

# KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emotet Returns with Novel **Evasion Techniques** 



Tracker ID: TN2342 **Date:** March 15, 2023 **Category:** Malware **Industry:** All Region: All

### **Background**

After a three-month pause, Emotet phishing activities restarted in March 2023, when researchers discovered an Epoch 4 botnet began sending emails with zip files containing malicious documents. Emotet continues to employ malicious emails laced with macros to deliver the malicious payload. To avoid detection, the threat actors behind these emails used a novel technique like binary padding, which increased the size of both the dropper document and the Emotet DLL files to 500+ GB.

The document template employs social engineering techniques to persuade users to activate macros. After enabling the malicious document's macros, one of seven hardcoded and obfuscated URLs is used to download a ZIP file until the file is successfully obtained. After that, the macro will verify that the response is 200 (indicating a successful retrieval of the file). If such is the case, it will then assess whether the file is a PE or a Zip file, as the threat actor may employ file formats other than Zip files, including binary-padded PE files.

The macro uses a function to determine the file type of the downloaded payload based on the first two bytes of the file. The macro then deletes the temporary folder files after extracting the contents of the zip file to the target folder using the "CopyHere()" method of the "Shell32.FolderItems" object. To silently execute the Emotet payload and infect the endpoint, regsvr32.exe is eventually executed, and the DLL is loaded with the /s switch.

Binary padding is used to increase file sizes to circumvent file size restrictions imposed by anti-malware tools such as sandboxes and scan engines. The overlay padding for the Emotet DLL increases the PE file's size from 616KB to 548.1MB. The 00-byte padding method is used by Emotet to increase the file size in both the dropper document and the PE files. To evade suspicion by the security software, malicious actors compress the relatively small files with Zip before sending them via HTTP and email, where they are then decompressed and inflated. Further, the system information from the compromised machine is used for reconnaissance and IP configurations.

Emotet has shown to be a tenacious menace, even withstanding the destruction of its infrastructure in 2021. We've seen Emotet evolving throughout the years by adopting different evasion tactics, unique malware distribution channels, and including an extra second and even third-stage payloads into its routines. Users should be cautious of emails from unknown senders or with suspicious subject lines to avoid being infected by malicious spam emails. These types of emails are accompanied with social engineering techniques aimed to convince users to click on a link or download an attachment concealing malware.

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 endeavour to provide accurate and timely nformation. 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

© 2022 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.



This document is for e-communication only.



















## KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emotet Returns with Novel **Evasion Techniques** 



**Tracker ID:** TN2342 **Date:** March 15, 2023 Category: Malware **Industry:** All Region: All

#### **MITRE ATT&CK Tactics**

Initial Access, Execution, Defense Evasion, and Command and Control.

### **Indicators of Compromise \***

Please refer to the attached sheet for IOCs.

#### Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Check the URL the one is visiting to ensure the site is legitimate before clicking on it or downloading software. The intended URL may be like a legitimate domain name, but it may have errors like a misplaced letter.
- End users should be made aware of the latest phishing tactic employed by the threat actors and ensure not click on any suspicious URLs or emails.
- Organizations should ensure that macros are disabled in Microsoft Office program and users should refrain from enabling them when prompted.
- Before emails arrive in the user's inbox, spam filters should be implemented to automatically remove suspicious or undesired emails.
- In order to prevent malware or TAs from stealing data, keep an eye on the beacon at the network level.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

### References

Ian Kenefick, Emotet Returns, Now Adopts Binary Padding for Evasion, TrendMicro, March 13, 2023, External Link (trendmicro.com).

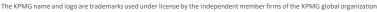
In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI

KPMG in India Cyber Response Hotline: +91 9176471471

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 endeavour 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 © 2022 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.



This document is for e-communication only.



















# KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emotet Returns with Novel **Evasion Techniques** 

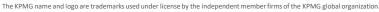


Region: All **Tracker ID:** TN2342 **Date:** March 15, 2023 **Category:** Malware **Industry:** All

