KPMG

KPMG Cyber Threat Intelligence Platform

Black Basta: Yet another Rebrand?

Black Basta ransomware group sprang into action in April 2022 and have already attacked a dozen organizations around the globe including American Dental Association & Deutsche Windtechnik. Although very little is known about this group, researchers believe that it could likely be a rebrand of a well-seasoned ransomware group. Judging by the similarities in negotiation style, look & feel of leak site, payment site, etc., there's heavy speculation that it could be a rebrand of the infamous Conti group.

While the initial attack vector & payload delivery remains unknown, analysis has shown that Black Basta ransomware executable stays harmless until executed with administrator privileges. Post execution with required privileges, the ransomware deletes Volume Shadow Copies to deprive the victims of any available backup files. It then establishes persistence by hijacking a legitimate windows service like 'Fax' to launch the encryptor. The boot configuration is then changed to enable the hijacked service to run in 'Safe Mode and the system is rebooted into 'Safe Mode' allowing the hijacked service to execute the payload which encrypts the folders in a multi-threaded encryption routine. The ransomware also sets custom wallpaper and file icon for encrypted files, drops ransom note and reboots back into normal mode post all its operations.

Keen on targeting corporate data, Black Basta follows the footsteps of previous successful groups in the art of double extortion by hosting a leak – "Basta news" to force the victims into paying the ransom. While the group is continued to be closely studied and monitored, organizations must keep a watchful eye on unwanted CPU utilization and strengthen overall security posture to fend off such upcoming threats.

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

KPMG

KPMG Cyber Threat Intelligence Platform

Black Basta: Yet another Rebrand?

Indicators of Compromise: Domains
aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd[.]onion

Indicators of Compromise: Hashes
3f400f30415941348af21d515a2fc6a3
6257f732bfc75408b14a445c224e2a78
998022b70d83c6de68e5bdf94e0f8d71
53fdeb923b1890d29b8f29da77995938
571b8340a0b83b0b5aa1f3575b9e891f
a70F03BEB3A8246595EAB83935227914
30638a4b2fcf493e2c4dd58ea7386902
64146ad89bc89691e2700241776b2c4c
f5eac9bb7a5931fe3c044829d9bd33dd
f4651a600eef52d985bed3a74723b25c
ea2b5b3a785be51d8f616086927a32e9
c803c270fb424d2a925484bea59c80ba
145ce3ed0385962da86e5d78507e425d
f801fbd8a5fccd19ea0b3aef3e961b77
623b13cd65a557c85bf8025b17b24018
a70f03beb3a8246595eab83935227914
bd0bf9c987288ca434221d7d81c54a47e913600a
d8dd8f5269e93e78311c14cf258cb2fa9c885d6c
b87a947f3e85701fcdadd733e9b055a65a3b1308
a996ccd0d58125bf299e89f4c03ff37afdab33fc
b5b72bea332bb21962601cb446ab93fd110f994a
3889abc62b9c643a2c99ce13e6230296c8288e9d
5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa
eb07a24f63d7f56fb13e34dd60e45a4c8522c32892c8be7dca7d3f742fa86b0a
7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e
0a3a4469952ceb03bb4ed00ae63b27a2cf486742dd885b64dab1329ee2a4904b
e64a1150535a823aa2d2c4c92ab8a3804703aae7126500fd000a4447233b65fb
09cab65c35d8ca664e91d2670ec18b31c6a8015beda279986a47633a09be52a6
0ab3379f6dc3a5a62fca6d31030b254dba365bbbac7903ca845c3b0b9cad6086
6a04f5890646e57651e8e15c040dfaceddd889394ec652122e6b494b5507bc0f

