În ultimele luni, o serie de entități publice și private din România au fost puternic afectate de valuri succesive de atacuri cu malware de tip EMOTET, care au generat numeroase probleme. Acest tip de atacuri a cunoscut o creștere consistentă în această săptămână, vizând o plajă largă de ținte din aceeași categorie.

**Ce este EMOTET?**

EMOTET este un malware-ul de tip bancar, care infectează computerele care folosesc sistemul de operare Microsoft Windows, prin intermediul link-urilor sau a atașamentelor malspam infectate (e.g. PDF, DOC, etc.). EMOTET este un troian cunoscut, descoperit în urmă cu aproximativ 6 ani, mai întâi în Europa și mai apoi în SUA.

EMOTET se activează pe computerul unui utilizator, prin intermediul link-urilor sau a atașamentelor malspam din e-mail-uri, cu intenția de a fura date financiare. Principalele informații vizate inițial erau cele de ordin financiar, dar ulterior EMOTET a evoluat în complexitate și a dobândit capacitatea de a efectua alte atacuri în interiorul unui dispozitiv. Ținta primește mesaje care de regulă par să provină de la adrese legitime, , instituții sau chiar persoane fizice. Mai mult, în anumite cazuri mesajele pot proveni direct de la o sursă reală, dacă aceasta a fost deja infectată cu EMOTET.

În acest moment există 3 modalități prin care vă puteți infecta PC-ul/rețeaua cu EMOTET, în toate cazurile pornindu-se de la un mail tip spam:

1. Mail de tip spam, cu un atașament ce conține macro-uri care descarcă malware.
2. Mail de tip spam cu atașament ce conține macro-uri, dar fișierul malițios este inclus într-o arhivă cu parolă (parola este comunicată în textul mail-ului, pentru ca victima să îl poată dezarhiva).
3. Mail de tip spam care are inclus în text un link. Apăsând pe acel link, victima ajunge să își infecteze dispozitivul cu malware.

**Recomandări pentru evitarea atacurilor cu EMOTET**

**În ultimele luni, echipa CERT-RO a furnizat o**[**serie de alerte**](https://www.facebook.com/CERT.RO/posts/3654235284640832)**pe canalele oficiale de social media despre cum funcționează acest tip de atac și cum ne putem proteja. Se recomandă, în primul rând,  verificarea adresei reale de mail de pe care primim aceste mesaje**. Acest lucru se poate face prin verificarea sursei (header).

Principalii pași care trebuie avuți în vedere ar fi următorii:

1. **Sporirea vigilenței,**care este principalul atu pe care un utilizator obișnuit îl are oricând la dispoziție. Fiți atenți atunci când verificați e-mail-urile primite, în special cele care conțin atașamente! EMOTET este încă activ, se propagă prin intermediul e-mail-ului și vizează deopotrivă persoane fizice, instituții publice sau companii private.

În cazul în care aveți suspiciuni legate de veridicitatea informației din mail,**verificați autenticitatea informațiilor oferite** de presupusul expeditor direct cu acesta, utilizând alt canal de comunicare (preferabil telefonul).

1. Înainte de a face o acțiune care ar putea dăuna, **scanați cu o soluție de securitate** instalată pe dispozitiv, sau cu una disponibilă gratis online (ex: [Virus Total](https://www.virustotal.com/gui/home/url)) **link-urile sau atașamentele** **suspecte** din căsuța dvs. de mail. Nu uitați să aplicați la timp update-urile pentru aceste soluții!

Scanarea cu antivirus nu este suficientă însă. EMOTET nu este ușor de identificat și interceptat, deoarece **eludează de multe ori soluțiile antivirus** convenționale. Este un virus polimorf, codul se schimbă ușor pentru a evita detectarea de către scanerele de malware bazate pe semnături. De asemenea, EMOTET detectează când rulează pe o mașină virtuală. De îndată ce este înregistrat un mediu sandbox, programul intră în modul stand-by și nu ia nicio acțiune dăunătoare în acel moment.

