# What’s up with Emotet?

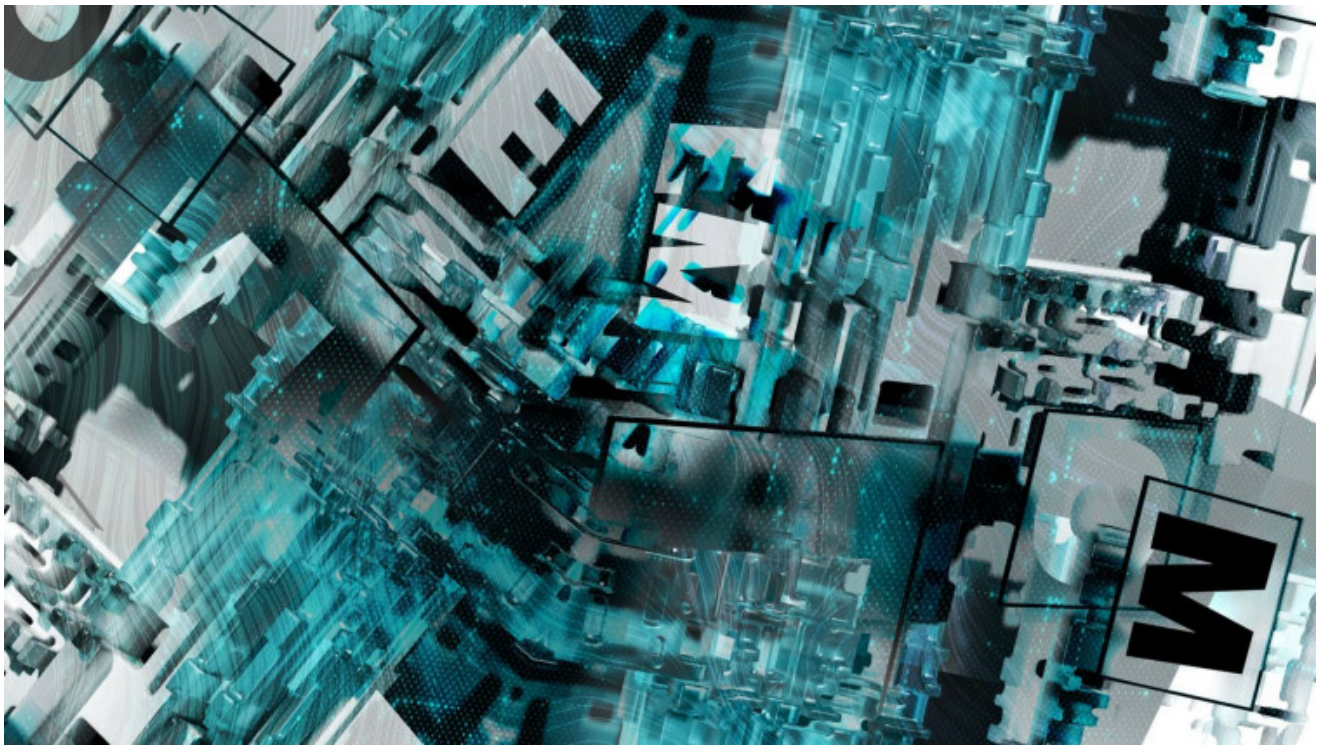
welivesecurity.com/2023/07/06/whats-up-with-emotet/

ESET RESEARCH

A brief summary of what happened with Emotet since its comeback in November 2021

**Jakub Kaloč**

06 Jul 2023 , 17 min. read



Emotet is a malware family active since 2014, operated by a cybercrime group known as Mealybug or TA542. Although it started as a banking trojan, it later evolved into a botnet that became one of the most prevalent threats worldwide. Emotet spreads via spam emails; it can exfiltrate information from, and deliver third-party malware to, compromised computers. Emotet operators are not very picky about their targets, installing their malware on systems belonging to individuals as well as companies and bigger organizations.

In January 2021, Emotet was the target of a takedown as a result of an international, collaborative effort of eight countries coordinated by Eurojust and Europol. However, despite this operation, Emotet came back to life in November 2021.

> **Key points of this blogpost:**
>
> - *Emotet launched multiple spam campaigns since it re-appeared after its takedown.*
> - *Since then, Mealybug created multiple new modules and multiple times updated and improved all existing modules.*
> - *Emotet operators subsequently have put a lot of effort into avoiding monitoring and tracking of the botnet since it came back.*
> - *Currently Emotet is silent and inactive, most probably due to failing to find an effective, new attack vector.*

