KPMG Cyber Threat Intelligence Platform

Karakurt: The Conti Extortion Arm

The Karakurt data extortion group, also known as Karakurt Lair is a threat actor group active since late 2021, recognized to be a side-operation of the infamous Conti Ransomware group. They quickly amassed record numbers with over 40 victims to its name with majority of their targets in Canada, UK and Germany. Their ransom demands can range from $25k to $13M worth of Crypto and they coerce their victims into paying the ransom by harassing their partners, clients & employees via Emails and phone calls prodding them to ask for negotiations.

Karakurt group has a diverse set of tactics, techniques, and procedures tailored to the victim environment making it difficult for defense and mitigation. They also skip the encryption process and go straight for data exfiltration. Their approach is to quickly move through its hit list of targets, keeping clear of major business interruptions and focusing on stealthy data exfiltration tactics. These rapid movements suggest that they come with pre-supplied access to victim networks and intelligence. They have been observed to use compromised credentials, service creation, remote management software, archiving software and distribution of command-and-control beacons via Cobalt strike to further their foothold in the victim network and maintain persistence.

The threat actor group has also been observed to extort victims which have been previously compromised by other ransomware variants for instance Conti Ransomware. Subsidiary groups like Karakurt are able to use a modern approach to exploitation and accomplish greater financial success than typical locker model.

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

KPMG

KPMG Cyber Threat Intelligence Platform

Karakurt: The Conti Extortion Arm

Indicators of Compromise: IP Addresses	
5.8.119[.]60	80.93.19[.]227
5.45.83[.]32	37.252.0[.]143
45.8.119[.]60	104.194.9[.]238
31.14.40[.]64	209.222.98[.]19
61.19.125[.]2	95.170.133[.]54
1.116.139[.]11	45.141.84[.]126
185.5.251[.]35	49.232.93[.]149
139.219.4[.]103	61.177.173[.]17
159.65.140[.]76	109.169.14[.]109
172.241.27[.]91	104.243.34[.]214
104.238.61[.]153	46.166.143[.]114
212.220.115[.]145	108.177.235[.]127

Indicators of Compromise: Domains	
kisizo[.]com	karakurt[.]co
karakurt[.]group	confedicial.data[.]download
stok-061153.stokermate[.]com	karakurt[.]tech
omx5iqrdbsoitf3q4xexrqw5r5tfw7vp3vl3li3lfo7saabxazshnead[.]onion	
lhxxtrqraokn63f3nubhbjrzxkrgduq3qogp3yr424tkpvh3z7n4kcyd[.]onion	

Indicators of Compromise: Hashes
e2bce0f3162076fa56de5215fd31e3ab
ca2883a7f300abd755706d3a9b55916b
286aaf0974d06d9b02d11611b2acccef
1bf171b1f388691c3985df6fb6c3f0d1
074863c3352d6dda17dcb8bdc6a8929f
8e6a8cfba63453bd545e0c78b3b3ed9c
3e9f31b4e2cd423c015d34d63047685e
c5762cc7623ae18ec0250a79792ca542
b10f4f4d75ea7f09b2a2063e55c36513
9d75035519940dfc8b8971f2e55915dc
76d2d1a7515e1f1a823484460421db9b
1f354d76203061bfdd5a53dae48d5435

