KPMG

KPMG Cyber Threat Intelligence Platform

Rorschach – New Fastest Ransomware in the Town

Rorschach, (a.k.a BabLock) due to its striking similarity to Babuk and Lockbit, emerged as a formidable malware strain in June 2022, spreading its reach globally, excluding CIS countries. It has one of the quickest time to encrypt and targets platforms across Windows, Linux, and ESXi. Its impact has reverberated across various sectors such as transportation, manufacturing, technology, education, healthcare, and government agencies. The Dev-0569 group suspected to be behind Rorschach, gained notoriety as one of the most active ransomware groups of 2022.

Gains initial access through phishing or exploiting vulnerabilities in public-facing services or by exploiting RCE on email software Zimbra. The threat actor employs DLL side-loading techniques to load the injector by abusing the legitimate Cortex XDR file 'cy.exe'. The payload is protected with UPX-style anti-analysis protection and code virtualization using VMProtect, enhancing its defenses against detection. Once executed, the payload terminates system processes through scheduled tasks and employs direct system calls to delete shadow volume copies and backups, clear Windows Event logs, disable Recovery Mode, and security solutions. The threat actor executes commands by leveraging process argument spoofing to avoid detection. Further, network shared drives are enumerated to gain access to more files in the victim's network for encryption. If executed on a Domain Controller, the malware automatically creates a Group Policy to spread itself to other machines within the domain. The encryption of files is achieved using a combination of the curve25519 and eSTREAM cipher hc-128 algorithms.

To safeguard against such threats, it is crucial to enforce stringent email security protocols, consistently patch and update public-facing services, and proactively monitor for any signs of suspicious activity.

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

Indicators of Compromise: Hashes
3e3d20f82c4ce395b4a1d1ab60363fc6
68967ebc319aacdb0247eae8b3768f04
7e37d457ec756179fb58713b7ff76edf
88167052a74057a93e12673599451baa
f02ff25c2169c6575bdf3cd6f120c324
4b4fd546be8d9f32fb852c000fcc24f7
6bd96d06cd7c4b084fe9346e55a81cf9
58f266404cbbf32c7f45f0cafb96564f
17ac512e7236478951716727dfc8fd06
2c262e801afc2e3b3b9e2edf557e5ac9
d8015f175663a679bb8f3dc9249262d7
6fdc4035601d3b8e70d6edf35a5daa20
7c60c0c03b119332ead410b24c74a3b5
49d61da2ab37f5ff735f4c50d7684cf6
72547c8217f5aa2ef04d1614610b024c
28e9ccce24fe86ede0e53f6afd73dee6
3e49fffd059e80ad27f62543a961ef64
00f0aa59725e32e1b78ba415e3382795
965df3a8aba44bca8acc7000fae70e22
3def86d498ad2ab8ef04159a10076bcb
4a8d3392b96092d766a9e05a7d92d990688b0ced
661db483ff60ad43d8a966bfa3971c65b9c9b6d6
87527c740bdfdab7b86a500fe2551a909bbcfaf0
88e3a57c8d8919aed0200c04b19e08660ca3262e
77cf37b1f30967fef0b2d348e94b34480d4af578
fd3bf4fb6ca878bce3e31344d048697560735555
b99d114b267ffd068c3289199b6df95a9f9e64872d6c2b666d63974bbce75bf2
b711579e33b0df2143c7cb61246233c7f9b4d53db6a048427a58c0295d8daf1c
e14b88795bde45cf736c8363c71a77171aa710a4e7fa9ce38470082cb1bdadbb
aa48acaef62a7bfb3192f8a7d6e5229764618ac1ad1bd1b5f6d19a78864eb31f
66bcad0829a59c424d062b949c2a556b11c509b17515dffecb9cbf65f13f3dc6
03c41019faf7e4cc26ca0dd3a2c41b2115e4c4ebd561402079bc4a20256c1813
2fd264f58ba82a2675280ec8c6759612def2bcc62aa6160f5e23071f67bb67ab

Indicators of Compromise: Hashes
38c610102129be21d8d99ac92f3369c6650767ed513e5744c0cda54e68b33812
7d62a33e9a2fedff6cf27aaa142ff15838a766ccd4a8d326424611e155442775
83052cc23c45ecaa09fe5c87fd650c7f8e708aea46756a2b9d452d40ce3b9c00
88081a21e500e831d86666ca5d7a3d348f7c03bc5c471b6d17d8b18a022f25be
de5a53131225dd97040d48221d9afd98760f7ff2f55613f0d08436891ca632b9