KPMG Cyber Threat Intelligence Platform

ViperSoftX Malware – A Multi-Stage Malware with Global Reach

TLP : Clear

KPMG. Make the Difference.

ViperSoftX is a sophisticated, PowerShell-based information-stealing malware that was first identified in 2020 and has since evolved to incorporate advanced evasion techniques. Recent variants have introduced enhanced modularity, stealth, and persistence capabilities, including encrypted command-and-control (C2) communications. The malware primarily targets individuals and enterprises in regions such as South Korea, Australia, Japan, the United States, and Southeast Asia, posing serious risks to cryptocurrency users and organizations.

ViperSoftX infiltrates systems through trojanized software cracks, activators, and key generators that users unknowingly execute. To evade detection, the malware checks for existing instances using a GUID-based mutex and delays execution if necessary. Persistence is maintained via a PowerShell script in the AppData directory, a scheduled task (WindowsUpdateTask), a Run key in the HKCU registry, and a batch file in the Startup folder. Communications are disguised as legitimate traffic using the .NET HTTP Client, with all data base64-encoded and transmitted over HTTPS. The malware periodically retrieves a server ID and resets the session if the backend infrastructure changes, ensuring continued control. System information including OS version, username, installed applications, and public IP address are collected via fallback web services. ViperSoftX then searches for digital wallets and password managers to target sensitive assets. Collected data is XOR-encrypted and exfiltrated to the C2 server. Responses from the C2 are then decrypted and executed using PowerShell background jobs that run silently and asynchronously to avoid user detection and maintain system stability.

ViperSoftX evades detection through fileless execution and encrypted communications, necessitating script-level auditing and behavioral monitoring for effective threat mitigation.

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.

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

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

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

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

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

ViperSoftX Malware – A Multi-Stage Malware with Global Reach

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
160.191.77[.]89	185.245.183[.]74

Indicators of Compromise: Domains	
chatgigi2[.]com	wmail-blog[.]com
arrowlchat[.]com	contaboserver[.]net
myststemsgame[.]com	static-cdn-349[.]net

Indicators of Compromise: Hashes
0ed2d0579b60d9e923b439d8e74b53e1
0efe1a5d5f4066b7e9755ad89ee9470c
197ff9252dd5273e3e77ee07b37fd4dd
1ec4b69f3194bd647639e6b0fa5c7bb5
fc6d6ebc7d9c6897a4e177f00843736d
22ad6535e9de133be1fb61c2d004d7f0
5ec7fe95ccf864a04c639cbd7a34d181
c00e53e8cbb5701157002091db4a2500
c5406f9393033f9d7963b5b18a196b5b
ca3c34d6de7d4a3a192c1fef8f4b368e
896bc30cf98ea2decbf93703e52da0cb
cabfc81913788c7ff73646b0ea02c584
66bdc2d36d460fb25bb2114f770d5ade
7d96642ae24666d204ba6f80357344e7
4e453eb8f3b0359ba3f9d3001bc6557f
b7150c7a3eff69f8e7da129678c27d34
02b5fdab8aa41bcac97a185c1660530a

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

ViperSoftX Malware – A Multi-Stage Malware with Global Reach

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
064b1e45016e8a49eba01878e41ecc37
78fcab271700c972704bd45db512433c
da7b6952930a355ea2959397100b2188
af04b60d2b540575a26fe56f8cc9cdfb
fd6ab61c569c20b811940ebb1a51be10
5a68f0e5440301d96fc13c620b95e8d3
b63bf727e413bb88c745582f2a324cab
5e37a37eb243e78255a426cbe948ef92
8e830d755317dedb5b2ea5e948012f05a7d3b672
2e380dd1fc5b47129925c284bf9a9605ee853dd2
9f0f01ac0e65e3cb6b34dc62613654fe5152769a
ba006337afecb5e6e1387acd40d0c8848a3cde15
2bc1a718e77210d49ffe27f40c6660e3a26f40f1
9a4fb1737c6edd3254bd91fc12acb6703b54b7d5
3f2188a56c8902d273190ee8d7728a6f18704320
1a8d144671324d876315b38121f398da63d94caf
e59d6d96bdb630323eaa19feefd584732fd320ed
749366c9052b77e5084a586d2b0657d04b0c3d21
b1baa751276613d023d8d014846f7ca076126719
36f371c77e31e3a6539790fb698276299d95f02c
9722a6e0e14b4a048ef37eb2726530eb5080fa62
bdaf322d573d18530897211d8cc940fb47975ad7
2ff4646034ec174080ff49c46e38b6ae0f5c1855
91551e98d010a417ba13ab82070ac71fef776f54
f00c3352758a2ab36a3705d86fd5234d24901284
97ab697bf826cfecd448cf5e1af78d477e241b83