KPMG

KPMG Cyber Threat Intelligence Platform

Karakurt: The Conti Extortion Arm

Indicators of Compromise: Hashes
6966421d99fc56e65aeac52238204c4b
ea0bfac7ee884708606739ffec6714f0
c61965b520ba25ecfb75450d078ca912
b93fd83ec5ce5f660aad93389e296582
0956617f4ad1cc74d3205009775613c4
c3835a817335a2a5150f84df5e05c027
c33129a680e907e5f49bcbab4227c0b02e191770
030394b7a2642fe962a7705dcc832d2c08d006f5
8b516e7be14172e49085c4234c9a53c6eb490a45
fdb92fac37232790839163a3cae5f37372db7235
0e50b289c99a35f4ad884b6a3ffb76de4b6ebc14
7e654c02e75ec78e8307dbdf95e15529aaab5dff
4d7f4bb3a23eab33a3a28473292d44c5965ddc95
10326c2b20d278080aa0ca563fc3e454a85bb32f
86366bb7646dcd1a02700ed4be4272cbff5887af
d18c007d856b98ad09818e62fc05acb755dae86c
8a07e8326dec5b754becce68b5b02b85653d6029
401341a7a604ae8d80d9240cb54dde5e26a5cfdb
05a9b0c93f7e1ca272b4236d489f903c399e5faa
b23c86a6d8593ba601894319362129e614946fbc
7dd646e7dc3fc9a73795cb14b97acd5d21d28d36
3e625e20d7f00b6d5121bb0a71cfa61f92d658bcd61af2cf5397e0ae28f4ba56
563bc09180fd4bb601380659e922c3f7198306e0caebe99cd1d88cd2c3fd5c1b
5e2b2ebf3d57ee58cada875b8fbce536edcbbf59acc439081635c88789c67aca
712733c12ea3b6b7a1bcc032cc02fd7ec9160f5129d9034bf9248b27ec057bd2
0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298
fce5d9eff62cf1c58256b78b92ae68697b363275392e6a255570264a93806ba1
8cfdb99185fba9abd91d915425826ca9c6ce360fe68f4c8430c358ceab0acf24
c249ad169385a38c12ccd58b0aea42934449c76e7c29eda999916cb2450a9061
7fbf191412ca61ef90644bea7a387dd57608a0286cbe99662f932fce8c9bc5f8
5e26dc57b4acce95df56c8096f16f7dd3c01aea3503685bf02d0406e9834d198
3f8d58edaee9f8d3571e71bd25c2067edb94a5a7f49cc7620e092a1d9f8752d4
6fe939ca7356ffaf75c5506a21730db34d7dd842dccb6e212ed5929987624931
58eb77490fc53c592b18bba92f42a14d42e9ad264ca52f0c232fca9ee9f67922

KPMG

KPMG Cyber Threat Intelligence Platform

Karakurt: The Conti Extortion Arm

Indicators of Compromise: Hashes
b911e5e6eaf8c46be7c073dda6fc3dc028387547989050cae26c7e470867cbe7
1d923328e882bd262b6ae340451fa87674f1df23f09f91f71cfada4ebee81519
15a06cf42b4434282e603b4b31bbbbaf0f24fb8b2d85936cf7cce44852804173
190bb297cb9b5cc3713c60be659e2e08dc448d6d04fbc35866064b2a1118037b
7ee22cf0465a76c912f1975a776ad5a94eda55576fad12a6f06c5bc37c25867e
8bb99dd7c8755557d6e3996eb74cb548d20b5e641676eef511a8eb8ce7761316
0373f1b69f90e62a87993f8d65ad12099a7fb4cc864366e6ffe0173a972045fc
434e0536715171d9ee59f27a813bc3e4b432e299880d41dcdf4322e172fb527f
96f8252968b0ce4e675b34aaae9b094a5dcc05618d852dcc4837a6ac36a1e420
1b749c370150fd841784ae78bf2fdc5051754fb9bba52f5acd8879d500b65ee2
465ab7c1fc72b367a83356b95adf2f571e1304736fa91b1a5ec2114d7dd23f8c
435d861aa1e3ce4173f4913789c9536bcbbacef0484382d294b581fe19a24f37
3807440302fc6f6c109919fcbf43b994d35ded5856c44ae80cfe4dbaddd7ed66
6a547a672dc7f5ddf2013eddf84f3734e5ea08ce4f4ad3a20e80472a250da5bb
35ba7624f586086f32a01459fcc0ab755b01b49d571618af456aa49e593734c7
060e6a1dda0c7c5e21b4e7ca1e46c651e9345f3427d0fe3a293a4fcd9ece902b
18b39e97aa7e26a3824566489df5715ddc295de817da1e808e51a527fe8342f0
3e88f6189db5bb5aa78cd4cf7ecab4b5ae2c6398403b8f716477b7e06bff8e46
58f31f13b189b596c27246c54338757af8e1205de588496923f24c93a30c0eb7
596ccc911c1772735aac6a6b756a76d3d55bcecd006b980cf147090b2243fa7b
6fb6118b5785e760160aba9e7142ef079e15e5435d7ff1319d0da0f666899372
876b51660453d8ace37df0d98e6fa45dc6f75f36ee0e6000b3bc20dac4deb05e
683bf53191258474bb5e6d2b1176a9dcc97a728d310d48b6c70e23532a5c2d6b
6d3c4193c61e88c7069179c05a9e1df155ce0267a27fceb3d093d6bf3a4a9d27