KPMG Cyber Threat Intelligence Platform

Cylance - Tale of a New Cross Platform Ransomware

With recent discovery in March 2023, a new ransomware strain called Cylance, has been targeting both Windows and Linux operating systems. This emerging malware appears to be in its early stages of development, indicating that its creators are actively working to refine and expand its capabilities. Cylance accepts various command-line parameters allowing customized encryption mode and attack tactics. Despite being named after a popular EDR platform, its worth noting that there is no actual relation between the ransomware & Cylance security firm.

Windows variant of Cylance is compiled using Microsoft Visual C/C++ compiler. Upon execution, the Cylance ransomware elevates privileges using Windows API calls to gain access to restricted actions such as modifying system security settings, debugging and restoring files & directories. After execution, the malware creates a scheduled task for persistence and a mutex to ensure that only one instance of the malware runs on the victim's system at a time. Further, it gathers disk volume details using API functions to enumerate directories and files for encryption. Additionally, Cylance deletes volume shadow copies using WMI queries to obstruct restoration activities. The Windows variant of the malware uses Salsa20 for encryption. The Linux variant's attack tactics are largely similar except for the use of ChaCha encryption algorithm. The malware then appends the encrypted files with '.Cylance' extension.

Despite being in its early stages, Cylance ransomware has already proven to be a potent threat, successfully carrying out multiple attacks. With new wave of multiple cross-platform ransomware spreading in the wild, it is important to have sufficient monitoring and coverage of all critical assets with proactive monitoring to minimize the risk of a potential attack.

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

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

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

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

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

Cylance - Tale of a New Cross Platform Ransomware

Indicators of Compromise: IP
146.0.36[.]62
62.182.84[.]61
194.233.93[.]50
195.58.39[.]167
139.99.233[.]175

Indicators of Compromise: Domains	
667fm[.]com	adacaranya[.]com
abttt[.]win	vowlashes[.]co.uk
365heji[.]com	apsocreto[.]online
avdeeva[.]info	allforfun[.]online
365-8119[.]com	991-touring[.]info
117ygh9x[.]com	betfury-platform[.]net
10086253[.]vip	applicationsdown[.]store
060jinbo[.]com	allison2patrick[.]online

Indicators of Compromise: Hashes
521666a43aeb19e91e7df9a3f9fe76ba
4601076b807ed013844ac7e8a394eb33
31ed39e13ae9da7fa610f85b56838dde
79ed9cc42065eddd516347afe3e17986
59a995eb167bb3b7386180d103059e15
63f482fd70043beef0625623d4c05648
58fc241a2abb6daaad22c12f182f9827
b7c2f32ec77f8a47351c6bfc540c4a15
e0ac8b5b2b3c5179b36a2363d60040bc
663081e2767df7083f765a3a8a994982959d4cbe
933ad0a7d9db57b92144840d838f7b10356c7e51
13ab26808c270527c019853e76fb88f5aadf704f
ff602997ce7bdd695a282bd373daf57bea7a051f
dd0c3acb1f9bb4bd5bfc0dda8eafa14019c5d240
14861a7648509a59378e9122ad79c52e03edf856
3945462993f25ff2b19d298e87e04484db2e009b

Indicators of Compromise: Hashes
63adfa123895f60ce523e5f3cf46105826b0ed61
872067726afe12a29e8dc90eac037fa90150ad0c
ec8952dc14bac73174cef02a489539e244b378b7de76c771126a8ba7ce532efd
d1ba6260e2c6bf82be1d6815e19a1128aa0880f162a0691f667061c8fe8f1b2c
7a5e813ec451cde49346d7e18aca31065846cafe52d88d08918a297196a6a49f
f55ce0741ed4615bae5646c644b3a971323ac344b12693495d5749c688d5d489
9e1b4f2d408e187ca641c0c16269069d0acabe5ae15514418726fbc720b33731
8e12b85676aaf45a93c91e2db2065151e19f184907da6d85701ac3b13d0e6052
6a726fb5c93adbae0f3061b40b19745587c0114deb86bd72c90acdd69242cbe0
3bd86f3906f59f627bf65664d2bfacf37a29dbaafeae601baf5eeb544396f26c
dade95dd9dff8ebfe6c8d35b620c1cc87822d018f8f1105851cc015e18a648fb
bf8ad39774cef668a64cc403c2e71a78e10303b1adaced06990a882cf1eab713
949a4ad4cf3dcc3392f825e6bbf5375cff79ac64dca64afef8b5455c3667ebdb
55b10b9c897aee00e6ffcfe61f63f7b0689569928fd0500066762218908d0c6b
1f65433addd2e598137cbbb30cf55f5e45ad3e9f87b083001a9bfd43367d4723
1c6f5bc55fdc675ec5653767aadd094789f28ec2a31119112c45b4e1b1bc7f8b
0ce5d529d00bed33668c3fbb6bb774db03f3b8d3a4359203382dfc378a1c142c
0a751a0516ca17a11f5ae8c1a20afc280ad4bc3d57b84ac5443d4f71b43b4937