KPMG

KPMG Cyber Threat Intelligence Platform

ValleyRAT - Returns with Enhanced Capabilities

ValleyRAT, a sophisticated Remote Access Trojan identified in early 2023, is linked to a China-based threat actor. Recent versions feature improved device fingerprinting and unique bot ID generation, enabling targeted attacks and persistent control over compromised systems. The malware boasts an extensive command set and primarily targets large corporations across diverse sectors and countries.

ValleyRAT is often distributed via phishing emails or malicious downloads, utilizing an initial stage downloader that retrieves five files from an HTTP File Server (HFS). The downloader checks for the existence of the file "NTUSER.DXM". If it is not detected, the downloader proceeds to download it from the web. Upon retrieving "NTUSER.DXM", the malware decrypts the file using XOR and RC4 algorithms with hardcoded keys, revealing a DLL file named "WINWORD2013.EXE" posing as a legitimate Microsoft Word executable. It conducts anti-AV checks, downloads "wwlib.dll" and "xig.ppt" from the HFS server, establishes persistence through registry modifications, and hides file attributes to evade detection. The "xig.ppt" file decrypts and injects shellcode into a suspended svchost.exe process, manipulating thread execution to establish C2 communication and initiate the download of the final payload. If the payload is not present, the malware sends Login module.dll_bin to the C2 server for retrieval. The final payload executes via reflective loading techniques, loading directly into memory to evade detection by traditional methods. Employs BKDR hashing for API resolution, and dynamic file attribute settings, providing stealth in its operations.

ValleyRAT's complex multi-stage process demonstrates its sophisticated approach to achieving objectives, necessitating robust preventive measures.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

ValleyRAT - Returns with Enhanced Capabilities

Indicators of Compromise: IP Addresses	
43.132.235[.]4	101.33.117[.]200
119.28.41[.]143	43.129.233[.]146
119.28.32[.]143	43.132.212[.]111
43.129.233[.]99	124.156.134[.]223

Indicators of Compromise: Domains	
kfurl[.]cn	hotshang[.]com
scpgjhs[.]com	wenjian2024[.]com

Indicators of Compromise: Hashes
984878f582231a15cc907aa92903b7ab
56384012e4e46f16b883efe4dd53fcb0
8c0cde825ee2d3c8b60cd2c21d174d4c
85f1c63c40918eb300420152eaf78e2c
0b63f0b83f78dff04ae26fe6b1da3b29
81ab4d6b9a07e354b52a18690f98b8aa
b79c69bb5d309b07e10a316ee9c2223e
ddb3c71de77a18421f6e86bc9fec6697
eb953e5f2a3eb68756f779b3fa4d5c4e
8995fbb4679ddd1516eacb3e453cb1ba
58f7311956c41e99f630286baa49d0ac
cc31928547ea412b9c7655ce958574bd
043b4cbe238bcf0b242dc2874e275bbc
019a5c4e67492e412f08758a06b3b354
abf0e40513a9d614266359e56ca54f90
2c6a865a746ca9f37f9381aa64c2c1be
00296149b1ec62f8280ba0b3d08152ee
02c1f92036278dfeabdc89d1a17da28f
c2ad2a683ff1898dd692e7d856c13d44
e9c4b65d39f73033d6ec3ee79bd39083
4df3bf214daaaafee88c455a384a4421
0d222e3084f9359a555acc3205c789fb
92ae1aff368611d62afe51d43c91bf0b

