Bitdefender

CEC Bank

ROMANIA SRI SERVICIUL ROMAN DE INFORMATII Patria a priori

RAPORT

THREAT INTELLIGENCE

AMENINȚĂRILE CIBERNETICE
LA ADRESA SECTORULUI
FINANCIAR-BANCAR ÎN ANUL 2020

THREAT INTELLIGENCE

REPORT

2020 CYBER THREATS
TO THE FINANCIAL -
BANKING SECTOR

DE CE ACEST MATERIAL

Raportul se înscrie în seria demersurilor Serviciului Român de Informații/ Centrului Național CYBERINT, Bitdefender și CEC Bank de dezvoltare a parteneriatului public-privat în domeniul securității cibernetice. Astfel, a fost resimțită nevoia unei abordări integrate a amenințării cibernetice asupra sectorului financiar-bancar, pe fondul caracterului flexibil al acesteia, având implicații atât asupra utilizatorilor individuali și companiilor din domeniul securității cibernetice, cât și asupra securității naționale.

Prin analiza perspectivelor expuse, raportat la anul 2020, ne dorim să aducem plus valoare în planul cunoașterii și înțelegerii amenințărilor cibernetice cu care domeniul financiar-bancar se confruntă. Doar prin asigurarea unui nivel superior de înțelegere a acestora, putem crea planuri solide de răspuns și adopta măsuri corespunzătoare pentru a preveni și contracara activitățile derulate de atacatori în spațiul cibernetic.
Astfel, în cadrul activităților subsumate criminalității cibernetice, datele bancare reprezintă cele mai atrăgătoare ținte ale atacatorilor, având în vedere perspectivele pe care obținerea lor le oferă: acces la conturi bancare, modalitate de șantaj al victimelor, comercializare pe forumuri de criminalitate cibernetică.

Unicitatea acestui demers rezidă în prezentarea comprehensivă a trei viziuni complementare asupra amenințărilor cibernetice: viziunea unui serviciu de informații raportat la securitatea națională, cea a unei companii private de securitate cibernetică și cea a unei instituții financiar-bancare. Fiecare dintre acestea contribuie, prin propria experiență și perspectivă, la cunoașterea și investigarea unui fenomen extins, de interes general, care afectează un număr mare de entități, fie ele private, publice sau utilizatori individuali, ceea ce generează implicații inclusiv asupra securității naționale.

CUM A FOST GÂNDIT

Deoarece spațiul cibernetic excede granițele teritoriale, iar securitatea cibernetică a unui sector de activitate nu poate fi abordată independent de situația de la nivel internațional, prima secțiune a raportului prezintă cele mai relevante riscuri și incidente/atacuri cibernetice asupra sectorului financiar-bancar

ARGUMENT FOR THE PRESENT REPORT

The present report is entailed in the series of intercessions conducted by the Romanian Intelligence Service (SRI)/ The CYBERINT National Centre, together with Bitdefender and CEC Bank, for the purpose of developing the public-private partnership in the area of Cyber Security. Thus, the need for an integrated approach towards the cyber threat regarding the financial and banking compartments emerged, fuelled by its flexibility and the impact it has on both individual users and enterprises, as well as on the national security.

After analyzing the present perspectives and by comparison to 2020, it is our desire to add value in the direction of a better knowledge and comprehension of the cyber threats for the financial and banking compartments. The development of stable response action plans and the application of appropriate measures for preventing and countering the activities of cyber attackers are only possible by ensuring a high degree of understanding.
Thus, banking information represents the most attractive target for the attackers, among the activities falling into the category of cyber criminal activities, taking into account the perspectives provided once such information is obtained: banking accounts access, a good means for blackmailing the victims, trading them on cyber crime forums.

The uniqueness of this endeavor resides in the comprehensive presentation of three complementary visions on cyber threats: the vision of an intelligence service in the context of national security, the one of a private company providing cyber security services and that of a financial institution. Each and every one of them contributes, through their own experience and expertise, to the cognition and inquiry of an extended phenomenon, which presents general interest, has an impact on a great number of entities, whether they are private, public, or individual users, which generates a series of implications on national security.

HOW THE REPORT WAS STRUCTURED

Taking into account the fact that cyber space exceeds territorial boundaries and that the cyber security of one area

înregistrate în anul 2020, atât la nivel mondial, cât și național.
A doua secțiune abordează tipurile de amenințări cibernetice cu care se confruntă instituțiile din domeniul financiar-bancar, acestea fiind împărțite pe două coordonate: amenințări la adresa instituțiilor, respectiv la adresa clienților acestora.

Raportul cuprinde inclusiv un studiu de caz asupra atacurilor cibernetice derulate cu troianul Emotet, impactul acestora fiind prezentat din pespectiva triplă a părților implicate.

