# KPMG Cyber Threat Intelligence Platform

## BlackByte : Learning from its Mistakes

Making its debut in July 2021,the infamous BlackByte has quickly made it to the top 10 ransomware groups of 2022. The group is back with Go based variants following the release of decryptor by security researchers due to poor encryption in its earlier versions. The group also puts its newly developed data exfil tool dubbed Exbyte to employ double extortion targeting critical sectors like government, finance, etc., in US & other countries around the globe. Distributed as Ransomware-as-a-Service, multiple TTPs are being associated with BlackByte.

BlackByte ransomware initiates the attack by targeting victims by phishing or webshells or by exploiting ProxyShell vulnerabilities in Microsoft Exchange servers. Post gaining access into a system by exploiting the vulnerability, tools such as Netscan, Anydesk are utilized for lateral movement by helping enumerate devices in the network, gather system info and gain remote access. Prior to encryption, it deletes volume shadow copies, deletes scheduled tasks related to ransomware protection, modifies the firewall settings to allow remote connections, disables windows defender and injects itself via the svchost.exe/regedit.exe instance. The ransomware then encrypts the files with ".blackbyte" extension & drops ransom note with ".onion" link for negotiation. Latest variants use an in-house developed data-exfil tool called ExByte, prior to encryption. It also runs anti-analysis checks to lookout for sandbox, debuggers or anti-virus software for defense evasion. ExByte enumerates all files and saves their path. The files are then compressed using WinRAR and exfiltrated to attacker owned account on cloud file sharing platforms.

To protect organizations from BlackByte attack which targets vulnerable applications, public facing applications must be updated and fully patched and multi-layer security should be implemented.

### 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

## BlackByte : Learning from its Mistakes

| Indicators of Compromise: IP Addresses | |
|---|---|
| 45.9.148[.]114 | 185.93.6[.]31 |

| Indicators of Compromise: Domains |
|---|
| file[.]io |
| anonymfiles[.]com |
| 7oukjxwkbnwyg7cekudzp66okrchbuubde2j3h6fkpis6izywoj2eqad[.]onion |
| fyk4jl7jk6viteakzzrxntgzecnz4v6wxaefmbmtmcnscsl3tnwix6yd[.]onion |
| p5quu5ujzzswxv4nxyuhgg3fjj2vy2a3zmtcowalkip2temdfadanlyd[.]onion |

| Indicators of Compromise: Hashes |
|---|
| bb7c575e798ff5243b5014777253635d |
| 9344afc63753cd5e2ee0ff9aed43dc56 |
| 78c378eb28485394d22259db7c33f0e7 |
| 580f30acd2a0828b174ba827fd6f4bb4 |
| 5483da573c6a239f9a5d6e6552b307b0 |
| 336fc2306fdab961bc0ff843a135dfcc |
| 303a9c45c7bf6e8e69f075bac3897145 |
| 20517cc89f5c736f2273586e5c2dd95a |
| 07a9b1fdfb383a2b1d0172802ce01033 |
| c3ce2163fa601199380c21e22a653c0c |
| 8f3ac02e38c6bcaaf235b1607886235a |
| 8d42417ef02e50249fb7f97fcbfbbb8b |
| 47870de17eb7d1758d705b593ac75cce |
| 03011da0f7f2e04ddfc9b8d2356dc4cb |
| 2d8e4f38b36c334d0a32a7324832501d |
| ee1fa399ace734c33b77c62b6fb010219580448f |
| ce92cdd517069ee7f6090340c04b4fe0c1741208 |
| c2eaca8799d335954ef3d9a1867ec1b629ca4f1a |
| ae4b8d4b8ec40bc4fd52ca13c47c46b2bc76f2f3 |
| 9b6a4bf704d4b430bc18caaef42648e743556dff |
| 82228e644a5a7603dfe8606d80e99f8df3f17a46 |
| 40c25f5ddc52fa9215c63bce62ec537138933260 |
| 351198e557151fa0f4eea2b3bb8771d180fa8432 |

KPMG

# KPMG Cyber Threat Intelligence Platform

## BlackByte : Learning from its Mistakes

| Indicators of Compromise: Hashes |
| --- |
| de9d361c8e00cf8fa1c1f96844a74cdc121809da |
| c27e85de8db2f634db44baee4273bbeeb152435c |
| b020684717fe72dd398e0be5c2a36c809221f206 |
| aeffc66ccb1f5750cc4c43ced237ea495b61053a |
| 0f7e3c94b2d3df1722950ff472a06b3f96f65399 |
| f361bafcc00b1423d24a7ea205264f5a0b96011e4928d9a91c2abc9911b433a1 |
| f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e |
| efc2125e628b116eb0c097c699e473a47a280dfcd3e02cada41bdf6969600b41 |
| eb24370166021f9243fd98c0be7b22ab8cbc22147c15ecef8e75746eb484bb1a |
| aeb1b789395357e8cc8dbd313b95f624fc03e037984040cd7c1704775bfb4bd2 |
| 794a5621fda2106fcb94cbd91b6ab9567fb8383caa7f62febafcf701175f2b91 |
| 754ac79aca0cc1bcf46000ef6c4cbe8bebeb50dae60823a1e844647ac16b6867 |
| 572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b |
| 4877ff7c3c2abd349646db1163814811e69b36374e289f5808cc794113ef55ae |
| 477382529659c3452020170d8150820210ab8cbdc6417a0f0ac86a793cd0d9b4 |
| 44a5e78fce5455579123af23665262b10165ac710a9f7538b764af76d7771550 |
| 3fb160e1770fafeedff2d77841bf02108c25cca4cb6d77e3fbf759077f356b70 |
| 20848d28414d4811b63b9645adb549eed0afbd6415d08b75b0a93fbf7cfbf21f |
| 1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a2240779864b1a6474ad |
| 0097b8722c8c0840e8c1a4dd579438344b3e6b4d630d17b0bbe9c55159f43142 |
| ffc4d94a26ea7bcf48baffd96d33d3c3d53df1bb2c59567f6d04e02e7e2e5aaa |
| e434ec347a8ea1f0712561bccf0153468a943e16d2cd792fbc72720bd0a8002e |
| 9103194d32a15ea9e8ede1c81960a5ba5d21213de55df52a6dac409f2e58bcfe |
| 6f36a4a1364cfb063a0463d9e1287248700ccf1e0d8e280e034b02cf3db3c442 |
| 388163c9ec1458c779849db891e17efb16a941ca598c4c3ac3a50a77086beb69 |
| 01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd |
| 8d2581e5cc6e6fdf17558afe025ff84d9023ea636aca74dee39900d8f523e912 |
| 91f8592c7e8a3091273f0ccbfe34b2586c5998f7de63130050cb8ed36b4eec3e |
| 3de8fe5cee8180e93697e4ddca87e721910b9dd922de849cab7b1b3a50e54a00 |
| 884e96a75dc568075e845ccac2d4b4ccec68017e6ef258c7c03da8c88a597534 |
| 9bff421325bed6f1989d048edb4c9b1450f71d4cb519afc5c2c90af8517f56f3 |
| d3efaf6dbfd8b583babed67046faed28c6132eafe303173b4ae586a2ca7b1e90 |
| 92ffb5921e969a03981f2b6991fc85fe45e07089776a810b7dd7504ca61939a3 |
| f8efe348ee2df7262ff855fb3984884b3f53e9a39a8662a6b5e843480a27bd93 |