Indicators of Compromise: Hashes
9aec2351a3966a9f854513a7b7aa5a13
0a55af506297efa468f49938a66d8af9
442f4ea7a33d805fb8944eb267b1dfad
c563f62191ea363259939a6b3ce7f192
d9ae9b2fa642658dc691442e197be96dc0dcd4c1
22cd0f235d5744a0585bebc9ebad2221e61ad5f8
f3f6a4617434ca8ce876ae366d731c336109e83f
beb906af13918b4ce21b02aa758da180e7273945
e69e4abd0d73a93ce4e75105a04c8b2a0f0541cd
63d1d132dc05dd37e4f94dc8e22f3d0c3e700be0
d8477bcd00e5ec0eaec26f640b792a48c420b222
4882903d0ce80b7667fec1839c05edf49f7fb4d9
f95f196eb050fd5e119cd3c0b28a26a48dae4677
857fa64483f911aaf2ed6238dec1b46d7017a1eb
291051e9e5c9a862cb1df2cc048e72d567b17c33
44ffdbb03e7e0b49c39d80e58adb94830feea919
eb409af6918044e9b5f6e009506b4bd89f3a78f7
23028886d38668bfa9245a442683180afd58d812
78eb03018194b7aadf859035d6092fcd7257ef77
08526537a12a645cace2fa84650cb21be87a2cb4
12614dcb5a552b50cc6aff59eaf043943b6bde69
74fdb04c97c04342eef85026d660e09afa13f788
73aa5db126a25014f28fdd9a2a27e48aa2d28deb
96c625be28e6c1f7232779e3ec157170120b2506
d9d132af32f69fa09c86434a0d167db6b4060553
4f1f1da488afd6ce9cf6b22a08d40e50f59b70da
711871dc88828994684a798729174b8ddb66896c
e11065431381023d16190b390504390dfeea16a9
470b18288f1fce4c024be7f7f01d66b062fbe41ff53d7fe50eef9d44ff79ad4b
1cf712b65cb67a06b0376921ffe2a697fc34284140eb6c79738daee3367dfec8
41d7e67176eb1c406fb8c545e4d14fa694a63bf38aa7423d61d8cd48999e40ce
3c9fe665d6170d6791182b565acead30e6c658962dd70af03f29826d4c35081e
24daf0b69dcc17c24bbc858d166cc85270bf82ab57bc159e88f193c7dc0b1501
4215b084afa323f090c209518501d2ae0e9fa27cfc7cfe791a668e8802c6be61

KPMG Cyber Threat Intelligence Platform

ValleyRAT - Returns with Enhanced Capabilities

Indicators of Compromise: Hashes
5010b0a72cf94c29d94e119767e2920ca5589055c89f4852273dc50420eb15e8
0d3dd8eb56184193ac883eb235746bb53e18fa2f8a735afad8eb9b04fe006678
06fc07710e9932a3ca4072adbe5bdea1b59336a888a7e2bdf001bc1f8955e8de
773a1cd04612e4e7346b200b46990d9ecc07aa9f917c0b0d7cc1975241d029ed
36c9500e41f43ef142c73d781669e976e44c472e55a67e27badb5e7f226d188b
8711dd15b2d9ef21c83cda2045bf360136e50399f817f59c21ead6f6d8e59a93
35cf0e36dd5c8ca090b51704dfdad6d939067b61f468f2e181dd0c2b5444bb9d
61d7aacc11ca248ae8c54bd56f3603a592435baa7fb36b5822e7b62e5c8fcd61
8b6694896f82a64ce6fd01d6f724c7ec64596577afd84e690377eb4c5bbe3ca3
2ad2dea7acc4cee8554a072d445bbee5c0ddfcf6b5bd1a2da8eb78c3bea96cba
646e7831bb18374b9abac184f1c6b9ab5e1ae3d919b8a7b311ac824fa869ceef
6b31ef2e4c43ee9fcdf3eeff0be269fa4c31aba5640e58c68c8865b3e625db0e
2393fe7adb5f51d741323d06a5acf477a88e29b6a365b646565750ddb43088e9
e4163490b168b5529fc9b3d60ad6f18bfae0a9eaaf462388fe7f9f53becf5aa9
96c51bca692a2be817edf453408a0bdb3079ca4e264d558de3b03e2063d70d9f
bbffd56707ee8a73de608fd0ab91adfdcc77c05440c6fc3fe3b43193ec500c53
156fbe07471a2ef51eb6c2b00853309eb9d710c21d859ae5b759870c05590d13
f5ebe440931d1d003a51133ad1f727daf2410ba50d9f51818938c269bb7fe806