KPMG Cyber Threat Intelligence Platform

HardBit 2.0 – The Ransom Negotiator

HardBit came into light in October 2022, tested the waters and released an improved strain in November 2022. While majority of its operations is business-as-usual, HardBit stands apart with its approach to demanding ransom. Rather than demanding a pre-decided amount, HardBit is known to engage in ransom negotiation with its victims via Tox messenger to arrive at a figure. It is known to demand the victim's cyber insurance policy to fix an agreeable amount as the ransom.

While not having a preferred tactic, HardBit uses traditional ways like phishing, compromised credentials or exposed services to gain initial access and deliver the payload. Post execution, it gathers system information such as CPU, GPU & disk related info, network adapter settings, OEM & BIOS, timezone, hostname, etc. via WMI functions. Further, it specifically checks if FIPS-140 compliance is disabled using Win32 API to ensure the encryption routine doesn't fail. HardBit then lowers the security posture through a series of Registry changes by disabling Windows Defender features like tamper protection, anti-spyware, realtime behavioral & on-access protection. Services related to applications, data recovery & backup tools, and endpoint security solutions are terminated using net stop. VSS service, along with all existing shadow copies & backups are deleted to curb recovery activities. Boot configuration is edited to ignore all failures' & to disable recovery options. To maintain persistence, the payload renames itself to svchost.exe & copies itself to Windows Start-up folder. This is followed by encryption routine, changing file icons to HardBit logo & dropping ransom note.

As considerate as their new ransom negotiations might sound, organizations must refrain from engaging in such dialogue & disclosing insurance related information.

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

HardBit 2.0 – The Ransom Negotiator

Indicators of Compromise: Hashes
c0dab26a6f40cfd75fce1c938a4e15fd
31c0f6553c9407cc19e596eab41a553e
3191feae778309eb99df4e4e25c62f1a
1973990530feba052d3efb2e6a378347
863dee63f41e46b615c8b9a377cbb743
0d29947318fb9e19ab579ea631f8d0ff
f94f309d5610077f4a9022720ac54c00
5ebba0f6c8eb2f346afbbe147e3dcb66
fa1269ea0d8c8723b5734305e48f7d46
bdf898c0f9cc9de6f4098ac390d78aa1
f716efddcb69efb3d59bc768775e8d12
fd3bed7ce09d21f3220db1feec418805
5a7fca904daab425e349d66775f15fa6
be2151dad4ef1474967f803d507e1f67
4c0b556dcbe63a9c4656cdceee745d87
c19eca0e1d4017992532e735d6cd6a66
e490f5d266d2269cc188870af72e76a8
ff696f61f3ffd500ade82b79d5919a61
9e65daf83bc0f87a7c76c6a645ccd8a0
a40be7c36df5bd48efe9f0409c32c3f0
f1a5d0904f42c3870830d49364d7124e
4b99d9d18c858fe6cbf675ee742bd647
20168e7febfd0f9c5781c6fcb15e350e
3db3a5cb290ae35596e45df7c3cf0693
7e537600ac0527db98cef7c0117aa403
bbac4961abdf124914ab4a5f4465a284
17261c449c565ed96200a6a440841254
a9bc1346a393749721476814a85540ab
02448cf9327f3adb0a9f8ee7379d7feb
259750d0793cf0ccf647f7ef7eda6c5f
97cea8a567f863fb837362df671df457
fc20063993ed2baaa24d41ad11c0f258bab5bd7f
d639821e3fbbb15e14b46aed5b98568e3ce045c3
7cb0346e458efb75edeb19e7a1bf6898a51162bf

