KPMG Cyber Threat Intelligence Platform

Realst Infostealer – New Rust-Based Malware Targeting MacOS

Realst is an emerging and highly sophisticated info-stealer that propagates through deceptive blockchain games found on malicious websites. Developed using the Rust programming language, Realst poses a significant threat to both Windows and macOS systems, including the upcoming macOS 14 Sonoma release. The malware employs fake blockchain game offers to trick users, granting it the ability to infiltrate systems and steal valuable cryptocurrencies and sensitive data.

Initial access involves luring potential victims through direct messages on social media platforms to try out fraudulent blockchain games. The distribution strategy of the malware includes dedicated websites, Twitter and Discord accounts, all designed to deceive unsuspecting individuals through deceitful means. Upon visiting these sites, MacOS users fall victim to the Realst data-stealing virus, while Windows users face a similar threat through the RedLine Stealer. Malware is spread via malicious installers like '.pkg' and '.dmg' files using Electron apps or native macOS bundles. 16 variants are identified so far & categorized into 4 families that use similar functions but different implementations. Family A uses "AppleScript spoofing", Family B divides strings, Family C extracts from the keychain & Family D prompts victims via Terminal. Malware is embedded with scripts like "game.py" and "installer.py" which are further used to steal keystrokes, scrape password & sensitive data from browsers, crypto wallets, etc. Stolen data is exfiltrated to specific URLs, or public and private telegram channels which allows attacker to retrieve harvested information.

Realst's varied samples show strong efforts to target macOS users for data and crypto theft. Fake game sites, Discord, and Twitter are used to deceive users into launching data-stealing games. Caution advised due to growing interest in blockchain games promising earnings.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

Realst Infostealer – New Rust-Based Malware Targeting MacOS

Indicators of Compromise: IP Addresses	
37.220.87[.]1	78.153.130[.]209
77.91.84[.]110	212.113.116[.]143
167.172.103[.]83	

Indicators of Compromise: Domains	
evoliongame[.]com	pearlapi.eu-4.evennode[.]com
guardians-game[.]com	dawnland2.eu-4.evennode[.]com
playdestruction[.]com	peallandik.eu-4.evennode[.]com

Indicators of Compromise: Hashes
dd2507cefe8f866c87d9712aa5dca3ac
fdff0ccba08c8cc681759c55fa2f5103
1a5a07479f497aa1db945de48ea85de9
a2b214e13b90a307f72bf769dd81b390
9da6a8e9d56d6ef316d51352c81236ed
acc451f7b0de769d8e884c81b522b3ff
7ad5c63ab4d07fa7c95c6fd8e4b5f5d7
4f82e622161a1d3c94fd15474a664309
c85123e4d4bd6c9ef3deef3b87fc831b
13214ee2e2b5a453e713b6370db773f5
e68c36c4c6f28b6cdd3fce0675aca192
950e1390092ce15738f8fd0a34af1378
a90a934e41677fde8c7301bb28ee8ef0
d7c9e6e5ab89ffeac7adf595e28e90a1
f28c2b5c60c28841d3633038b1339ba4
91f60e4863245cb63a961923b6522a95
abf3fb28c2d2e17c9b1bcacd36ed890f
9a584cc2ec75975b803041ba24659d72
c96799ca54a8136f59fff5773ef1d7d4
9853a3c3469dfb3bce951c5c40ad4399
646f3b6da87d05eb5364c942e670c94c
8e8b68944650838a6ca278fbcc4c2dcc

KPMG

KPMG Cyber Threat Intelligence Platform

Realst Infostealer – New Rust-Based Malware Targeting MacOS

Indicators of Compromise: Hashes
091f960fe4317696fb30abc3b36d2c8a7eef4b65
0eeb66a08ca067f168779be8b22da25f90fe4f51
88880772b0f8723020e0feb2bb179dc71e482072
6ee0d99e3a56a72c60f3da790268286cd1e7a3ab
60a747b3e8a25b885ccd16945ba1a238a66e4439
8054b51a51c8c8f21fe4c51322ef36a9fa02b570
b8ac89eed011c0a4e5f4973acbee888323ec80f0
efccafe8cf2a7d63f82c69882195a565fbd60720
39060bb82061c5d426d4a7bad66e07888b05b354
b1aac3888403f4597d9cf14b505f572b2fe7d485
d890822af137df48a91f4ba47a27272dcacc9920
630b23a57d2d8e6d8e25c346173191af6273c3ab
087b3bf372928279d547fb6bb0ab656717fa8c4b
0a2a853251fe28333761cc6f9c4518807354dd27
13bdb3823b8555d846f17bdf381f9568b9a81d26
29a7eefff22156a72577ed920eaf9b903e9f164a
2d89ffbadddd62483bc2be33e296ce4e6036c45b
4e5a59a515981fb97bdb272e3e4acb7118e4e6b2
9719fd9415d438722f94877c55c9495708c64fee
c205d4ba044f2d69500f10a46c31aaf068e32c44
c716a02e3bc8603fcf0bb8d63fc4f7e3afab471d
dadfbd13b7bd0e9b6d87ebae30bc48c2eeae0eb3
09e8672af5e18ce99ad8ae608cdc0fa229f121f0
112b5637c8cbb7d2e216d89f969515809e1dc66d
44aa30ca902a22520b52789b81add44e15e74a50
713cdae1bc6c68c06d3b9cc18171b5de43957f98
859e5b3d534c8282d168ebe40c127576dc0b9c70
8d60062ad8a29b4e88c7b9ec3b649aa30476001f
963f55a93523c001fdec52ff33ff232e020135e5
144665cb2e5d65c88579aa4391cebbc116842536
56a0b37302829d5fb116d8aa5700dcc3af00dc34
5da136f267dc70447d420b28dee729d32fdf437f
15a1194ef9caa96a696001dd2d79dc90497189f6d38f617efa8f8cfa6be4563d
f05dc9f39141b886a57b1f07c220030333f50af530c8a5663b9ed6f667111969

