ed6d603d4727cb9f15ddc36, 247c50d19e7ad18f466558f9c1785ef29962ab7c, 32f06e3e9d8899f5224f3d5538724d132bda0921, 68dc1f80064f6c261e587cdbb2f01677c8f2e14a, 8b4cdd02330cf25f4e1d338b91ffd1c1dd87021a, ce42d202446cc6b316f668a072c17df87dcd495c, 2f61ddd391d23a6665fa326629e004cb380c4f85, 38ae4fa8f4fec9ab98c0003c455016464b62acce, 65c175f5fad31ea1c938a96a9cdc9987413fd1f2, 80483c5c95ed92da6f086e9497cd08cf7d3b7658, c4296e1a67545e50f44c3776adb674ea1d4d4c0e, d436de35164a045e3c0f7b51cf41fcefedf7e77d, f097123a1999a656a368114abbd848b68d523ee0, 158cf7a0c89544ce1c3294453be2a8c8ced9c9b0, 294392bcf166953c552443fe95ba1e8f15487f74, 294bfc9b97092904bb5e216531b184e38fb2c11f, 3685fdd3d14b500fd73f0a3d16dafcc028035204, 4053e0ecf5f59b6f7afc06750551d77e131ebd2d, 410e4e24f6f6c4f29c8a75723f84bf60ff96c2d5, ada7a47b7fecb142ff532c6e0f01a89bcb47afc9, bfac1b17ad79719c4602a2142435f02c529ec4ab, db9fe7ba9ff8771d28a2fa504d84059faab6be5b

TYPE	VALUE
Email Address	suoeruserff1[@]proton[.]me
URLs	hxxp://77[.]91[.]84[[.]]110:5000/opened, hxxp://77[.]91[.]84[[.]]110:5000/send_analytics, hxxp://77[.]91[.]84[[.]]110:8000/opened, hxxp://77[.]91[.]84[[.]]110:8000/analytics, hxxp://167[.]172[.]103[[.]]83:8080/opened, hxxp://167[.]172[.]103[[.]]83:8080/analytics, hxxps://www[.]dropbox[[.]]com/s/8d6t95xu7x2qbpk/Pearl%20Land%20Launcher%20v3[.]pkg?dl=1, hxxps://www[.]dropbox[.]com/s/br2z1mnirwzfq1r/Destruction[.]pkg?dl=1, hxxps://www[.]dropbox[.]com/s/updohgrf084jj3b/Destruction-x64[.]dmg[.]zip?dl=1, hxxps://www[.]dropbox[.]com/s/8m88qcmbz7obygw/MacBrawlEarth[.]zip?dl=1, hxxps://www[.]dropbox[.]com/s/c68klcfk38syz4o/SaintLegend[.]dmg?dl=1, hxxps://www[.]dropbox[.]com/s/ua1qmbvucb36tls/Dawn%20Land%20Launcher%20%28macOS%29[.]zip?dl=1, hxxps://www[.]dropbox[.]com/s/ka4c9e7yolhq5ze/WildWorld[.]zip?dl=1, hxxps://www[.]dropbox[.]com/s/igvcx4s89trnapa/GuardiansInstaller[.]pkg?dl=1, hxxps://github[.]com/EvolionBeta/evolion/raw/main/Evolion[.]pkg, hxxps://www[.]dropbox[.]com/s/fsm2gthe74ch5w6/Brawl%20Earth[.]dmg?dl=1

References

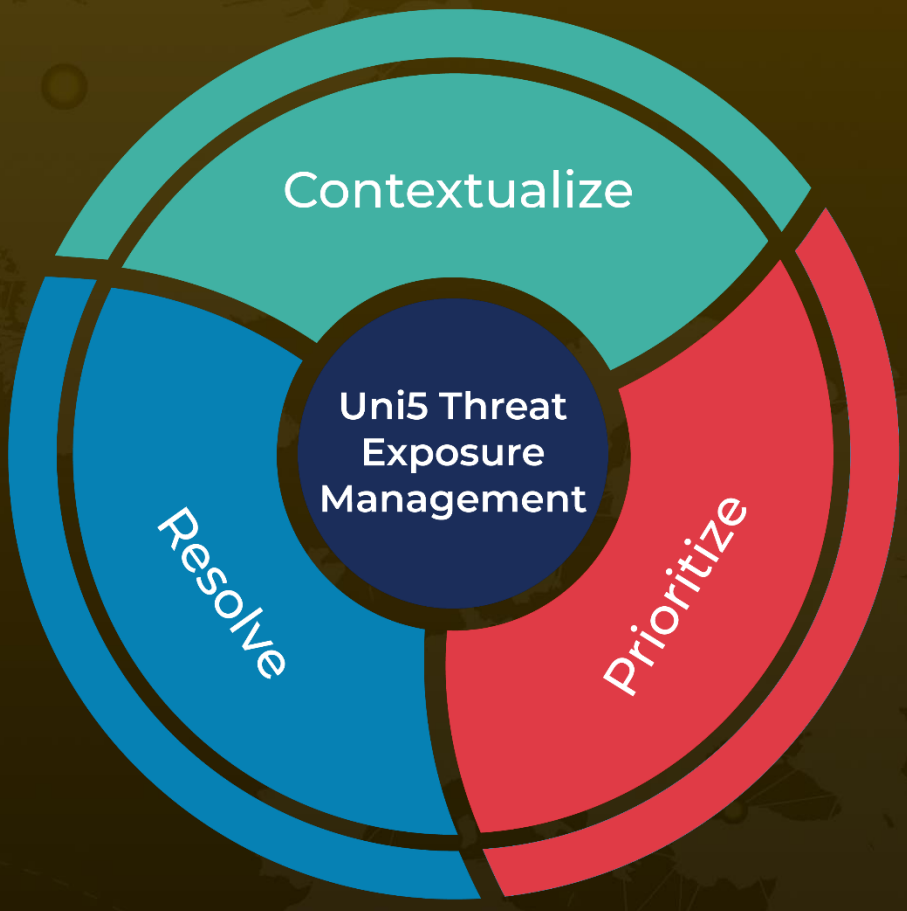
https://www.sentinelone.com/blog/apple-crimeware-massive-rust-infostealer-campaign-aiming-for-macos-sonoma-ahead-of-public-release/

https://iamdeadlyz.gitbook.io/malware-research/july-2023/fake-blockchain-games-deliver-redline-stealer-and-realst-stealer-a-new-macos-infostealer-malware#realst-stealer

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

July 26, 2023 • 4:00 AM

More at www.hivepro.com