|  |
| --- |
| [Nom de la société] |
| EMOTET |
| Cyber Threat Intelligence | Malware Analysis |

|  |
| --- |
| Abdallah Chbaro  09/04/2023 |

# About

Emotet is a malware strain and a cybercrime operation believed to be based in Ukraine.[1] The malware, also known as Heodo, was first detected in 2014 and deemed one of the most prevalent threats of the decade.

First versions of the Emotet malware functioned as a banking trojan aimed at stealing banking credentials from infected hosts. Throughout 2016 and 2017, Emotet operators, sometimes known as Mealybug, updated the trojan and reconfigured it to work primarily as a "loader," a type of malware that gains access to a system, and then allows its operators to download additional payloads.[5] Second-stage payloads can be any type of executable code, from Emotet's own modules to malware developed by other cybercrime gangs.

# Description

Emotet is a type of malware that is designed to steal sensitive information from computer systems. It was first discovered in 2014 and has since become one of the most dangerous and widespread forms of malware in the world. Emotet is primarily distributed through phishing emails, which are designed to look like legitimate messages from reputable sources such as banks, financial institutions, or government agencies.

When a user clicks on a link or opens an attachment in one of these emails, the Emotet malware is installed on their computer. Once installed, Emotet can steal sensitive information such as usernames and passwords, banking and financial information, and other personal data. It can also download additional malware onto the infected computer, turning it into a part of a larger botnet used for various criminal activities.

Emotet is a highly sophisticated and adaptable malware that is constantly evolving to evade detection by security software. It has been used in a variety of attacks, including ransomware attacks, credential theft, and even targeted attacks against specific organizations or individuals. Due to its sophistication and the difficulty of removing it once installed, Emotet is considered one of the most dangerous forms of malware in existence.

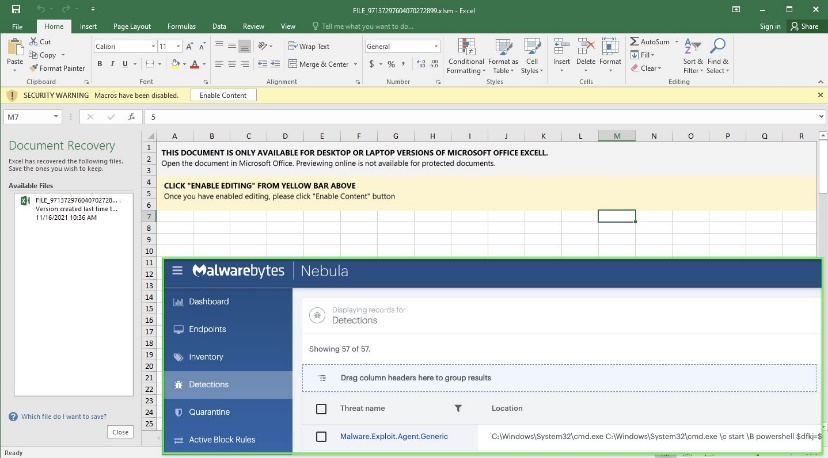
# Deepen Description

Emotet is a Trojan that is primarily spread through spam emails (malspam). The infection may arrive either via malicious script, macro-enabled document files, or malicious link. Emotet emails may contain familiar branding designed to look like a legitimate email. Emotet may try to persuade users to click the malicious files by using tempting language about “Your Invoice,” “Payment Details,” or possibly an upcoming shipment from well-known parcel companies.

Emotet has gone through a few iterations. Early versions arrived as a malicious JavaScript file. Later versions evolved to use macro-enabled documents to retrieve the virus payload from command and control (C&C) servers run by the attackers.

Emotet uses a number of tricks to try and prevent detection and analysis. Notably, Emotet knows if it’s running inside a virtual machine (VM) and will lay dormant if it detects a sandbox environment, which is a tool cybersecurity researchers use to observe malware within a safe, controlled space.

Emotet also uses C&C servers to receive updates. This works in the same way as the operating system updates on your PC and can happen seamlessly and without any outward signs. This allows the attackers to install updated versions of the software, install additional malware such as other banking Trojans, or to act as a dumping ground for stolen information such as financial credentials, usernames and passwords, and email addresses.