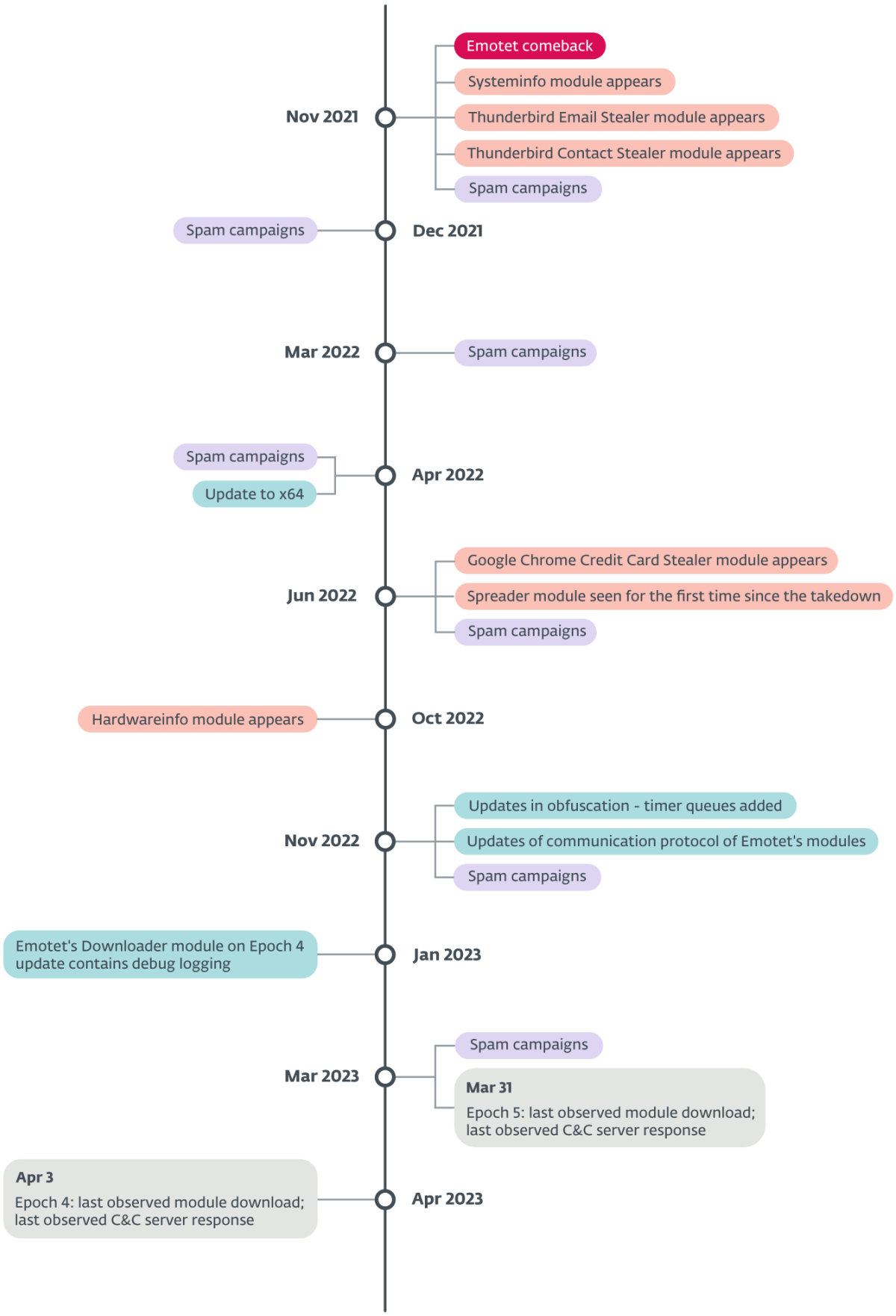



*Figure 1. Timeline of interesting Emotet events since its return*

## Spam campaigns

After the comeback followed by multiple spam campaigns at the end of 2021, the beginning of 2022 continued with these trends and we registered multiple spam campaigns launched by Emotet operators. During this time Emotet was spreading mainly via malicious Microsoft Word and Microsoft Excel documents with embedded VBA macros.

In July 2022, Microsoft changed the game for all the malware families like Emotet and Qbot – which had used phishing emails with malicious document as the method of spreading – by disabling VBA macros in documents obtained from the Internet. This change was announced by Microsoft at the beginning of the year and deployed originally in early April, but the update was rolled back due to user feedback. The final rollout came at the end of July 2022 and, as can be seen in Figure 2, the update resulted in a significant drop in Emotet compromises; we did not observe any significant activity during the summer of 2022.

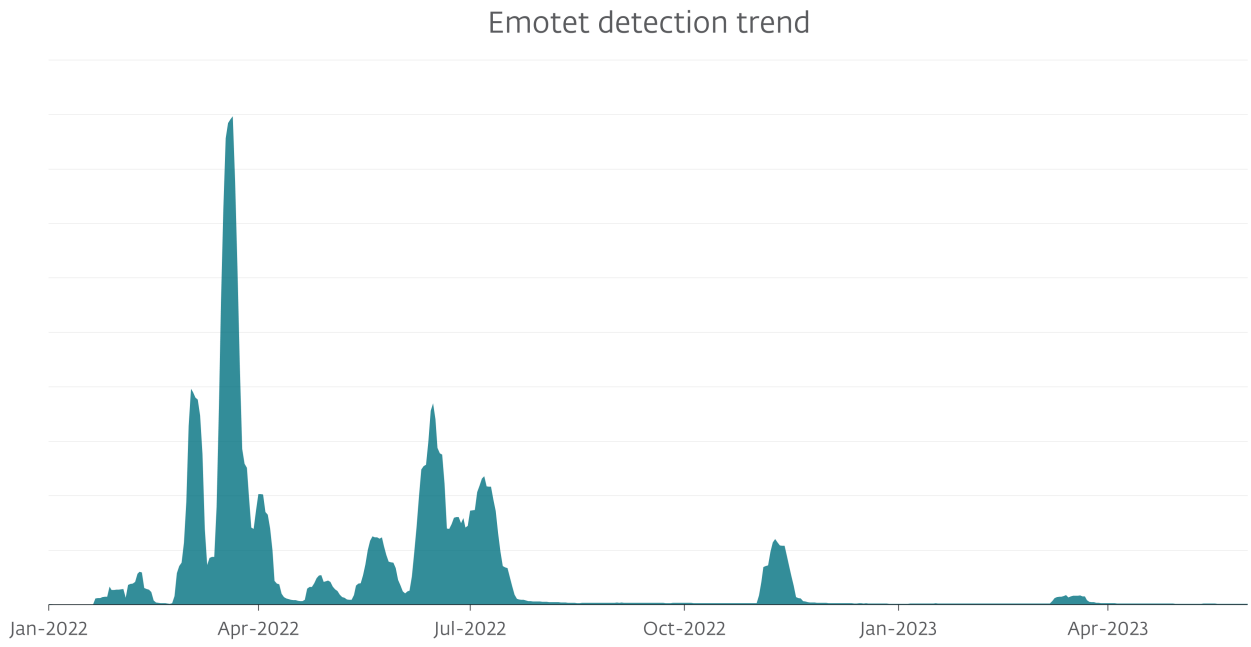



*Figure 2. Emotet detection trend, seven-day moving average*

Disabling Emotet's main attack vector made its operators look for new ways to compromise their targets. Mealybug started experimenting with malicious LNK and XLL files, but when the year 2022 was ending, Emotet operators struggled to find a new attack vector that would be as effective as VBA macros had been. In 2023, they ran three distinctive malspam campaigns, each testing a slightly different intrusion avenue and social engineering technique. However, the shrinking size of the attacks and constant changes in the approach may suggest dissatisfaction with the outcomes.

The first of those three campaigns happened around March 8th, 2023, when the Emotet botnet started distributing Word documents, masked as invoices, with embedded malicious VBA macros. This was quite odd because VBA macros were disabled by Microsoft by default, so victims couldn't run embedded malicious code.

