KPMG

# KPMG Cyber Threat Intelligence Platform

## QBot – Thriving With New Tactics

QBot, (a.k.a QuackBot, Qakbot, Pinkslipbot) with its humble origins as a banking trojan in 2007, has now grown into a sophisticated and formidable threat for organizations worldwide. QBot has since evolved to be capable of stealing sensitive information, evade detections, escalate privileges, download and execute additional malware. QBot has also been linked to distribution of multiple ransomware such as Black Basta, Egregor, DoppelPaymer, etc. Increasing infections of QBot has been observed in US, India, France, UK & Germany, targeting banking, financial, government & outsourcing sectors.

Recent initial attack vector involves large-scale phishing campaigns and email thread hijacking to send attachments or URLs to malicious PDF and OneNote documents. Malicious PDFs contain an image disguised as a notification from Microsoft Office 365 or Azure alert, which on clicking, downloads an archive file containing heavily obfuscated WSF script. On execution, the script connects to remote C2 to download the malware DLL. The OneNote attack path involves batch scripts, JavaScript & HTA files leveraging PowerShell or MSHTA to download and execute the malware DLL. Once loaded, QBot establishes persistence through task scheduler, injects itself into legitimate Windows Error Manager process & attempts to gain credentials through LSASS. It further conducts system discovery and communicates the same to the C2 server. It may also deliver other tools like Cobalt Strike beacon to further exploit the target system.

In conclusion, QBot is still highly active and is acting as both trojan and a malware dropper. It is crucial for organizations to leverage tools and employee awareness to prevent potential phishing attempts. Further, staying up-to-date with latest developments in cybersecurity can help to combat the ever-evolving threat landscape.

### 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

## QBot – Thriving With New Tactics

| Indicators of Compromise: IP Addresses | |
|---|---|
| 78.31.67[.]7 | 185.80.53[.]210 |
| 2.50.48[.]213 | 200.93.14[.]206 |
| 5.75.205[.]43 | 82.127.174[.]33 |
| 70.50.3[.]214 | 91.165.188[.]74 |
| 47.32.78[.]150 | 68.108.122[.]180 |
| 74.12.134[.]53 | 184.176.35[.]223 |
| 94.70.37[.]145 | 208.187.122[.]74 |
| 90.89.95[.]158 | 172.90.139[.]138 |

| Indicators of Compromise: Domains | |
|---|---|
| kmphi[.]com | a1revenue.co[.]uk |
| isoatte[.]com | agtendelperu[.]com |
| rjll.org[.]pk | limpiotucompu[.]com |
| dimingol[.]com | graficalevi.com[.]br |
| myvigyan[.]com | propertynear.co[.]uk |
| smartvizx[.]com | theshirtsummit[.]com |
| chimpcity[.]com | capitalperurrhh[.]com |
| jesofidiwi[.]com | rosewoodlaminates[.]com |

| Indicators of Compromise: Hashes |
|---|
| ebb7d6f41c73ee38f930a91b85382732 |
| 1a328206967348529bc19fe009714fd5 |
| 48f2dc820f3c34b027d84bdf91abd542 |
| bf9ba7fd5686f83c8955ba1acc9491d9 |
| fd60943221a1fc8db047542c7c887f8b |
| acbf3e17aa631000937f1658cbe4b0c2 |
| 532f8501f7499e2542a8e701e92f71e9 |
| f65d09f8897e1a913534281172f6c52d |
| ff8ebe94a6ba5e44b93fd7d3d4ea736a |
| 69a5e2a27296b178c26079469607cf19 |
| 75db6939982f4b034f8aad39cddf50aa |
| 68d9cca5d34f990d37689e8e9e94e778 |
| 6dc0782943440a8120095b0ac9d72103 |