1. Utilizatorilor li se recomandă să implementeze **filtre la gateway-ul de e-mail** pentru a înlătura e-mailurile cu indicatori cunoscuți de spam sau malware și pentru a bloca adresele IP suspecte din firewall.

**E-mailurile suspecte trebuie raportate departamentului IT** pentru izolare și investigare. Verificați periodic regulile contului de e-mail, care pot fi setate pentru redirecționarea automată a tuturor mesajelor, ceea ce ar putea duce la o scurgere de date, dacă există o infecție.

1. Pentru a vă proteja eficient împotriva EMOTET, trebuie să vă concentrați în principal pe poarta principală de acces a malware-ului: comunicarea prin e-mail. Deoarece **EMOTET se ascunde adesea în fișierele Microsoft Office și are nevoie de macrocomenzi**pentru a putea instala malware-ul dorit, este logic să nu le permiteți. Dacă totuși nu vă puteți desfășura activitatea fără macrocomenzi, este posibil să le permiteți numai celor semnate.
2. Orice **actualizare de securitate** implementată trebuie instalată imediat pentru sistemele de operare, programele antivirus, browserele web, clienții de e-mail și programele de tip Office.
3. Efectuați în mod regulat **backup al datelor**, în special a celor esențiale. Infecția cu EMOTET poate duce, de asemenea, la un ransomware, astfel că este vital să mențineți copii de siguranță ale datelor pentru a permite recuperarea acestora, în cazul unei infecții cu EMOTET. Deoarece ransomware-ul infectează în mod obișnuit dispozitivele de stocare conectate, asigurați-vă că backupurile dvs. sunt stocate offline sau sunt deconectate fizic, atunci când nu sunt utilizate!
4. **Accesul la rețeaua companiei ar trebui monitorizat continuu**, de către cei responsabili din Departamentele IT, deoarece astfel se poate determina în timp util dacă a apărut o infecție cu EMOTET.
5. **Dezactivați serviciile inutile**. EMOTET profită adesea de vulnerabilitățile găsite în serviciile care rulează în background, pentru a se răspândi pe alte computere din rețea. Remote Desktop Protocol (RDP), tehnologia care ne permite lucrul de la distanță. este un astfel de exemplu. Utilizatorilor li se recomandă să dezactiveze astfel de servicii dacă nu sunt necesare, pentru a împiedica malware-ul să le exploateze și să se propage în rețea
6. **Instalați o soluție de control al aplicațiilor.** Utilizatorii pot lua în considerare instalarea unui astfel de software care oferă listă albă de aplicații și/sau directoare. Astfel, se permite rularea exclusiv a programelor aprobate, în timp ce se restricționează altele. Este o practică bună de securitate pentru a proteja un sistem informatic.
7. **Asigurați-vă routerele!** EMOTET poate exploata rețele Wi-Fi nesigure, pentru a răspândi malware-ul, astfel că este extrem de important să vă protejați rețelele. Utilizatorii și administratorii de sistem sunt sfătuiți să facă acest lucru, asigurându-vă că modificați parolele implicite și că utilizați o parolă puternică pentru routerele dvs.
8. **Se recomandă verficarea adresei de mail de unde vin mesajele.**

**Cum procedăm pentru a verifica dacă suntem infectați cu EMOTET?**

Pentru a verifica dacă dispozitivul dvs. a fost deja infectat cu EMOTET, puteți folosi instrumentul de detectare și dezinfectare este disponibil pe GitHub: <https://github.com/JPCERTCC/EmoCheck>

Un scurt instructaj video explicit despre cum se poate utiliza această soluție, este disponibil pe canalul nostru de Youtube: [https://youtu.be/CytgMVjCduQ](https://youtu.be/CytgMVjCduQ%20)

Un alt instrument online, care se axează pe scanarea adreselor de e-mail sau a domeniilor, este disponibil aici: [https://www.haveibeenemotet.com](https://www.haveibeenemotet.com/), iar tutorialul de utilizare, produs de către echipa CERT-RO poate fi vizionat aici: [https://www.facebook.com/CERT.RO/videos/330312408067561](https://www.facebook.com/CERT.RO/videos/330312408067561%20)