In their second campaign between March 13th and March 18th, the attackers seemingly acknowledged these flaws, and apart from using the reply chain approach, they also switched from VBA macros to OneNote files (ONE) with embedded VBScripts. If the victims opened the file, they were greeted by

what looked like a protected OneNote page, asking them to click a View button to see the content. Behind this graphic element was a hidden VBScript, set to download the Emotet DLL.

Despite a OneNote warning that this action might lead to malicious content, people tend to click at similar prompts by habit and thus can potentially allow the attackers to compromise their devices.

The last campaign observed in ESET telemetry was launched on March 20th, taking advantage of the upcoming income tax due date in the United States. The malicious emails sent by the botnet pretended to come from the US tax office Internal Revenue Service (IRS) and carried an attached archive file named W-9 form.zip. The included ZIP file contained a Word document with an embedded malicious VBA macro that the intended victim probably had to enable. Apart from this campaign, targeted specifically to the USA, we also observed another campaign using embedded VBScripts and OneNote approach that was underway at the same time.

As can be seen in Figure 3, most of the attacks detected by ESET were aimed at Japan (43%), Italy (13%), although these numbers may be biased by the strong ESET user base in these regions. After removing those top two countries (in order to focus on the rest of the world), in Figure 4 it can be seen that the rest of the world was also hit, with Spain (5%) in third place followed by Mexico (5%) and South Africa (4%).