| SHA256 Hash  | IP              | Domain   |
|--|-----------------|--|
| 221608d1df1262559e6416acb37d114b0e6c4308e30fcde50b979548f64d709f | 153.92.5.27     | hxxps://diasgallery[.]com/about/r/                           |
| 2112b5695e7bbe910a6efbab32332027a7fd6384f54c55c6e61a26812ad47e6d | 202.129.205.3   | hxxps://www[.]snaptikt[.]com/wp-includes/am4cz6wp2k4sfg/     |
| e34f283e6c42994ac9075cde8a341480f9d0a8f85097f8de3b6b4a959bf8c2c9 | 115.68.227.76   | hxxp[://139[.]219[.]4[.]166/wp-includes/xxrrajtiutdhn7n13/   |
| 9b3119b6183eea08a6934736766f611e44ca00c0ae06aa890cbbbc57b83e6819 | 139.59.126.41   |  |
| 17278c375e4191ab84b5fff5d15a587f8d0b4a47111d0d9fa077fc6ec0e3d6fb | 91.207.28.33    | hxxps://esentai-gourmet[.]kz/404/edt0f/                      |
| 1aa186d60ccf50a91cbbecaa8a97d64e33f5bc7f995685566153dfdbc4524825 | 103.43.75.120   | hxxp://www[.]189dom[.]com/xue80/c0ajr5tfi5pvi8m/             |
|  |                 | hxxp://mtp[.]evotek[.]vn/wp-content/l/                       |
| d2d6f45a9f94e6531d6cd379637243b65a7ea4ad2fa76e4357b0ecff24066141 | 5.135.159.50    | hxxps://midcoastsupplies[.]com[.]au/confignqs/es2oe4geh7fbz/ |
| 1123590c74f22e24e047fb79c74bf61a4d2d52326805d046dd668c4c50b1318e | 163.44.196.120  |  |
| 224c824cb2c3021ce627024afec4dcdc7eba94abce6704ed4a4f1681767a904c | 82.223.21.224   |  |
| 6f9f0b51aaa11810ded4080d39bed24ff7649bc3fccc587ced5e9398951e27e0 | 147.139.166.154 |  |
| 064d6af066c9ffe0b45cd09f7424a4865c6ec839f7786ead27f40bd0ca21a15b | 119.59.103.152  |  |
| 534a5e2bdfdba8041ca3f218b35d35c6f70fef6db7e1b97e9f598a44706f2960 | 186.194.240.217 |  |
| 5400be12ec93d6936c2393bce3a285865e0b5f9280f2c0ce80b1827d07e84620 | 169.57.156.166  |  |
| 9a358c9a72d4c083975ad07939cc61be864d87dc31370be86ad25cfc38f6b5e4 | 95.217.221.146  |  |
| db732daf92ed02271c901c3fbf63cd065babe89d78e666952f1ef8b6cc6be7a9 | 183.111.227.137 |  |
| 9b85d53c592fa72cc4b83d2b1c7fc6b161f02131d82a5a9df5cc9196add8b5d8 | 160.16.142.56   |  |
| 50cf8c54a661864adc325101562012858204c266bd750df2111c1b360295f0b0 | 103.132.242.26  |  |
| 6f2c660d0241bd16353897f2f5053d7881d725cb11c80d4e3219d9a11a93d913 | 79.137.35.198   |  |
| 219b8b680cdb109192f256e6fea049b683ee5b8128821c962ea18dc8261999a2 | 1.234.2.232     |  |
| 6780fdcbeae81f470907367bb0d08a29738d0744344e31b3f125c3bbf139e872 | 201.94.166.162  |  |
| 839c0561c751c954c89eee7648790dba26457a5c450ef895738068c43cc09565 | 45.176.232.124  |  |
| 32c4a024eb1d2e6663eebf5881a6ae1b4e8e8c40cf44083c21a5b8ca52dbe865 | 129.232.188.93  |  |
| aac6d4928496db46eb70c7a9e5a0c27569b45df06e13203d9ed65cc2ba66acb8 | 159.65.88.10    |  |
| 3a5364f5c47a3082d2e5b9a1f9ff2b30bf1455e5a51e022f5a3a0253f74abfe5 | 167.172.253.162 |  |
| c6c30499dc0f62b933373f1bbe7484a94acd265a5d8a42298f970a82b4c883cd | 72.15.201.15    |  |
| 4c6682442c09628d31b0628976be2229243a444c333fa2f21587a09eecb66ff7 | 164.68.99.3     |  |
| f69f5abe3956b2dcb02592209f941d8bbd65630866da650e45d5d9c683d1e981 | 153.126.146.25  |  |
| fbe4c084d44a1b42840ece71b97198bae8ac059311c382c4d8005e6c69e027f6 | 197.242.150.244 |  |
| 38136a459b33a78c7e23691c880cb25ad463f5d615cf85cb8ceecda4e7f9ebc4 | 107.170.39.149  |  |
| 672a1e5a8a0d30687d3510672086e9ca7a29deff46b8a63dd7b7ba6149a01b42 | 173.212.193.249 |  |
|  | 185.4.135.165   |  |
|  | 110.232.117.186 |  |

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 endeavour to provide accurate and timely the information of the intended of theinformation, 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.





This document is for e-communication only.