Indicators of Compromise: Hashes
0b89d8ba4543092ddb4f900ebb79dbe32b35efcbe954a9c807bbc07746f5d88c
0ba22454e49cf1f6a335889d733cbf398a3fb9b8d6514071d0398113f0c38377
0cae4341aff259fb968a34cd87e829ff6554d480cc926fb44ca327267c86aa88
0ce769f6d067abf628f97066001801f2bb4836bcfd84b8965fd6736ebd8d628c
1253ad0344208f58916d1c4b9e36c62d8be518cf6aa3aece439c396de98e6808
13b79a142de8701d2a445149d28f30c8292fbdc6f7e73f63048df7f2c5d42e2d
141811d4e3c095d7e989c92ecb1ef9dd666108c44a9eff9e472343d3c0913b4e
16e035836a46c8553531ab324b18b6bf85ea82f60ebac595d6bc3b19bb8f1316
179a3ffc362033dc224610b006e3553fee93e0280e479358fac3b6888c4e55e3
1a5ff2b8bcd4777d9de53810bdff53b4f609d6469eb230a3fb697c24cabe849a
1bdf34292ab1c1ea62b5203948ca584a3526b27918f8d57c6d915a6f6135c32f
1e044b39ba32599264d04a3a06d6674e2188ada863b09467a057a07185c5855f
1fde813dd813702cb1a77e9315fa628cb8777c77bd298163c0a310e2dffb3bfb
203d05edd155b8130e9f34f003b2321823a7cce0ffbbffda18beb037c86a2007
22dd9c7f39052cc26b43194373ca4b1fb272be54fffafcfbda4d0a0e969a5e06
298ef56380b8f9f206114708b0bc1d493f1d059e987999e1ee71fcda0584f4ad
07f1301494b5fa21037e7391989ab2255a2a5e6571e7fd134efead7364b54d36
0ac8b25089b91cd55e3bcde3fc0613d9d87e5972167ed2b14ab0430511651c8b
0b330e5ae140978be6b79abe195f0c43a2b687b765c2beb46b60e93ce0f00a3d
102d38fb6d398281bb3121a9c7b4a06eeb08b0ad4f2e4cfbc4a8b61871168c37
1420476284175e207d21935c1c92be22a539e0e2bd6a81608afa5e47881d2895
173cd7247b5dca31e473f842cafc4594d9e514bb5cacaeded3d9d361d8c69685
17cedd65bfbffeee5af0393565d64d7bbd6ed068d2ba4fd97d646561c36757c5
18aad2eff54abc18897a7d08273ee578e930b76d41561d9cdc35a98c55aa2abf
1c4622480b61a040fd65fbec6ab0bcf55c9626180694289caeec44bada964b2e
1d118c0a6e34927643ef611dcb5eeb467891ec87da32f0c51645a5d4c3526f42
1d82b68b451188b96a786997bfcc5a1c5846ba19e0954cb59fac9aa6737d24d9
1f850262a1413cda88bd9fd260380810b04a2b31e9fb12f22fb4dca915e3d388
2208ced9f7e786c62f9eedc819dde9feba44c991ba0f9818fe3fbd82e76f8072
231535dc26060868538e92e701fc6a7084a04cf7587568900bab4bd7b4dd9552
241d140d085cad833fddf217f166e5d36ab7b66fe83061f5145418c0ada05755
246a6c1a85b4d0f1f9df852f55601a2ddf463ec6c4908c4215970ebea35e35b3
262857731e16e960613b5915f8fda3155a6ef4a317d7124ed4c2132c42f68217
26eec1701b44fd24b309736d57394db59d723d9b685dde518be7853171bd6fa8

KPMG

KPMG Cyber Threat Intelligence Platform

Black Basta: Yet another Rebrand?

Indicators of Compromise: Hashes
27394d3f8b63e88be9f1d84d2baa93b288aec51edf3f19f6a6737420567690e0
2967e1d97d32605fc5ace49a10828800fbbefcc1e010f6004a9c88ef3ecdad88
2d12d3f604a37003bdc0ae3c5d56754693b940f37d32372755789c74530ace38
2e481f80488d23c8d37d79bb994e9cb09326b31cda09f54dcd9a014c9707676a
05370a3d2c931f773ceff0c26b50a4121f5eb2b0a78a3895971320f40ec77269
0c2cd14f5652869a230d2046651168eadc44ded0d08ea3e2ac9089c9e5a24fe8
0c7114385f763f26503e7dd77e2db34343d61bb436d52ec15d3836c62e4afa2d
11c8fb8e56a857fc1459fc4b14bd6eeef7d8acba3adf4834b061cd8c85e9a788
20ad3bfbcf05f9f365810e38b97275dafd1a176a51053f88e12508099278473f
2629ec8ac2f9800e5c93616e264cd00eab3dc9c369e5c499496e8bb4c0adeaf0
26454dc5dafaf37107e953a703269304e3a9b4a4d46cdd69a28f31d3a662cb80
283c9e25f2b9e2e87be512d51f77a8d1aa153fe3584f30804e3865d5557c72de
294900325254770a08ac1540521da53fb9994aa3e2b68098edd6f24886976991
2e935e23df0562794bb8045b88436b40373199190af19b7ee3dd128f27e014cc
32dd50286f2c69bba496577661fddafffab42e1cbabaa93dd4ccc81899775b81
35feab4c65755d7ea92e7f11e0a56a6b73b01c5d74139b83802f4f15cd6dae18
3864b1a76b75b566d6e5d89aead5f36debae440e2da2ad11722ab9bb09618dd7
397a78de041380082c5778818843ee9c2b65a9647fbc0d251244e6cac76e170c
444b3ea45104cbb2acdffb5630dbafd52e553068dd9abbb5de325dfafa0c0412
46f6f66f50ce37252f70ae8edcb563a8b25f74671b5b9a665e918772b054a226
4d9a3052f6697c0646b157c95deeba394b5c4f239ac6aa5efde814f69110f3e7
4e8a1374c133ddb4f15b4ddb264c01f40941f8c435c759fa1c16101ed0235bff
52091353144aa18a798ad82c4c6a54c7cd48cb20277ff84e5e7e5895d9b53239
556f11b9d16a8bbe4528527dcb5f1c8b60fe45ddef93d24a69ca5b44bf73a0db
58ad78517f71b17c1423608fdccb0428623546673071e9e4a91492ebc8fd4bee
6286deca561e4e870613a14640b6e3829e1c6eb756fe9c0860ede3bd4d395cfd
63cd7e6eff265c0a666c0b4f64b32e8c634fdf46a43c718f51b5fab56be0eb03
6425ce273083754488385c8e0efd524904fb0b41885992b69d39e304201e24b6
650c3ec5e6f6171a964e01ba22de6baf90a8cc9e27b712b1b1a659e1f9e219f6
67c734db55c73a98b6a66f758df1f842d4364435cd2a6a1868b51cd88a21bde6
6a04f5890646e57651e8e15c040dfaceddd889394ec652122e6b494b5507bc0f