# Alerta CERT-RO: Mai multe institutii publice si private din România, atacate de malware-ul de tip bancar Emotet

**O serie de entitati publice si private din România au fost puternic afectate de valuri succesive de atacuri cu malware-ul de tip bancar Emotet, în ultimele luni, informeaza Centrul National de Raspuns la Incidente de Securitate Cibernetica (CERT-RO), într-o alerta publicata, joi, pe propria pagina de internet.**

Emotet este un malware de tip bancar, ce infecteaza computerele care folosesc sistemul de operare Microsoft Windows, prin intermediul link-urilor sau al atasamentelor malspam infectate (ex.: PDF, DOC etc.). Malware-ul este un troian cunoscut, descoperit în urma cu aproximativ sase ani, mai întâi în Europa si mai apoi în SUA.

Conform expertilor CERT-RO, virusul se activeaza pe computerul unui utilizator cu intentia de a fura date financiare.

"CERT-RO a observat în ultimele luni o persistenta, iar în ultimul timp o crestere a volumului atacurilor care vizeaza infectarea cu malware-ul de tip bancar Emotet. Atacurile nu au o tinta clara prestabilita si vizeaza atât utilizatori obisnuiti, cât si institutii publice sau organizatii private. Ce face Emotet? Vorbim despre un troian care încearca sa extraga detalii financiare de pe dispozitivele infectate. Este important de stiut fapul ca acest tip de atac poate fi evitat daca se respecta o igiena de securitate minimala. Pentru ca atacul se propaga prin e-mail, utilizatorii trebuie sa fie vigilenti, sa verifice în sursa mesajului adresa exacta de unde provine, iar daca înca au suspiciuni sa verifice informatia cu expeditorul. Totodata, utilizatorii trebuie sa evite accesarea link-urilor si atasamentelor din mail-urile suspecte, înainte de a le scana cu o solutie de securitate. În acelasi timp, subliniem importanta adoptarii unei rutine de securitate care cuprinde actualizarea frecventa a sistemului de operare si a software-ului folosit pe dispozitive, efectuarea unor back-up-uri (copii de siguranta) a fisierelor si configurarea corecta a instrumentelor cu care ne conectam la internet (ex: router). În cazul în care au fost infectati, sa se adreseze CERT-RO la numarul de urgenta 1911 sau adresa de e-mail alerts@cert.ro", a declarat, pentru AGERPRES, Mihai Rotariu, purtator de cuvânt al CERT-RO.

În acest moment, exista trei modalitati prin care se poate infecta PC-ul/reteaua cu acest malware de tip bancar, în toate cazurile pornindu-se de la un mail tip spam: e-mail de tip spam, cu un atasament ce contine macro-uri care descarca malware; e-mail de tip spam cu atasament ce contine macro-uri, dar fisierul malitios este inclus într-o arhiva cu parola (parola este comunicata în textul mail-ului, pentru ca victima sa îl poata dezarhiva); e-mail de tip spam care are inclus în text un link, care odata accesat va ajunge sa infecteze dispozitivul cu malware.

Pe acest fond, CERT-RO are si câteva recomandari pentru evitarea atacurilor cu Emotet.

"Fiti atenti atunci când verificati e-mail-urile primite, în special cele care contin atasamente! Emotet este înca activ, se propaga prin intermediul e-mail-ului si vizeaza deopotriva persoane fizice, institutii publice sau companii private. În cazul în care aveti suspiciuni legate de veridicitatea informatiei din mail, verificati autenticitatea informatiilor oferite de presupusul expeditor direct cu acesta, utilizând alt canal de comunicare (preferabil telefonul). Înainte de a face o actiune care ar putea dauna, scanati cu o solutie de securitate instalata pe dispozitiv sau cu una disponibila gratis online (ex: Virus Total) link-urile sau atasamentele suspecte din casuta dvs. de mail. Nu uitati sa aplicati la timp update-urile pentru aceste solutii", subliniaza expertii.

O alta informatie importanta este aceea ca scanarea cu antivirus nu este suficienta pentru a preveni infectate terminalului cu Emotet. Malware-ul nu este usor de identificat si interceptat, deoarece eludeaza de multe ori solutiile antivirus conventionale.

"Este un virus polimorf, codul se schimba usor pentru a evita detectarea de catre scanerele de malware bazate pe semnaturi. De asemenea, Emotet detecteaza când ruleaza pe o masina virtuala. Deîndata ce este înregistrat un mediu sandbox, programul intra în modul stand-by si nu ia nicio actiune daunatoare în acel moment. Utilizatorilor li se recomanda sa implementeze filtre la gateway-ul de e-mail pentru a înlatura e-mail-urile cu indicatori cunoscuti de spam sau malware si pentru a bloca adresele IP suspecte din firewall. E-mailurile suspecte trebuie raportate departamentului IT pentru izolare si investigare. Verificati periodic regulile contului de e-mail, care pot fi setate pentru redirectionarea automata a tuturor mesajelor, ceea ce ar putea duce la o scurgere de date, daca exista o infectie", se arata în informarea CERT-RO.

În acelasi timp, pentru a se proteja eficient împotriva Emotet, utilizatorilor le este recomandat sa se concentreze în principal pe poarta principala de acces a malware-ului si anume comunicarea prin e-mail. Totodata, orice actualizare de securitate implementata trebuie instalata imediat pentru sistemele de operare, programele antivirus, browserele web, clientii de e-mail si programele de tip Office.

La fel, este imperios necesara operatiunea de backup regulat al datelor, în special a celor esentiale, iar accesul la reteaua companiei ar trebui monitorizat continuu de catre cei responsabili din Departamentele IT, deoarece astfel se poate determina în timp util daca a aparut o infectie cu Emotet.

În plus, se recomanda dezactivarea serviciilor inutile, inclusiv a Remote Desktop Protocol (RDP), tehnologia care ne permite lucrul de la distanta, precum si asigurarea routerelor, întrucât Emotet poate exploata retele Wi-Fi nesigure pentru a raspândi malware-ul.

O verificare pentru a vedea daca dispozitivul a fost deja infectat cu Emotet se poate face cu ajutorul instrumentului de detectare si dezinfectare disponibil pe GitHub: https://github.com/JPCERTCC/EmoCheck.

Un alt instrument online, care se axeaza pe scanarea adreselor de e-mail sau a domeniilor, este disponibil aici: https://www.haveibeenemotet.com, iar tutorialul de utilizare, produs de catre echipa CERT-RO poate fi vizionat la adresa https://www.facebook.com/CERT.RO/videos/330312408067561.