Capabilities

* Information Theft: Yes
* Rootkit Capability: Yes
* File Infection: Yes
* Propagation: Yes
* Download Routine: Yes

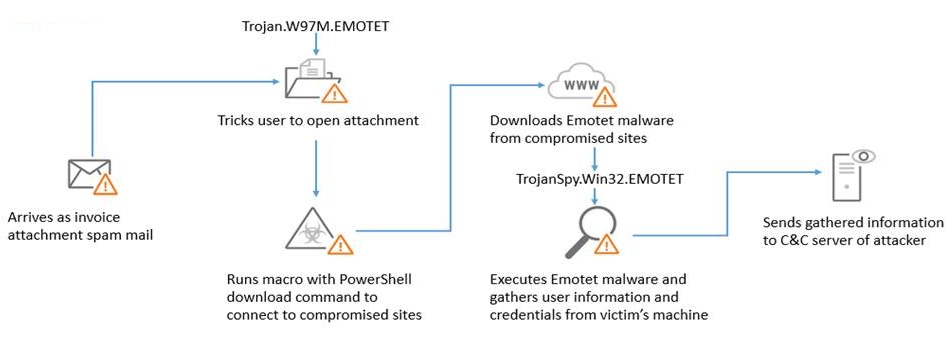
# How does Emotet Spread?

The primary distribution method for Emotet is through malspam. Emotet ransacks your contacts list and sends itself to your friends, family, coworkers and clients. Since these emails are coming from your hijacked email account, the emails look less like spam and the recipients, feeling safe, are more inclined to click bad URLs and download infected files.

If a connected network is present, Emotet spreads using a list of common passwords, guessing its way onto other connected systems in a brute-force ­attack. If the password to the all-important human resources server is simply “password” then it’s likely Emotet will find its way there.

Researchers initially thought Emotet also spread using the EternalBlue/DoublePulsar vulnerabilities, which were responsible for the WannaCry and NotPetya attacks. We know now that this isn't the case. What led researchers to this conclusion was the fact that TrickBot, a Trojan often spread by Emotet, makes use of the EternalBlue exploit to spread itself across a given network. It was TrickBot, not Emotet, taking advantage of the EternalBlue/DoublePulsar vulnerabilities.

# Infection Chain



# Attack Phases – Operation Mode

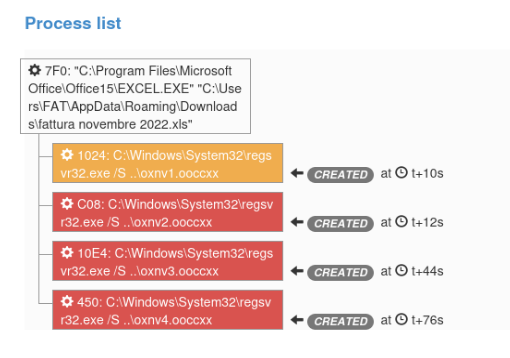
As expected, Emotet is currently making a noisy comeback by heavily spamming again since this morning, in multiple languages (including English, German, Italian, French, etc.).

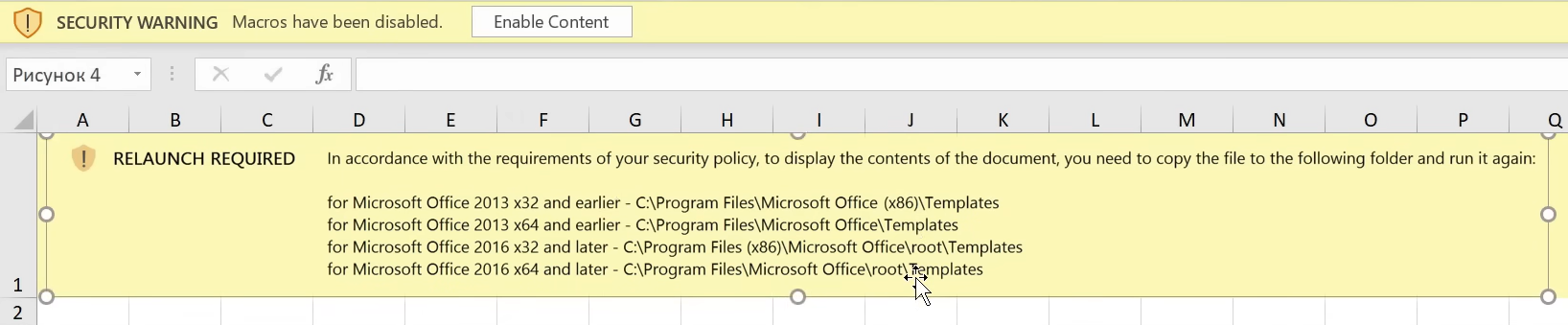
Most of TTPs used haven't changed, with Excel documents either directly attached or embedded in password-protected ZIP archives within unsolicited emails, disguised under various names as shown in samples received on VirusTotal (that you will find in Appendices). If the embedded macros are activated, a call to regsvr32.exe is performed to drop the DLL.

The successful "thread hijacking" tactic is indeed used again in that spamming spree, in both Emotet botnets (Epoch 4 and 5). But so far, only one same malware sample seems to be dropped, as no hashbusting -a technique that randomly adds characters to data in order to change the data's hash sum- seem to be used. This variant is well detected by antivirus engines, as VirusTotal shows. Furthermore, only a handful of malicious URLs (still hosted on compromised domains) were yet identified.

