KPMG Cyber Threat Intelligence Platform

Clop Ransomware – Reckless Data Exfiltration Spree

Derived from Russian CryptoMix variant, Clop ransomware has been actively targeting Windows and Linux systems to encrypt and extort ransom. However, the group has recently gone all-out on exploiting the zero-day vulnerability in GoAnywhere MFT since early 2023. The group has reportedly compromised 130 organizations including major banks and hospitals to exfiltrate customer data. The group majorly targets US, Spain, Brazil, Turkey, etc. focusing on sectors like healthcare, finance, media, energy and educational institutions.

Clop targets organizations rather than individuals and employs multiple methods for initial access. The recent data-breaches involve Clop using one of its older techniques of exploiting zero-days in file sharing applications. Back in 2020, the group was found abusing a zero-day vulnerability in Accellion FTA and has tread down the same path this time. The group has exploited a Remote Code Execution vulnerability in Forta's GoAnywhere MFT, tracked as CVE-2023-0669 that allows them to inject malicious code without authentication and gain unauthorized access to stored sensitive data. Apart from this new modus operandi, the group is still capable of carrying out organization wide ransomware attacks. The group uses a suite of malware droppers like Get2, TrueBot and FlawedAmmyy to carry out various stages of the attack. Once inside the environment, Clop is keen on compromising AD for maximum impact & uses it as a means to deliver the ransomware executable to other systems & detonate it.

With Clop becoming cross-platform and constantly evolving attack vectors, organizations must secure their network by frequently patching vulnerabilities and by ensuring constant monitoring. Further, access to admin console of such critical file sharing applications must be limited to few systems in the internal network and not be exposed to the internet.

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.

© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

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

Clop Ransomware – Reckless extorting encryptor

Indicators of Compromise: IP Addresses	
91.38.135[.]67	185.99.133[.]153

Indicators of Compromise: Hashes
f21146030cbe2ebe5a8e3fd67df8e8f3
e42dc20972ce557a0feaf2dda0ae1f3f
3fe02fdd243979106f6d91ae2df8ccff
a04eb443870896fbe9a0b6468c4844f7
3b980d2af222ec909b948b6bbdd46319
a98dc09226b97ddc0d959e0aaa08abe0
34f8228a3f12fa9542f1a4181f96edec
f774a3790fd4f0720f77e3db3bdf9bf3
903b01eff4351f92605e6eaefc6c3e7a
8b8a7b787ef09035d6cec57c4f09c08d
8752a7a052ba75239b86b0da1d483dd7
592a37d9d808f97c43f45ee515e9c914
8fc09cb1540a6dea87a078b92c8f2b0a
91b05a8c97429ef315ddb7e00613f133
0571bb4ecf3dbf5d5185eabd7d03d455
9ca31cf03258d8f02ab4cd8fccbf284b
B65646fd89d5860c470112417a54fb2f
c777107d839938da8c41beacc78802a0e05e8b74
5785023ccac0de3fb47e2214cf66e489e4380346
9d59ee5fc7898493b855b0673d11c886882c5c1d
e3001ef25b1386763caec9b5339ec6ddb0275a71
06e6e5305cf34511b58d77efbff4bc8edb398589
9d97ae1a629fe2ed0ce750d1da1513c5dbf9cf8b
e3001ef25b1386763caec9b5339ec6ddb0275a71
06e6e5305cf34511b58d77efbff4bc8edb398589
9d97ae1a629fe2ed0ce750d1da1513c5dbf9cf8b
2b44afeb746cef483929fb04f15479083ce71323
47250d9d0d4f338f591cff6fe57beea6cc66760e
d6dc7b324388759ff2f88e41406b545f3d422ad3
697b1244e27323cc895b25652243d63e2878bf18

KPMG

KPMG Cyber Threat Intelligence Platform

Clop Ransomware – Reckless extorting encryptor

Indicators of Compromise: Hashes
6eeef883d209d02a05ae9e6a2f37c6cbf69f4d89
87e8d54eb7a494649724804f5cb8f4276090068d
16f48624ea2a575e1bdceb4ac6151d97d4de80b6
2a870e331c2322ed00b22d418173e57c87db71bf
98fe0eb11fcccef4785e433f8c837371ae6eec41
e1fb096873ac5ca990dda56d381f676178159885
57d589642b57f034cd1439fee637f0325cf5b4da
2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb
cf3e3ee221ba2c3d863b97d7f138e741199d16fa833b996d3d8e01d2f1bfae76
bc59ff12f71e9c8234c5e335d48f308207f6accfad3e953f447e7de1504e57af
a867deb1578088d066941c40e598e4523ab5fd6c3327d3afb951073bee59fb02
09ab880f3021ac2d05e09bebd567ddf5f6f7cfb396573efd819a056931f3b391
968307a367471e25bef58b0d4687ab4fdf34539bbfb603b5b19ae99d4d0c0340
94b76ce34e5493bb59586b41f41b23baa07a55f2397e80775573714b1311103c
6e0f1d0b0a4b5ecc7de4f34dc670fc788325e1b4329b1d6e596d66fb47c30ed4
0778c67835cce4819fecc56c1059c791c0cf023a3a2c4db0ac696d1c3966f9e2
111773fea3e49a77d35abfbeffc2b33fd4b0527d36a643f34be123850ae51fb9
3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207
cf0a24f1cdf5258c132102841d5b13e1c6978d9316ba4005076606dc60ec761b
389e03b1a1fd1c527d48df74d3c26a0483a5b105f36841193172f1ee80e62c1b
85c42e1504bdce63c59361fb9b721a15a80234e0272248f9ed7eb5f9ba7b3203
cb36503c08506fca731f0624fda1f7462b7f0f025a408596db1207d82174796a
af1d155a0b36c14626b2bf9394c1b460d198c9dd96eb57fac06d38e36b805460
ad320839e01df160c5feb0e89131521719a65ab11c952f33e03d802ecee3f51f