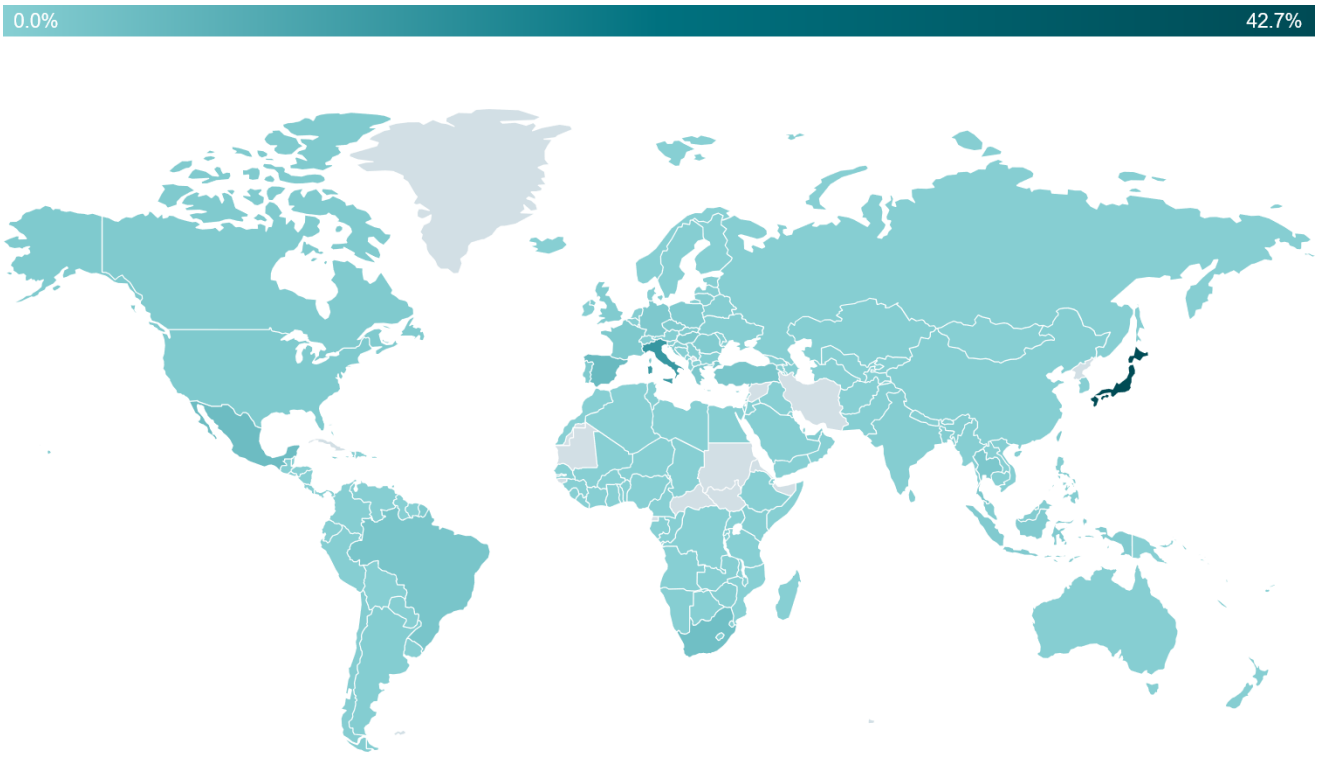



*Figure 3. Emotet detections Jan 2022 – Jun 2023*

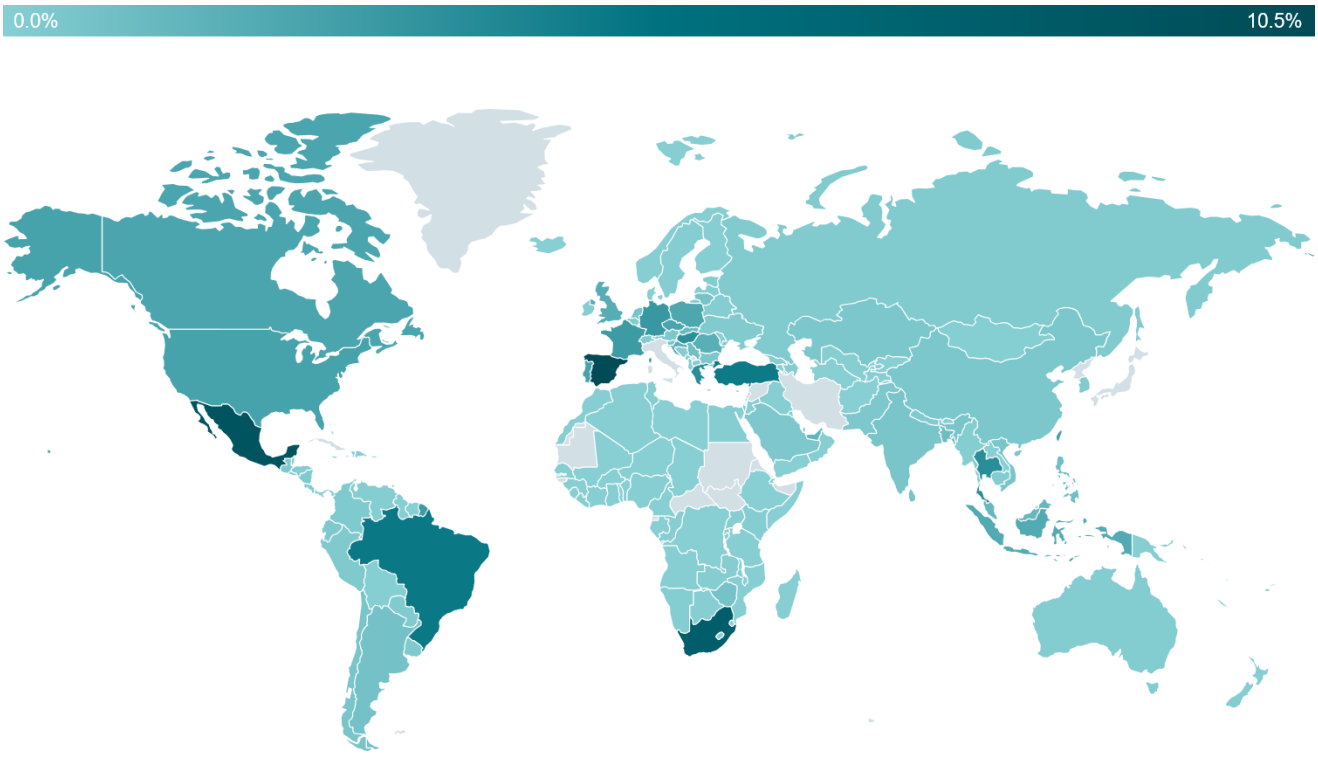



*Figure 4. Emotet detections Jan 2022 – Jun 2023 (JP and IT excluded)*

## Enhanced protection and obfuscations

After its reappearance, Emotet got multiple upgrades. The first notable feature is that the botnet switched its cryptographic scheme. Before the takedown, Emotet used RSA as their primary asymmetric scheme and after the reappearance, the botnet started to use Elliptic curve cryptography. Currently every Downloader module (also called Main module) comes with two embedded public keys. One is used for the Elliptic curve Diffie Hellman key exchange protocol and the other is used for a signature verification – Digital signature algorithm.

Apart from updating Emotet malware to 64-bit architecture, Mealybug has also implemented multiple new obfuscations to protect their modules. First notable obfuscation is control flow flattening which can significantly slow down analysis and locating interesting parts of code in Emotet's modules.

Mealybug also implemented and improved its implementation of many randomization techniques, of which the most notable are the randomization of order of structure members and the randomization of instructions that calculate constants (constants are masked).

One more update that is worth mentioning happened during the last quarter of 2022, when modules started using timer queues. With those, the main function of modules and the communication part of modules were set as a callback function, which is invoked by multiple threads and all of this is combined with the control flow flattening, where the state value that manages which block of code is to be invoked is shared among the threads. This obfuscation adds up to another obstacle in analysis and makes following of the execution flow even more difficult.

## New modules

To remain profitable and prevalent malware, Mealybug implemented multiple new modules, shown in yellow in Figure 5. Some of them were created as a defensive mechanism for the botnet, others for more efficient spreading of the malware, and last but not least, a module that steals information that can be used to steal the victim's money.