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

ViperSoftX Malware – A Multi-Stage Malware with Global Reach

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
5e4d062d6430e9035593801d913d3ae2da9e9893
30ecc59e35b2a9a968a5b3fc1d5f90f2e9a10bbe
ba7a1e76029ce02ef94303ebff2ad1b6b24b0f04
a2dac3fae7453444a30b2e3cb3a8a9131e6bc939
039489401fb8ff33c1ae11f35ec0fbd7d6387808
c3ec0f45a342a0688c54e274bb26b150f9226b4f
c31d3e9622f598da78cbf58abb328ed2cc53a015
b990107333027f0f52e75406b9ad90e646de0255
5854510d74846befbbb58817c5fe51b02186e7e45eebb38f1a8470a2745b5b2d
24e88b2f16e47212f5667e115f33f5fa352fd1609bdcb21cebd8b517ee695cb9
63cc4b889888273175132bea0de4889e92a84f7877435a045281876dcb8380e1
220d1ba6b2f72975190ae3e8b2b5cdf3a0c526ef50105268411a5039410a100f
b1f12e6aaec7e74198d35e7ee31fa6658a6388cca85d9aabc42e832709373047
3d8e310755b9d0936401cdeb2c4c7fd5a48c1043d1c96f2f1ea424ed8aa681d0
0b70fa121a1b0267a8620e5b8bf000ea80fa3d9f40a1b23642d3332f5f597a53
9614128f6815a66c7b306ff5af169de9f529846073eb11a6036a17485824fd68
b7f472f8ede1fc14427316505375017a1a295424c57cf50dfa82f1e952966eec
0fd307aa85f5fbf0def17df1a2b733c20ffcf235c6129bd2e2b10b2abdbd1995
fd3d4666355d140ab1a7630671c0cac708c2cc0b60a0136c6a5fa1b54bf1bb1e
01fd9710f16d78f080665e44066b5c339663c2515dcf6dc874631d1611cb8bdd
0b798ce8880a01eaf5496830e31cde3adceb933b15da8e1cdab6e8796993e23a
2fded09822a516938374cc86f31188fd6101757cd9e5c59ab5f6f23e7105bfb5
408623533e3b1889dee3f00b5bfbb24afaa112a6703c19a4d06158ab871b6962
5896dbc54fe973c18bc0a4505f4a8cfc215f6743609cb29e9d9738c087797e08
d8ad3199fc9c59a76e1109de428d9d89baf5ba13a5e18d7b20fd4dc078355da0
cdf84c4aea1ef4da426ca8160b4a8b2b63b4e495cfe80bae7ea8640ac19e2506

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

ViperSoftX Malware – A Multi-Stage Malware with Global Reach

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
6b8809f6f282778aeaa9634e1108f0776066d32e096526fa4c00cbba3dacc30e
6ca4b83ff71f42e15032e59a47b8275c298d28c2dcc646c4e4325b2243425235
8047b20dc50317fb38f7e805992b65eabad92362acd8ff728903da5a86e4f23d
83b8eca3bc4fe79fa47d918d34917344a2e179b0c4efc5c769b9f3a380a65247
85ecdeb135cf384cb82e62dea82baa7c01f56e88bdabb5784ee7401cd5537e69
8a2939ad4ee9cea394aba543b98076504cfdfafce76cecfb8fc88ade77bb6f59
8eff0c96aecd3f144a26699b8f3d6ec8d44b9ae4154417121f604d5297073cd8
96ddf314a4c6f10936622361416ac9b93b5cf4b61b148bfb42592d22a83f0634
a498168cdac52a10a25499a46e0d30db2db86c4dadd737bb6628c61a99810b79
aaf389bbbe02c31bf4605fcba51b1d5228337358cf66efafe979f782251b7fc5
b59dce85b24f078285d73553a05cd157c11d3495f399b753f21b3e7506bbe60f
bb681757fc4dac5a64bf1b263e0ddd16db6e055d0efb2089ad04af5bba007d0a
c313e51f884672b16adcb0731bc338a554ff351fdbe921d266564c67dc730fcc
d07a06783eb4fde909c0f4f09ec6f69a91820010b9327fc7fa318b199f1ca1e4
d5799651ab7bb5939136addde222255f81e090c3c127d05727b71b3b2cbc9860
f1e6821caa29aade550171d640ed5605556e7d074542eea5d5370168f2c09880
f310e01a9ed40b6563b88de23d560cf839079b503260eb86a7bc32160129170b
f39386ba9605b7a1ac360a8460c4f5c5fc916d5c159ba3ba226545447cd7e4c7
fa31f03cfbb8ae682deab86660810ca244a718009cf4a24827699d679139067d
0a0b5f64870c166c1fe246a7ac815f738e15dbc8481b985da862026f61c48282
3529336d0733bd2ee92acc8ed332f6c4eed36a8b0b272371ffdeb80117689b26
42018acd1660989d939814b2bdfaac086540f7a793b0d1b5b82ef72cd7dc2d6a
7c028a7a4eccd48049f0b66ab0211cccf136e56d2af8cd27cfb1c720a43993d0
88c46a74d0b7ba05e4641628f546cf29b322f1e0147b5bcb8439f3716f6da847
cc35166bacf6491af4bf3251c7173a502e85af8e84239660155b26ec0b9ea3b6
0a4888750a50461effd10757fc9bebfacbc661a9ad57fd4c23eefbc735f7ca94