KPMG Cyber Threat Intelligence Platform

Ransomware Hits C-EDGE - Payment Services Affected

C-EDGE Technologies, a joint venture between Tata Consultancy Services (TCS) and State Bank of India (SBI), has been potentially hit by a ransomware attack that has disrupted its services. The attack has been attributed to the notorious RansomEXX v2.0 group, known for targeting large organizations with substantial ransom demands. It has primarily impacted Brontoo Technology Solutions, a key collaborator with C-EDGE Technologies. The National Payments Corporation of India (NPCI) was informed of the attack on July 26 and has responded by temporarily isolating C-EDGE Technologies from accessing its retail payments system.

The potential origin of this attack chain begins with a misconfigured Jenkins server, which was exploited to gain unauthorized access. The suspected ransomware attack has impacted approximately 0.5% to 1% of the country's payment system volumes, affecting nearly 300 small banks, including cooperative and regional rural banks. Online transactions for multiple district cooperative banks have been disrupted. In response, the NPCI has temporarily isolated C-Edge Technologies from accessing its retail payments system, leading to the unavailability of UPI, IPMS, and other payment systems for the affected bank networks. NPCI has issued a public advisory and is conducting a forensic audit to determine the source of the attack. At present, there have been no reports of financial losses due to the attack, and efforts are focused on expediting recovery and securing the affected systems.

What should you do?

- Check if you have any direct connectivity with a bank gateway which has been impacted.
- Identify if any of your third-party vendors/providers are impacted due to non-availability of payment systems.
- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Follow updates from your bank and NPCI on the status of services and recovery efforts.

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

KPMG

KPMG Cyber Threat Intelligence Platform

Ransomware Hits C-EDGE - Payment Services Affected

Indicators of Compromise: Domains	
pexxota[.]space	kastellira3[.]space
wellernaft[.]top	awerityubfer[.]club
bowepripos[.]uno	cleantheplace[.]top
timerework[.]fun	artilleryin[.]online
berxion9[.]online	iq3ahijcfeont3xx[.]sm4i8smr3f43[.]com
shrapnell[.]space	iq3ahijcfeont3xx[.]fenaow48fn42[.]com
caliberunity[.]club	iq3ahijcfeont3xx[.]tor2web[.]blutmagie[.]de

Indicators of Compromise: Hashes
aa1ddf0c8312349be614ff43e80a262f
b0fd45162c2219e14bdccab76f33946e
c7b28fe059e944f883058450d5c77b03076b0ea1
b18ff26e82916eba8a7a69e5f5ccf6ba0f87ccf9
cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849
da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5
f983be9d613d636731beba91e404fda55467350aa963ca3896fc1995f12c708d
62e9d5b3b4d5654d6ec4ffdcd7a64dfe5372e209b306d07c6c7d8a883e01bead
6962e408aa7cb3ce053f569415a8e168a4fb3ed6b61283c468f6ee5bbea75452
981e6f2584f5a4efa325babadcb0845528e8147f3e508c2a1d60ada65f87ce3c
98266835a238797f34d1a252e6af0f029c7823af757df10609f534c4f987e70f
ad635630ac208406cd28899313bef5d4e57dba163018dfb8924de90288e8bab3
b6ed0a10e1808012902c1a911cf1e1b6aa4ad1965e535aebcb95643ef231e214
b89742731932a116bd973e61628bbe4f5d7d92b53df3402e404f63003bac5104
d931fe8da243e359e9e14f529eafe590b8c2dd1e76ca1ad833dd0f927648f88b
ec2a22d92dd78e37a6705c8116251fabdae2afecb358b32be32da58008115f77
f9c6dca22e336cf71ce4be540905b34b5a63a7d02eb9bbd8a40fc83e37154c22
09c99e37121722dd45a2c19ff248ecfe2b9f1e082381cc73446e0f4f82e0c468
4cae449450c07b7aa74314173c7b00d409eabfe22b86859f3b3acedd66010458
78147d3be7dc8cf7f631de59ab7797679aba167f82655bcae2c1b70f1fafc13d
259670303d1951b6b11491ddf8b76cad804d7a65525eac08a5b6b4473b42818b
48301f37e92a9d5aa29710bda4eee034dd888a3edd79e2f74990300ffd8eb3b6
48460c9633d06cad3e3b41c87de04177d129906610c5bbdebc7507a211100e98
452c219223549349f3b2c4fe25dfef583900f8dac7d652a4402cf003bf5ecf46

KPMG

KPMG Cyber Threat Intelligence Platform

Ransomware Hits C-EDGE - Payment Services Affected

Indicators of Compromise: Hashes
4b8103cd9fbb0efb472cbf39715becacf098f7ee44bf98f6672278e4e741542b
5c3569c166654eed781b9a2a563adec8e2047078fdcbafcdef712fabf2dd3f57
5ccf8c6bf9c39ccb54c5ebabd596a1335da522d70985840036e50e3c87079ab4
335d1c6a758fcce38d0341179e056a471ca84e8a5a9c9d6bf24b2fb85de651a5