Une image contenant texte

Description générée automatiquement





|  |  |  |  |
| --- | --- | --- | --- |
| Behavior | Tactic | Technique | Detection |
| Emotet Excel documents either directly attached or embedded in password-protected ZIP archives  Also using “thread hijacking” tactic | Initial Access **[TA0001]** | Phishing: Spearphishing Attachment  **[T1566.001]** | **SIEM ; SEG (file meta data):**  (Author = Gydar OR Heading Pairs : “Листы, 6, Макросы Excel 4.0, 1”) AND MIME Type = “application/vnd.ms-excel”  AND subject = “RE:\*” |
| Emotet Excel documents either directly attached or embedded in password-protected ZIP archives | Execution **[TA0002]**  Defense Evasion **[TA0005]** | Command and Scripting Interpreter: Visual Basic **[T1071.002]**  User Execution: Malicious File **[T1204.002]**  System Binary Proxy Execution: Regsvr32 **[T1218.010]** | **EDR** :  Parent Process = “EXCEL.exe” AND Process = “regsvr32.exe” |
| Emotet Excel documents either directly attached or embedded in password-protected ZIP archives | Execution **[TA0002]**  Defense Evasion **[TA0005]** | Command and Scripting Interpreter: Visual Basic **[T1071.002]**  User Execution: Malicious File **[T1204.002]**  System Binary Proxy Execution: Regsvr32 **[T1218.010]** | **EDR :**  Process = “regsvr32.exe” AND (CommandLine = “\* ..\\*») |
| Emotet Excel download and drop a DLL from compromised infrastructure | Resource Development **[TA0042]**  Command and Control **[TA0011]** | Compromise Infrastructure: Web Services **[T1584.006]**  Application Layer Protocol: File Transfer **Protocols [T1071.002]** | **SIEM (Proxy logs) :**  user-agent=\*; .NET\* AND mime-type=application/x-msdownload AND URL=\*/wp-\* AND URL=\*/ |
| Emotet DLL perform initial discovery via systeminfo and ipconfig. | Discovery **[TA0002]** | System Information Discovery **[T1082]** | **EDR :**  Parent Process = “regsvr32.exe” AND Process IN (“systeminfo.exe”, “ipconfig.exe”) |
| Emotet perform persistence via autorun registry key | Persistence **[TA0003]** | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder **[T1547.001]** | **EDR:**  Key path: « HKEY\_CURRENT\_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN“ AND Key\_name=“\*.dll’ AND registry data = “\*\AppData\Local\\*” |
| Emotet copy the malicious DLL into %LOCALAPPDATA%. | Defense Evasion **[TA0005]** | System Binary Proxy Execution: Regsvr32 **[T1218.010]** | **EDR:**  file name = “\*.dll” AND file path = “\*\AppData\Local\\*” AND action type = “create” AND process= “\*regsvr32.exe\*” |

# IOCs

|  |  |
| --- | --- |
| URL/IP/MD5 | Date Added |
| https://149.56.131.28:8080/rrdbsqzgxbfbh/epaypyumcgk/yyhmufdwvlfb/zqilzqdgtxgv | 2023-03-29 16:09:28 |
| https://159.65.88.10:8080/rrdbsqzgxbfbh/epaypyumcgk/yyhmufdwvlfb/zqilzqdgtxgv/ | 2023-03-29 16:09:24 |
| https://159.89.202.34/rrdbsqzgxbfbh/epaypyumcgk/yyhmufdwvlfb/zqilzqdgtxgv/ | 2023-03-29 16:09:20 |
| https://167.172.199.165:8080/rrdbsqzgxbfbh/epaypyumcgk/yyhmufdwvlfb/zqilzqdgtxgv/ | 2023-03-29 16:09:15 |
| https://187.63.160.88:80/rrdbsqzgxbfbh/epaypyumcgk/yyhmufdwvlfb/zqilzqdgtxgv/ | 2023-03-29 16:09:11 |
| https://91.121.146.47:8080/rrdbsqzgxbfbh/epaypyumcgk/yyhmufdwvlfb/zqilzqdgtxgv/ | 2023-03-29 16:09:06 |
| https://149.56.131.28:8080/cqigynpvgknevqx/vqdidzpifwvde/bdlgputiektde/fgogmpcei/ | 2023-03-29 16:04:17 |
| https://159.65.88.10:8080/cqigynpvgknevqx/vqdidzpifwvde/bdlgputiektde/fgogmpcei/ | 2023-03-29 16:04:13 |
| https://159.89.202.34/cqigynpvgknevqx/vqdidzpifwvde/bdlgputiektde/fgogmpcei/ | 2023-03-29 16:04:08 |
| https://167.172.199.165:8080/cqigynpvgknevqx/vqdidzpifwvde/bdlgputiektde/fgogmpcei/ | 2023-03-29 16:04:04 |