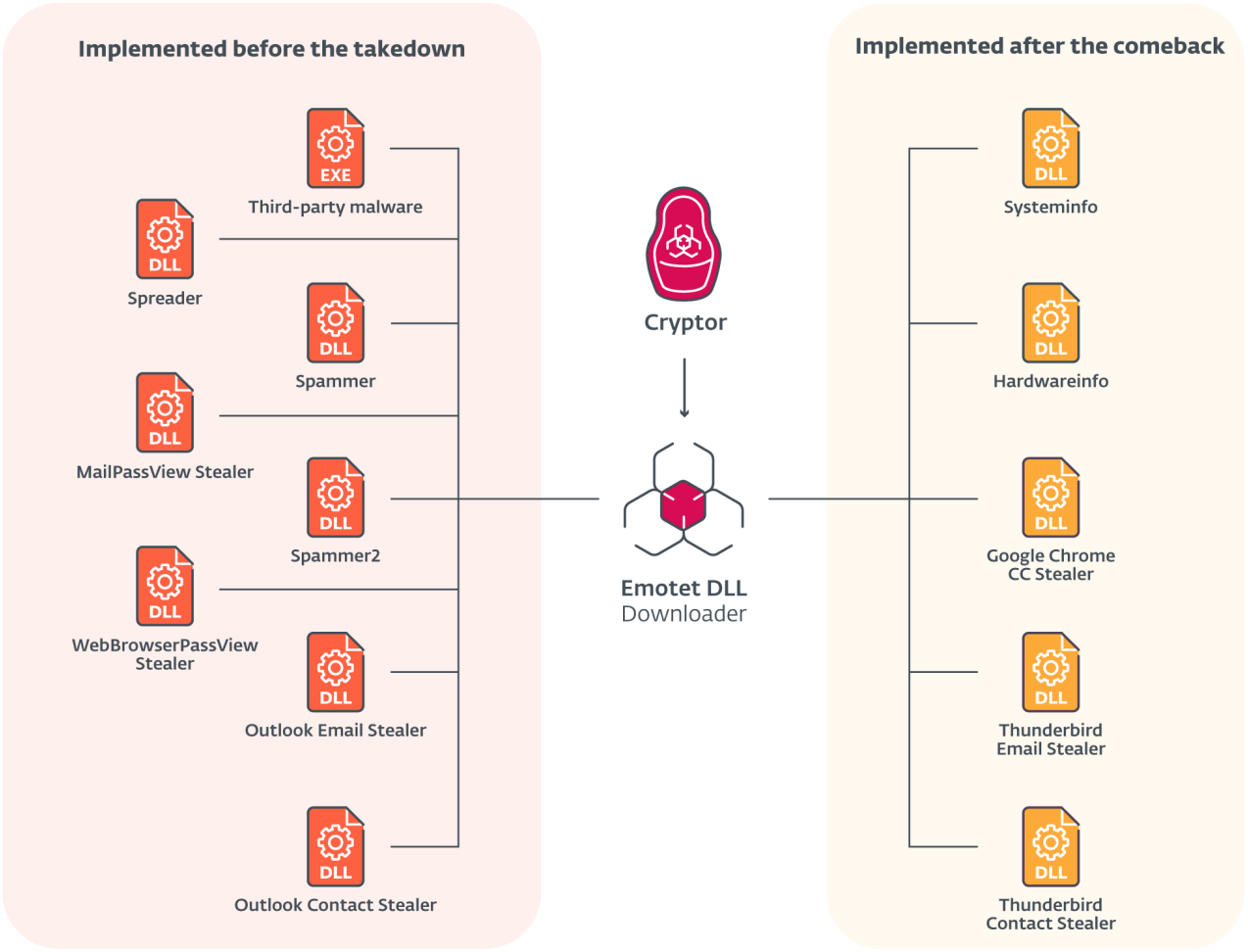



*Figure 5. Emotet's most frequently used modules. Red existed before the takedown; yellow appeared after the comeback*

### Thunderbird Email Stealer and Thunderbird Contact Stealer

Emotet is spread via spam emails and people often trust those emails, because Emotet successfully uses an email thread hijacking technique. Before the takedown, Emotet used modules we call Outlook Contact Stealer and Outlook Email Stealer, that were capable of stealing emails and contact information from Outlook. But because not everyone uses Outlook, after the takedown Emotet focused also on a free alternative email application – Thunderbird.

Emotet may deploy a Thunderbird Email Stealer module to the compromised computer, which (as the name suggests) is capable of stealing emails. The module searches through the Thunderbird files containing received messages (in MBOX format) and steals data from multiple fields including sender,

recipients, subject, date, and contents of the message.  All stolen information is then sent to a C&C server for further processing.

Together with Thunderbird Email Stealer, Emotet also deploys a Thunderbird Contact Stealer, which is capable of stealing contact information from Thunderbird. This module also searches through the Thunderbird files, this time looking for both received and sent messages. The difference is that this module just extracts information from the From:, To:, CC: and Cc: fields and creates an internal graph of who communicated with whom, where nodes are people, and there is an edge between two people if they communicated with each other. In the next step, the module orders the stolen contacts – starting with the most interconnected people – and sends this information to a C&C server.

All this effort is complemented by two additional modules (that existed already before the takedown) - the MailPassView Stealer module and the Spammer module. MailPassView Stealer abuses a legitimate NirSoft tool for password recovery and steals credentials from email applications. When stolen emails, credentials, and information about who is in contact with whom gets processed, Mealybug creates malicious emails that look like a reply to previously stolen conversations and sends those emails together with the stolen credentials to a Spammer module that uses those credentials to send malicious replies to previous email conversations via SMTP.

## Google Chrome Credit Card Stealer

As the name suggests, Google Chrome Credit Card Stealer steals information about credit cards stored in the Google Chrome browser. To achieve this, the module uses a statically linked SQLite3 library for accessing the Web Data database file usually located in %LOCALAPPDATA%\Google\Chrome\User Data\Default\Web Data. The module queries the table credit_cards for name_of_card, expiration_month, expiration_year, and card_number_encrypted, containing information about credit cards saved in the default Google Chrome profile. In the last step, the card_number_encrypted value is decrypted using the key stored in the %LOCALAPPDATA%\Google\Chrome\User Data\Local State file and all information is sent to a C&C server.

## Systeminfo and Hardwareinfo modules

Shortly after the return of Emotet, in November 2021 a new module we call Systeminfo appeared. This module collects information about a compromised system and sends it to the C&C server. Information collected consists of:

- Output of the systeminfo command
- Output of the ipconfig /all command
- Output of the nltest /dclist: command (removed in Oct. 2022)
- Process list
- Uptime (obtained via GetTickCount) in seconds (removed in Oct 2022)

In October 2022 Emotet's operators released another new module we call Hardwareinfo. Even though it doesn't steal exclusively information about the hardware of a compromised machine, it serves as a complementary source of information to the Systeminfo module. This module collects the following data from the compromised machine:

- Computer name

- Username
- OS version information, including major and minor version numbers
- Session ID
- CPU brand string
- Information about RAM size and usage

Both modules have one primary purpose – verify whether the communication comes from legitimately compromised victim or not. Emotet was, especially after its comeback, a really hot topic in the computer security industry and among researchers, so Mealybug went to great lengths to protect themselves from tracking and monitoring of their activities. Thanks to the information collected by these two modules that not only collect data, but also contain anti-tracking and anti-analysis tricks, Mealybug's capabilities to tell apart real victims from malware researchers' activities or sandboxes were significantly improved.

## What's next?

According to ESET research and telemetry, both Epochs of the botnet have been quiet since the beginning of the April 2023. Currently it remains unclear if this is yet another vacation time for the authors, if they struggle to find new effective infection vector, or if there is someone new operating the botnet.

Even though we cannot confirm the rumors that one or both Epochs of the botnet were sold to somebody in January 2023, we noticed an unusual activity on one of the Epochs. The newest update of the downloader module contained a new functionality, which logs the inner states of the module and tracks its execution to a file C:\JSmith\Loader (Figure 6, Figure 7). Because this file has to be existing to actually log something, this functionality looks like a debugging output for someone who doesn't completely understand what the module does and how it works. Furthermore, at that time the botnet was also widely spreading Spammer modules, which are considered to be more precious for Mealybug because historically they used these modules only on machines that were considered by them to be safe.

```
writeStateAndInfoToFile((WCHAR *)L"C:\\JSmith\\Loader", L"%u", STATE_CALLBACK);
```

*Figure 6. Logging of behavior of the downloader module*

```
commRes = communicate(PTR_COMM_INFO_STRUCT, &responseData, UNUSED_ARG(), UNUSED_ARG(), &dataToSend, 1);
writeStateAndInfoToFile(L"C:\\JSmith\\Loader", L"ChannelStatus: %u", commRes);
```

*Figure 7. Logging of behavior of the downloader module*

Whichever explanation of why the botnet is quiet now is true, Emotet has been known for its effectiveness and its operators made an effort to rebuild and maintain the botnet and even add some improvements, so keep track with our blog to see what the future will bring us.

