# KPMG Cyber Threat Intelligence Platform

## Ducktail - Malware That Preys on Business Social Media Accounts

Active since 2021 and initially based off of .NET Core, Ducktail malware has undergone updates to a newer version using PHP. The latest rendition specifically targets individuals having access to Facebook Business accounts, irrespective of their level of access. Primary goal is to breach personal and business-related social media accounts by accessing browser cookies, enabling threat actors to harvest sensitive information and promote ads for financial gain. Ducktail operators predominantly use Vietnamese infrastructure, employing shared tactics across multiple targeted countries like Kazakhstan, Ukraine, Germany, Portugal etc.

Threat actors employ multi-faceted approach, combining malvertising & social engineering techniques to gain initial access. Often themed as job postings, the victims are tricked into opening a fake pdf executable file that drops malicious PowerShell script, DLL, & browser extensions. The PowerShell script is then executed, dropping a decoy PDF and terminating the browser after a small wait time. Simultaneously, a malicious library "libEGL.dll" is deployed, modifying the launch string for Chromium-based browsers to load the malicious extension. This extension poses as "Google Docs Offline" stored in a directory linked to the legitimate NordVPN extension for enhanced camouflage. The covert extension discreetly steals Facebook Business Account & Ad account details and cookies. It can also bypass two-factor authentication by using auxiliary options offered by Facebook API and Vietnam's 2fa[.]live services, sending stolen credentials to a Vietnamese C2 server.

Ducktail's frequent updates enable it to get around popular social media platform's user security. Strong host-based defenses and strict security controls on social media accounts are essential to stay safe.

### 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

## Ducktail - Malware That Preys on Business Social Media Accounts

| Indicators of Compromise: Domains | |
|---|---|
| dauhetdau[.]com | cavoisatthu2023asd[.]com |
| motdanvoi20232023[.]com | voiconprivatesv2083[.]com |

| Indicators of Compromise: Hashes |
|---|
| 618072b66529c1a3d8826b2185048790 |
| 691ca596a4bc5f3e77494239fb614093 |
| b4125e56a96e71086467f0938dd6a606 |
| 7296eef8cb11e6e648a72eb30e767001 |
| 6048d59a06bd28c5ee8418f08dfc40e9 |
| c50b7dd6fe4225df984409a507eb8cba |
| c8c598f4a00c442f3bc7ab944fd601df |
| 9a55cc71fdbf468d6fa0ff9e85d5c175 |
| 3b4263545e0bba6fde5993ffa65ec23a |
| 017f6cfa19aa01380c32e3ef0ece27bc |
| 570b64e953bc1263ac2f005f53569ac0 |
| 72f0c57264a8f1648b489103fe0f3b57 |
| 7a9c8a203531141d7969508545206afa |
| 14cbd4148bbfa2a76ca049bfff28e815 |
| dfe5ce49d061c1655d4285810d032586 |
| 301f258bd28783e31bfaea2e825fa963 |
| 3323bcacba0834d72bafb7cd7030b2cc |
| a1eb0683d13696bf4feef9cb64d8b62a |
| 0a640e4bc6859651fb2ea46f39d96f0b |
| 49e913c2174205f601ed77ffccaeeac8 |
| 0ff37ddf8332cf0a8ba98a21405a2376 |
| 54418411d4628fd2b6f4c072810dbe27 |
| 9c95496b857a6b830e9ffde434d4f1b3 |
| f3b9a461910646724df25425205e5b68 |
| 322ca4ee8b2b81ce664273affd370aee |
| 06de661ee417343127387a4c268a291f |
| 936139fc7f302e3895f6aea0052864a6cb130c59 |
| 20f53032749037caa91d4b15030c2f763e66c14e |
| e692a626c6236332bd659abbd4b1479b860bf84a |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Ducktail - Malware That Preys on Business Social Media Accounts