# KPMG Cyber Threat Intelligence Platform

## QBot – Thriving With New Tactics

| Indicators of Compromise: Hashes |
|---|
| 7cccf2703f2607fe6c03d6cd1fbb8afe |
| 383b39ed5c084db53fb0712a9366df62 |
| 5d9e1a89eaf571e719596dad908c70d56ca522f0 |
| c4b81dd13e3d538e153902d2edcb538fce58883c |
| 449d5bdc85cfb527b5c3159ad5278e83f65a68bf |
| 101ab816ce3f438b17f9b9f4b4555a3680be27ed |
| 872fecd4e93e5f823100c9387137597db01be181 |
| 56205e2b7fcf4d165bf8babe63ad22ffad324a1b |
| 488f3826c59f787c811253664c42d8e515ed9b09 |
| 8361e18e20e7377acf3685c6edd89ff65e1e8953 |
| b9bb08a25cd8109587bee7217edfc707a0367b5c |
| 75d1f32b4b545cc4ad8af3249ddd715538704807 |
| 8b3e76df4b65c9c57046bdd654672de3453d7674 |
| 6484c860389f40812f47908c94439f6961565834 |
| 131904f3212ca6ecc8c146d6a65eda98a846014f |
| c1650da1c52020a39f6d44d037fe74b7029c5d90 |
| 54814140f2a8c609caa5b39610fc8a148149138b |
| b99603a7aa97b27891115663c5fa0fc4a3831b1 |
| 0b6b00e097ebf942666af726f6a01f262df5ecb7 |
| c990d717af38f4d79ac8f66c2efbff6d7e56a00fcaf8c34b407bcb15a61ad162 |
| aaa6836b1a960b7ec733fb03685735533f7614db2c151de3c222a7b046670ba5 |
| b442c963ba07858c4daa34db1376f0afb7a713796ceaf6ec5d1fe635a2e97638 |
| 18202bb48fbefe39d09dfd47026114793ebc1967d73e9d583999f4a48f5f33f1 |
| 37625e7bf4f992b7652d194fa8cda2c1b5535f2b6b8843491d16a9f1a236ab35 |
| 083fcb69a8202f63d0b5528fbe9e8d67422be2fb891b84381b8019effb0aea58 |
| 8b75b295d0d52f30ff5d08cd1cc8fde0fb17ca46f76817b3efcfb2954be05e97 |
| 12168e774a0f4823f5d5c6c4ad2357bc72ccd351788d65e1ee7c7ab444518d78 |
| 9f5ee00410dee0884f0b71eb563a2da6c7d637c70d0e0afc2aee1e50c008bf95 |
| 37bcc4325891b743f98e99029ac3e7188ec4a55203f85ac63e109428254c2a8d |
| 8ab735a9a48b4bb80f52b95f4d8cb31075402f8590469e5bd4a2283d5bd6ad09 |
| 5a7aaa552bd5a35cf28fc44d4e893fa01feac0e7d4bad48998ec100c4e8b461c |
| a0b78db0602489bdde29587feb7abcd0e4c539e4cec1e782c1a76855a69a7a8b |
| 8cb725a9c6bd2fd2899006c00e238a8d162b64d67430c45bc26c03a0c42ec262 |
| f2ffe1270f496e0d824e96548559ce9ffcae13cf2ee59322b6e19f62444f6005 |

KPMG

# KPMG Cyber Threat Intelligence Platform

QBot – Thriving With New Tactics

| Indicators of Compromise: Hashes |
|---|
| 4b2241e0763a352001000e4b94d71114968dde1aeefdcb91ce71b415e95b4163 |
| b409eede1efbf8e37c67a164ac47bf6c06fecd2b313103c9e4d4053b04fcb7a2 |
| 939f843a1e7bbee4f9c2afff4add9975e3b48cef5b3051c6ba861ebc1462b3df |
| 8a6cdd99ee6a28671e45ac373ebe052320d7aa04cef4ddf5d1409e3d3e9fd6f9 |
| 247b35b6ea73755ce7b19dd236f6c993fb3765b472c2ebc93b8290c0d587ca60 |