KPMG

KPMG Cyber Threat Intelligence Platform

Realst Infostealer – New Rust-Based Malware Targeting MacOS

Indicators of Compromise: Hashes
00ac5235afdd1c22b8a28d2f5cbfbf9d5127680d8991cf21abc035222d0a0613
1b490af5dc35d69068318cd0ab4c442d14ce94bc29d207d7973cfcb7a5c6a621
e8b7e12a44d7c605762e8a3220d26c53ee6c179f02f607c899d4e08a8132f6c5
012bfb490493cd15e6f1c1e1638929651a2f65886b60288ec937152b374710d8
016a1a4fe3e9d57ab0b2a11e37ad94cc922290d2499b8d96957c3ddbdc516d74
e581b456d13a52ac58f91f47916950b6e7442c54d7dfb15b76fff844e00e0382
03044ce1dea80b43b94497cc7bad22eb3e9c4c7bd4b4d13f74432152fed19411
066e988a6917647f58ff3d228201f25b8301bde7225f8a498caade91a1cd1f73
fe3ac61c701945f833f218c98b18dca704e83df2cf1a8994603d929f25d1cce2
0271fa9f8eac2a7408b3e8427e8c99fa2256e57d879aa5a28323e05efd3a2845
e9f1012ed31062dfb4e1f8e6df7b1c07e0bf3c3b75d2bce80c724c03c56d09b3
2af0e212ad70eaf8b96a645045ef2764700b5adf7b1187ae3d82240f96f613e2
c729f5715ca5a6039562d9cc52b65cc7ce16ef1ed1451cfc812c7654fa8e3c48
8d506b3527714b7d18d4c9ba292b940aa455876c7bac03b13b00645236f25888
2c321b1416fb7226bffd1633a2a053ef3921fef9a1de5c49b71ef9c7b0914b00
4b93ec3fd49c0111e8a11ac8a0a197f5366cda19732932ce4cb84e024c648a38
016a1a4fe3e9d57ab0b2a11e37ad94cc922290d2499b8d96957c3ddbdc516d74
e0eeb9b87c7ca8b812e9e9a3b6711e0200c80883780b59a3c258c8a3c0d73a29
2c0cc8b60e502e9a2a82a1a6acdfa340ff43608dd6fdad32db9ce99b383513e3
e0eeb9b87c7ca8b812e9e9a3b6711e0200c80883780b59a3c258c8a3c0d73a29
e39cca965dbf7957d04f848572aacfbb736e6aff71e319a788c3f61e52abe795
78b2fa0df9fba56ba6a773faa0d280977a1a830fce4f2427935f87de11cb9012
00dc363063917641ae11eab414a6e2ae8f2e6d671e163339f7b71577f702d068
03044ce1dea80b43b94497cc7bad22eb3e9c4c7bd4b4d13f74432152fed19411
a0b8789ef3249b5fa8eb3590cd6f183e24273b5886560233025fc9d8de52ce0b
149784b07294ec991db4ed913ff726a602d6e071899ddb051a05498a3790bd63
1a5db06dca0667a72d24e092c81f1a3a6d8b535696813012cdc636fc652de743
8050a585fe1d534cafecaa56bda08ce2ef3bc26ea2b0ddad90c6b0c2be1ef3af
b08740de7bd8d6805ca2c3c8be1db69fbb7aa9bd6aad1c0582881e4196574aa9
f5644d70a9885e17dcde888c0270d1b78a0358bb766fccb331742c00c34dda9b
fc438c6e231c80c0d5de5b5a194fdba87f88e334414b248047c5e412ed613a6a
ccbb7510e84df49e1e6bd523ec739ddec71b67e84269d065b0d0ea3942f30471
ff7b879e7fb4f58c954e46125f0c58f2e413a8a729c5e9e3353152cc8e2509f8
64fec4bcd85b3e2129c0e1f3a0201f6effb5667f52067caeba21cade08cd7b94