| Indicators of Compromise: Hashes |
| --- |
| d89fcfc4d02217ec9b467cd4b223da70d2556b76 |
| af91268d21c08bf89b17797c6a6b4813b3bd582f |
| 73b9f70ce4535e05555f4865553a7de96d0b6f7e |
| 6151c76874f5a1e14d82ec083fe5ae28b0c6dd98 |
| 10ff9df05ff652c5e4665faff9c2f8e8d12c7474 |
| 28dd7acf5c254a445cca1bb46d967a9b1c1bcbdb |
| 5216dc54a8a481d05810a4f1434c1924d379d07b |
| a513bc9942e610058a3b261600ad25d9d3521d29 |
| f34b4f24070697d477e19999063f72e4a10e7f8a |
| f791ef52bb0941caca728a69c668b1181aeff311 |
| 6eff35b64dbd51205a96478378cfc673106ec37e |
| 6cfff59f20078b21689e1477faa59836b5351c7c |
| 68ad4a24bf5ff7abb43dbcfbaefcd61e5d4a1475 |
| 2aedc40c2ea91bbb39805316ce506bda03d03897 |
| 63c62f6d4cc509cbc1dee1a983c2dc96fe8d2ba7 |
| 7b13f13999b2f0164845e4145415024cd49b3e16 |
| 156c9afd6f0d15f54c1d296dbc195b51abacdfc7 |
| 57e3b5adf08bbe9d4fa60e06ae418a74d2b309f8 |
| f684676221b09d9a1e84e6b38581d04a0051af56 |
| 9ba4f481754a30675cbe41e938db83c59d62b330 |
| 3a16be032d84b34b184c0b7ab1dc99a027ffb8e0 |
| 77979761e9ea253d9f7c5655c24a3ce5db4c9429 |
| 3d4a10eb1f3f83bd9eb79701bc0630afd9fc9c01 |
| 2650e6160606af57bd0598c393042f60c65e453f91cde5ecc3d0040a4d91214d |
| f024e7b619d3d6e5759e9375ad50798eb64d1d4601f22027f51289d32f6dc0ca |
| 385600d3fa3b108249273ca5fe77ca4872dee7d26ce8b46fe955047f164888e7 |
| ece76ea531d6b51b051469b81a64e1c3a962e3d360dd0f302208d2f5be7963de |
| 1f27c6d936213c25f5094cfd20ed6e257e130a7c4a92d2e51b04c474a981cf25 |
| c82b959d43789d3dbf5115629c3c01fa8dd599fbec36df0f4bc5d0371296545a |
| 2b3decf08bf9223fb3e3057b5a477d35e62c0b5795a883ceaa9555ca7c28252f |
| 69257876e2ec5bdbe7114d6ce209f13afbfddb2af0006a6d17e6e91578966870 |
| da13db80b0f3c25b512a1692494f303eff1ff1778a837208f79e2f3c81f8192e |
| bde696a0ae901864716320e3111d5aa49cba3b1d9375dce2903f7433a287b2f2 |
| d4f10bd162ee77f4778ecc156921f5949cd2d64aab45b31d6050f446e59aed5a |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Ducktail - Malware That Preys on Business Social Media Accounts

| Indicators of Compromise: Hashes |
| --- |
| 04dd228d0b088c4116b503c31de22c1746054226a533286bec3a3d0606d73119 |
| 89f016d32707f096cc8daf674e5a9fc2ba6cf731d610f5303d997fc848645788 |
| 7da7ca7fcbc6e8bc22b420f82ae5756ecd3ad094b8ebcbd5a78a2362eb87b226 |
| 655a8ea3bc1baff01639dcdc43a294f8a5dc622e543d8f51e9d51c6eaaae6f6e |
| 1117a93b4b4b78e4d5d6bd79f5f0e04926759558218df30e868464f05bf1bd3d |
| 554353cda0989c3a141c2ab0d0db06393e4f3fd201727e8cf2ed8d136f87d144 |
| b9a984383a5825868c23bc3afdc70e3af2a56d26d002431940d2429c8e88ace9 |
| c6ae36e28668c6132da4d08bca7ceb13adf576fa1dbdb0a708d9b3b0f140dd03 |
| d03e1a0fce0b112bba4d56380c8d1be671845dd3ed90ec847635ba6015bad84d |
| ab95f377bf7ae66d26ae7d0d56b71dec096b026b8090f4c5a19ac677a9ffe047 |
| f59e2672f43f327c9c84c057ad3840300a2cd1db1c536834f9e2531c74e5fd1c |
| ba8eb1a7f18e4cfca7dd178de1546d42ffb50028c8f3f7ba6551f88c11be75db |
| 06afd110d91419ece0114a7fdeaeba4e79fbc9f2a0450da8b4f264e4ae073a26 |
| 64f6cbe9adf91bc4ed457c79643d764a130b0d25364817c8b6da17b03ff91aa7 |
| bdf8dea28f91adcba7780a26951abc9c32a4a8c205f3207fd4f349f6db290da7 |