> For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
> ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

## IoCs

### Files

| SHA-1 | Filename | ESET detection name | Description |
|---|---|---|---|
| D5FDE4A0DF9E416DE02AE51D07EFA8D7B99B11F2 | N/A | Win64/Emotet.AL | Emotet Systeminfo module. |
| 1B6CFE35EF42EB9C6E19BCBD5A3829458C856DBC | N/A | Win64/Emotet.AL | Emotet Hardwareinfo module. |
| D938849F4C9D7892CD1558C8EDA634DADFAD2F5A | N/A | Win64/Emotet.AO | Emotet Google Chrome Credit Card Stealer module. |
| 1DF4561C73BD35E30B31EEE62554DD7157AA26F2 | N/A | Win64/Emotet.AL | Emotet Thunderbird Email Stealer module. |
| 05EEB597B3A0F0C7A9E2E24867A797DF053AD860 | N/A | Win64/Emotet.AL | Emotet Thunderbird Contact Stealer module. |
| 0CEB10940CE40D1C26FC117BC2D599C491657AEB | N/A | Win64/Emotet.AQ | Emotet Downloader module, version with timer queue obfuscation. |
| 8852B81566E8331ED43AB3C5648F8D13012C8A3B | N/A | Win64/Emotet.AL | Emotet Downloader module, x64 version. |
| F2E79EC201160912AB48849A5B5558343000042E | N/A | Win64/Emotet.AQ | Emotet Downloader module, version with debug strings. |
| CECC5BBA6193D744837E689E68BC25C43EDA7235 | N/A | Win32/Emotet.DG | Emotet Downloader module, x86 version. |

## Network

| IP | Domain | Hosting provider | First seen | Details |
|---|---|---|---|---|

| IP | Domain | Hosting provider | First seen | Details |
|---|---|---|---|---|
| 1.234.2[.]232 | N/A | SK Broadband Co Ltd | N/A | N/A |
| 1.234.21[.]73 | N/A | SK Broadband Co Ltd | N/A | N/A |
| 5.9.116[.]246 | N/A | Hetzner Online GmbH | N/A | N/A |
| 5.135.159[.]50 | N/A | OVH SAS | N/A | N/A |
| 27.254.65[.]114 | N/A | CS LOXINFO Public Company Limited. | N/A | N/A |
| 37.44.244[.]177 | N/A | Hostinger International Limited | N/A | N/A |
| 37.59.209[.]141 | N/A | Abuse-C Role | N/A | N/A |
| 37.187.115[.]122 | N/A | OVH SAS | N/A | N/A |
| 45.71.195[.]104 | N/A | NET ALTERNATIVA PROVEDOR DE INTERNET LTDA - ME | N/A | N/A |
| 45.79.80[.]198 | N/A | Linode | N/A | N/A |
| 45.118.115[.]99 | N/A | Asep Bambang Gunawan | N/A | N/A |
| 45.176.232[.]124 | N/A | CABLE Y TELECOMUNICACIONES DE COLOMBIA S.A.S (CABLETELCO) | N/A | N/A |
| 45.235.8[.]30 | N/A | WIKINET TELECOMUNICAÇÕES | N/A | N/A |
| 46.55.222[.]11 | N/A | DCC | N/A | N/A |
| 51.91.76[.]89 | N/A | OVH SAS | N/A | N/A |
| 51.161.73[.]194 | N/A | OVH SAS | N/A | N/A |
| 51.254.140[.]238 | N/A | Abuse-C Role | N/A | N/A |
| 54.37.106[.]167 | N/A | OVH SAS | N/A | N/A |
| 54.37.228[.]122 | N/A | OVH SAS | N/A | N/A |
| 54.38.242[.]185 | N/A | OVH SAS | N/A | N/A |
| 59.148.253[.]194 | N/A | CTINETS HOSTMASTER | N/A | N/A |
| 61.7.231[.]226 | N/A | IP-network CAT Telecom | N/A | N/A |
| 61.7.231[.]229 | N/A | The Communication Authoity of Thailand, CAT | N/A | N/A |
| 62.171.178[.]147 | N/A | Contabo GmbH | N/A | N/A |
| 66.42.57[.]149 | N/A | The Constant Company, LLC | N/A | N/A |
| 66.228.32[.]31 | N/A | Linode | N/A | N/A |
| 68.183.93[.]250 | N/A | DigitalOcean, LLC | N/A | N/A |
| 72.15.201[.]15 | N/A | Flexential Colorado Corp. | N/A | N/A |

| IP | Domain | Hosting provider | First seen | Details |
|---|---|---|---|---|
| 78.46.73[.]125 | N/A | Hetzner Online GmbH - Contact Role, ORG-HOA1-RIPE | N/A | N/A |
| 78.47.204[.]80 | N/A | Hetzner Online GmbH | N/A | N/A |
| 79.137.35[.]198 | N/A | OVH SAS | N/A | N/A |
| 82.165.152[.]127 | N/A | 1&1 IONOS SE | N/A | N/A |
| 82.223.21[.]224 | N/A | IONOS SE | N/A | N/A |
| 85.214.67[.]203 | N/A | Strato AG | N/A | N/A |
| 87.106.97[.]83 | N/A | IONOS SE | N/A | N/A |
| 91.121.146[.]47 | N/A | OVH SAS | N/A | N/A |
| 91.207.28[.]33 | N/A | Optima Telecom Ltd. | N/A | N/A |
| 93.104.209[.]107 | N/A | MNET | N/A | N/A |
| 94.23.45[.]86 | N/A | OVH SAS | N/A | N/A |
| 95.217.221[.]146 | N/A | Hetzner Online GmbH | N/A | N/A |
| 101.50.0[.]91 | N/A | PT. Beon Intermedia | N/A | N/A |
| 103.41.204[.]169 | N/A | PT Infinys System Indonesia | N/A | N/A |
| 103.43.75[.]120 | N/A | Choopa LLC administrator | N/A | N/A |
| 103.63.109[.]9 | N/A | Nguyen Nhu Thanh | N/A | N/A |
| 103.70.28[.]102 | N/A | Nguyen Thi Oanh | N/A | N/A |
| 103.75.201[.]2 | N/A | IRT-CDNPLUSCOLTD-TH | N/A | N/A |
| 103.132.242[.]26 | N/A | Ishan's Network | N/A | N/A |
| 104.131.62[.]48 | N/A | DigitalOcean, LLC | N/A | N/A |
| 104.168.155[.]143 | N/A | Hostwinds LLC. | N/A | N/A |
| 104.248.155[.]133 | N/A | DigitalOcean, LLC | N/A | N/A |
| 107.170.39[.]149 | N/A | DigitalOcean, LLC | N/A | N/A |
| 110.232.117[.]186 | N/A | RackCorp | N/A | N/A |
| 115.68.227[.]76 | N/A | SMILESERV | N/A | N/A |
| 116.124.128[.]206 | N/A | IRT-KRNIC-KR | N/A | N/A |
| 116.125.120[.]88 | N/A | IRT-KRNIC-KR | N/A | N/A |
| 118.98.72[.]86 | N/A | PT Telkom Indonesia APNIC Resources Management | N/A | N/A |