KPMG

KPMG Cyber Threat Intelligence Platform

HardBit 2.0 – The Ransom Negotiator

Indicators of Compromise: Hashes
1253a3dcaf9de84954410979781 66f677c0ee3db
4076ee9b26fa5e7d826c09e079f738e849369555
b7865edba76ba5722f3e5a50ccaff9ffba0f8098
ce5933b13abf771b922403c22e57dc9a6679ad08
209060797327ef0d83d155468a5f5f81da4b2851
244f421f896bdcdd2784dccf4eaf7c8dfd5189b5
1127932d55c84d22f4cc3023275cb62c1359bd32
e37737898dc84bf63f2a863fbfd3ef3120a5c312
a1a5ba24fbe88c5b58e11dbe87816e0b16f81fcd
12c7f5b6790eeefca2d7577382d3fbb790dc271b
95cee19c0dad7ab1f2b54294424d9c3fb07cd93d
0ea926efea837e425c556b506b14e85bc069e22d
dc2af3d88b20de737621296a30ea2ff7bb05558e
1598038cfbfcfb33cfa069ddba9777eaa9cb4f46
9673aa695b8bac748f6285871629d81d615e655e
f2951ad7ef9dc98f764b4e8ceec1ea854649b5bc
5bdc9e79ca82a6037cff57ee13f7b6efe7eca6d6
5355ca8205baee8d79c4a16f94c454053b6756b0
d62a878b1591218c686eb1ed7b8feed8385889ae
412ad0bc7ac811996d718b9b74fdd20bbe23bc07
58c70bff7264a29fe5b158132754467b8ccb8aa4
d458d36426cb407f5b4b32c47ebbb678e604290d
fd2344a2c2da44f35a4b29b8090c9d2783841228
bcbe4b96aa0e6b8e953a30e35f999ee60bf277ae
7eaa146fdac807ea4dd63c8b88bf499b115504ee
63a667e5104af5165ffce7c38d6d91ebec313d97
cb78117a4140d836c778815b89d0acbb071480f9
4db7b58e64c8e0e3eace27c482f80795deb24981
422e0e4e01c826c8a9f31cb3a3b37ba29fb4b4b8c4841e16194258435056d8a3
a0138b24593483f50ae7656985b6d6cfe77f7676ba374026199ad49ad26f2992
b565a7b25dc4227872fe972ceee9ff8fce91eb10b373ebc9401f4f32348244ef
cb239d641cfa610b1eaf0ecd0f48c42dd147f547b888e4505297c4e9521d8afe
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
fafbe16c5646bf1776dd3ef62ba905b9b2cb0ee51043859a2f3cdda7dfe20d4c

KPMG

KPMG Cyber Threat Intelligence Platform

HardBit 2.0 – The Ransom Negotiator

Indicators of Compromise: Hashes
78be3aeb507db7e4ee7468c6b9384ee0459deebd503e06bd4988c52247ecea24
4514bfd702d5084197bd40c14af52c21178fc9319b878dc28aac09f931e44c03
027d0f9d3b924d76cfa043e7b0b51facb401f2b8bceb1e9778d8bbe87cdc8717
1fce6b44988d023903ec6aff481c986044b64c78f562e80628a54df0502828f7
5791295c637967aefde6512179ec41464ac3e0019773a14b477a127c2e8771e3
40bb7c19d83961a97efc7ee2c9ec195c53e153923c71372b419309922edb230c
4568d5fde617fd6a3755a7e6b0203be74416de79080fa91cbfc410414e200418
3fd3783e9e4fc28fa27e63cccea59dc3bdf1ae71fdd0032f542b9dd0fc9047af
2d34864872eeba29c93f70effb44de1e6c6a520bb1cb609c6a65293b4e20fa5e
322b4de7d8454b6b08483ce17fa4166675078e7c169b5be17d2fa1da10800be9
24e928e255cacb3cb5181c50a1fe525ffb2bda72218a54a9f1c379b3da75a875
4815ad8eaae4fd82c468a97edc49a2d45f97419cacedbbc353a5b278591a4f87
1c6efa2249c42b66eb0b3882459ca1e67c1a01ebc584fb506d0cd3227568ae8b
30030a8032404a01d4ff813e7eeaf9ff008afdfc728e4cfe3e59daa43e1d5088
69a956e3482be98c01f6cbeeeee190ed2363f685f771404a03cce951a726b13b
5ef40d09b49852f665c6d61c0213dc5f881ef3bf82719c4b40e65ee7d6f66a12
eda8e52c3dd40d8c6bda38de1a2804e205f78306baa9acdd9fffedc32c421558
05c974c3b2c3341dd5d22de8e398b1ac8c9bb692331c18e0eaaf35227246062d
d19643c2f0b68378788d722078300b217473f45f4c2349647d05b123de70f7af
4606a528fc50115b4f6ff5cb6594a1435513f567c813b20ee834fe8e2d57d21d
19c8e5e8f63b452283462c57b20d9188a7981d3a91324e064d7e27c0ba93cb92
097eeeeb59fa8c1dceb1bde5578c392182254484c565325bc3dca33f19ccfedb
9c7b593b016ed1cb9204f72cc2bf15d81d3d61c3e1c441af0e8ec6d7aa04786c
b94403ed8166a0abdd4c52a2f7e44bbd06c1ca804ae4da308e06155f60271990
04bf0773f33f6c2ef54baf8be0752ff055adb96a0620d60e7f32e8385e74114e