| IP | Domain | Hosting provider | First seen | Details |
|---|---|---|---|---|
| 119.59.103[.]152 | N/A | 453 Ladplacout Jorakhaebua | N/A | N/A |
| 119.193.124[.]41 | N/A | IP Manager | N/A | N/A |
| 128.199.24[.]148 | N/A | DigitalOcean, LLC | N/A | N/A |
| 128.199.93[.]156 | N/A | DigitalOcean, LLC | N/A | N/A |
| 128.199.192[.]135 | N/A | DigitalOcean, LLC | N/A | N/A |
| 129.232.188[.]93 | N/A | Xneelo (Pty) Ltd | N/A | N/A |
| 131.100.24[.]231 | N/A | EVEO S.A. | N/A | N/A |
| 134.122.66[.]193 | N/A | DigitalOcean, LLC | N/A | N/A |
| 139.59.56[.]73 | N/A | DigitalOcean, LLC | N/A | N/A |
| 139.59.126[.]41 | N/A | Digital Ocean Inc administrator | N/A | N/A |
| 139.196.72[.]155 | N/A | Hangzhou Alibaba Advertising Co.,Ltd. | N/A | N/A |
| 142.93.76[.]76 | N/A | DigitalOcean, LLC | N/A | N/A |
| 146.59.151[.]250 | N/A | OVH SAS | N/A | N/A |
| 146.59.226[.]45 | N/A | OVH SAS | N/A | N/A |
| 147.139.166[.]154 | N/A | Alibaba (US) Technology Co., Ltd. | N/A | N/A |
| 149.56.131[.]28 | N/A | OVH SAS | N/A | N/A |
| 150.95.66[.]124 | N/A | GMO Internet Inc administrator | N/A | N/A |
| 151.106.112[.]196 | N/A | Hostinger International Limited | N/A | N/A |
| 153.92.5[.]27 | N/A | Hostinger International Limited | N/A | N/A |
| 153.126.146[.]25 | N/A | IRT-JPNIC-JP | N/A | N/A |
| 159.65.3[.]147 | N/A | DigitalOcean, LLC | N/A | N/A |
| 159.65.88[.]10 | N/A | DigitalOcean, LLC | N/A | N/A |
| 159.65.140[.]115 | N/A | DigitalOcean, LLC | N/A | N/A |
| 159.69.237[.]188 | N/A | Hetzner Online GmbH - Contact Role, ORG-HOA1-RIPE | N/A | N/A |
| 159.89.202[.]34 | N/A | DigitalOcean, LLC | N/A | N/A |
| 160.16.142[.]56 | N/A | IRT-JPNIC-JP | N/A | N/A |
| 162.243.103[.]246 | N/A | DigitalOcean, LLC | N/A | N/A |
| 163.44.196[.]120 | N/A | GMO-Z com NetDesign Holdings Co., Ltd. | N/A | N/A |

| IP | Domain | Hosting provider | First seen | Details |
|---|---|---|---|---|
| 164.68.99[.]3 | N/A | Contabo GmbH | N/A | N/A |
| 164.90.222[.]65 | N/A | DigitalOcean, LLC | N/A | N/A |
| 165.22.230[.]183 | N/A | DigitalOcean, LLC | N/A | N/A |
| 165.22.246[.]219 | N/A | DigitalOcean, LLC | N/A | N/A |
| 165.227.153[.]100 | N/A | DigitalOcean, LLC | N/A | N/A |
| 165.227.166[.]238 | N/A | DigitalOcean, LLC | N/A | N/A |
| 165.227.211[.]222 | N/A | DigitalOcean, LLC | N/A | N/A |
| 167.172.199[.]165 | N/A | DigitalOcean, LLC | N/A | N/A |
| 167.172.248[.]70 | N/A | DigitalOcean, LLC | N/A | N/A |
| 167.172.253[.]162 | N/A | DigitalOcean, LLC | N/A | N/A |
| 168.197.250[.]14 | N/A | Omar Anselmo Ripoll (TDC NET) | N/A | N/A |
| 169.57.156[.]166 | N/A | SoftLayer | N/A | N/A |
| 172.104.251[.]154 | N/A | Akamai Connected Cloud | N/A | N/A |
| 172.105.226[.]75 | N/A | Akamai Connected Cloud | N/A | N/A |
| 173.212.193[.]249 | N/A | Contabo GmbH | N/A | N/A |
| 182.162.143[.]56 | N/A | IRT-KRNIC-KR | N/A | N/A |
| 183.111.227[.]137 | N/A | Korea Telecom | N/A | N/A |
| 185.4.135[.]165 | N/A | ENARTIA Single Member S.A. | N/A | N/A |
| 185.148.168[.]15 | N/A | Abuse-C Role | N/A | N/A |
| 185.148.168[.]220 | N/A | Abuse-C Role | N/A | N/A |
| 185.168.130[.]138 | N/A | GigaCloud NOC | N/A | N/A |
| 185.184.25[.]78 | N/A | MUV Bilisim ve Telekomunikasyon Hizmetleri Ltd. Sti. | N/A | N/A |
| 185.244.166[.]137 | N/A | Jan Philipp Waldecker trading as LUMASERV Systems | N/A | N/A |
| 186.194.240[.]217 | N/A | SEMPRE TELECOMUNICACOES LTDA | N/A | N/A |
| 187.63.160[.]88 | N/A | BITCOM PROVEDOR DE SERVICOS DE INTERNET LTDA | N/A | N/A |
| 188.44.20[.]25 | N/A | Company for communications services A1 Makedonija DOOEL Skopje | N/A | N/A |

| IP | Domain | Hosting provider | First seen | Details |
|---|---|---|---|---|
| 190.90.233[.]66 | N/A | INTERNEXA Brasil Operadora de Telecomunicações S.A | N/A | N/A |
| 191.252.103[.]16 | N/A | Locaweb Serviços de Internet S/A | N/A | N/A |
| 194.9.172[.]107 | N/A | Abuse-C Role | N/A | N/A |
| 195.77.239[.]39 | N/A | TELEFONICA DE ESPANA S.A.U. | N/A | N/A |
| 195.154.146[.]35 | N/A | Scaleway Abuse, ORG-ONLI1-RIPE | N/A | N/A |
| 196.218.30[.]83 | N/A | TE Data Contact Role | N/A | N/A |
| 197.242.150[.]244 | N/A | Afrihost (Pty) Ltd | N/A | N/A |
| 198.199.65[.]189 | N/A | DigitalOcean, LLC | N/A | N/A |
| 198.199.98[.]78 | N/A | DigitalOcean, LLC | N/A | N/A |
| 201.94.166[.]162 | N/A | Claro NXT Telecomunicacoes Ltda | N/A | N/A |
| 202.129.205[.]3 | N/A | NIPA TECHNOLOGY CO., LTD | N/A | N/A |
| 203.114.109[.]124 | N/A | IRT-TOT-TH | N/A | N/A |
| 203.153.216[.]46 | N/A | Iswadi Iswadi | N/A | N/A |
| 206.189.28[.]199 | N/A | DigitalOcean, LLC | N/A | N/A |
| 207.148.81[.]119 | N/A | The Constant Company, LLC | N/A | N/A |
| 207.180.241[.]186 | N/A | Contabo GmbH | N/A | N/A |
| 209.97.163[.]214 | N/A | DigitalOcean, LLC | N/A | N/A |
| 209.126.98[.]206 | N/A | GoDaddy.com, LLC | N/A | N/A |
| 210.57.209[.]142 | N/A | Andri Tamtrijanto | N/A | N/A |
| 212.24.98[.]99 | N/A | Interneto vizija | N/A | N/A |
| 213.239.212[.]5 | N/A | Hetzner Online GmbH | N/A | N/A |
| 213.241.20[.]155 | N/A | Netia Telekom S.A. Contact Role | N/A | N/A |
| 217.182.143[.]207 | N/A | OVH SAS | N/A | N/A |

## MITRE ATT&CK techniques

This table was built using version 12 of the MITRE ATT&CK enterprise techniques.

| Tactic | ID | Name | Description |
|---|---|---|---|

| Tactic | ID | Name | Description |
|---|---|---|---|
| Reconnaissance | T1592.001 | Gather Victim Host Information: Hardware | Emotet gathers information about hardware of the compromised machine, such as CPU brand string. |
| T1592.004 | Gather Victim Host Information: Client Configurations | Emotet gathers information about system configuration such as the ipconfig /all and systeminfo commands. | |
| T1592.002 | Gather Victim Host Information: Software | Emotet exfiltrates a list of running processes. | |
| T1589.001 | Gather Victim Identity Information: Credentials | Emotet deploys modules that are able to steal credentials from browsers and email applications. | |
| T1589.002 | Gather Victim Identity Information: Email Addresses | Emotet deploys modules that can extract email addresses from email applications. | |
| Resource Development | T1586.002 | Compromise Accounts: Email Accounts | Emotet compromises email accounts and uses them for spreading malspam emails. |
| T1584.005 | Compromise Infrastructure: Botnet | Emotet compromises numerous third-party systems to form a botnet. | |
| T1587.001 | Develop Capabilities: Malware | Emotet consists of multiple unique malware modules and components. | |
| T1588.002 | Obtain Capabilities: Tool | Emotet uses NirSoft tools to steal credentials from infected machines. | |
| Initial Access | T1566 | Phishing | Emotet sends phishing emails with malicious attachments. |
| T1566.001 | Phishing: Spearphishing Attachment | Emotet sends spearphishing emails with malicious attachments. | |
| Execution | T1059.005 | Command and Scripting Interpreter: Visual Basic | Emotet has been seen using Microsoft Word documents containing malicious VBA macros. |

| Tactic | ID | Name | Description |
|---|---|---|---|
| | T1204.002 | User Execution: Malicious File | Emotet has been relying on users opening malicious email attachments and executing embedded scripts. |
| Defense Evasion | T1140 | Deobfuscate/Decode Files or Information | Emotet modules use encrypted strings and masked checksums of API function names. |
| | T1027.002 | Obfuscated Files or Information: Software Packing | Emotet uses custom packers to protect their payloads. |
| | T1027.007 | Obfuscated Files or Information: Dynamic API Resolution | Emotet resolves API calls at runtime. |
| Credential Access | T1555.003 | Credentials from Password Stores: Credentials from Web Browsers | Emotet acquires credentials saved in web browsers by abusing NirSoft's WebBrowserPassView application. |
| | T1555 | Credentials from Password Stores | Emotet is capable of stealing passwords from email applications by abusing NirSoft's MailPassView application. |
| Collection | T1114.001 | Email Collection: Local Email Collection | Emotet steals emails from Outlook and Thunderbird applications. |
| Command and Control | T1071.003 | Application Layer Protocol: Mail Protocols | Emotet can send malicious emails via SMTP. |
| | T1573.002 | Encrypted Channel: Asymmetric Cryptography | Emotet is using ECDH keys to encrypt C&C traffic. |
| | T1573.001 | Encrypted Channel: Symmetric Cryptography | Emotet is using AES to encrypt C&C traffic. |
| | T1571 | Non-Standard Port | Emotet is known to communicate on nonstandard ports such as 7080. |

## Let us keep you up to date

Sign up for our newsletters