PEISAJUL AMENINȚĂRILOR CIBERNETICE LA ADRESA SECTORULUI FINANCIAR-BANCAR LA NIVEL INTERNAȚIONAL/ NAȚIONAL

Amenințarea cibernetică este una foarte dinamică și cu impact puternic asupra tuturor celorlalte segmente de activitate, având, de cele mai multe ori, un caracter disruptiv la adresa unor procese și servicii, inclusiv cele esențiale. Atacatorii cibernetici dau dovadă de flexibilitate în desfășurarea activităților în spațiul cibernetic, adaptând modul de operare și utilizând o plajă largă de instrumente pentru a asigura succesul și anonimitatea operațiunilor.

Având în vedere toate aceste elemente, atribuirea atacurilor cibernetice către entitățile care le-au realizat devine un obiectiv din ce în ce mai dificil de îndeplinit. Granița dintre tipurile de actori regăsiți în spațiul cibernetic este una fină, aspect accentuat de fenomenul cybercrime-as-a-service care facilitează schimbul de cunoaștere și de tool-uri între atacatori.

Una dintre cele mai prolifice categorii de actori, care profită de toate aceste aspecte, este reprezentată de grupările de criminalitate cibernetică. În dinamismul ce caracterizează spațiul și amenințările cibernetice există totuși și câteva constante, precum interesul acestor grupări pentru a obține beneficii materiale și apetența acestora pentru sectorul financiar-bancar.
Instituțiile financiar-bancare reprezintă ținte atrăgătoare pentru entitățile cybercrime atât din perspectivă proprie, cât și prin prisma clienților acestora, o posibilă infecție oferind atacatorilor acces la sume semnificative de bani.
Mai mult, pe lângă furtul datelor bancare și manipularea tranzacțiilor,

of activity cannot be tackled out of the international context, the first section of this report presents the most relevant cyber risks and incidents/ attacks on the financial and banking compartments of 2020, both globally and nationally.
The second section focuses on the existent types of cyber threats that the financial institutions are facing, and which are divided into two categories: threats targeting the institutions, and threats for their respective clients.

The report also contains a case study based on the cyber attacks carried out through the Emotet Trojan, while their impact is presented from the perspectives of the three involved parties.

THE NATIONAL/ INTERNATIONAL CONTEXT OF CYBER THREATS IN THE FINANCIAL - BANKING SECTOR

The cyber threat is a very dynamic element, with a great impact on all the other areas of activity, as it most often than not has a disruptive character towards a certain number of services and processes, including the essential ones. The cyber attackers have proven to be flexible in developing their activities in cyber space, adapting their modus operandi and using a wide range of instruments for the purpose of ensuring the success and anonymity of their operations.

Taking into account all these elements, assigning the cyber attacks to the actual entities that have carried them out becomes a goal that is ever more difficult to achieve. The border between the types of actors in the cyber space is a very thin one, a flaw that is punctuated by the cybercrime-as-a-service phenomenon, which facilitates the exchange of know-how and tools between the attackers.

One of the most prolific actor categories, which take advantage of all the aforementioned aspects, is represented by the cyber crime groups. Despite the dynamic character of the cyber space and threats, there are some invariable elements, such as these groups interest to obtain material gains, as well as their taste for the financial and banking compartments.
The financial - banking institutions represent attractive targets for cybercrime entities, both on their own, as well as through their customers, a possible infection giving attackers access to significant amounts of money.

prin atacuri asupra instituțiilor bancare, actorii cibernetici urmăresc exfiltrarea de date personale ale clienților, pe care le pot folosi ulterior, pentru șantaj sau comercializarea pe forumuri de cybercrime. În acest fel, un atac asupra infrastructurii unei instituții bancare poate determina pierderi financiare la nivelul întregului flux monetar gestionat, precum și prejudicii de imagine.

În anul 2020, activitatea actorilor cibernetici cu motivație financiară s-a intensificat, amenințarea fiind amplificată în contextul eforturilor de gestionare a pandemiei de COVID-19. Grupările cybercrime au considerat contextul social ca fiind o oportunitate în asigurarea succesului activităților derulate, diversificând și adaptând TTP-urile și instrumentele utilizate în scopul exploatării contextului pandemic.

De asemenea, aceștia au exploatat atât nevoia populației de informare cu privire la evoluția pandemiei, cât și aplicarea modelului „work from home", ca parte a măsurilor de distanțare socială.

În acest context, peisajul amenințărilor cybercrime la adresa sistemului financiar-bancar a fost marcat de campanii cu frecvență și amploare ridicate, printre cele mai întâlnite aplicații malware utilizate prin exploatarea contextului pandemic în 2020 fiind Agent Tesla, Cerberus, Emotet, Qbot, Trickbot, Lokibot.

TIPURILE DE AMENINȚĂRI CIBERNETICE CU CARE SE CONFRUNTĂ INSTITUȚIILE DIN SECTORUL FINANCIAR-BANCAR

1. AMENINȚĂRI LA ADRESA INSTITUȚIILOR BANCARE

În ultimul an a existat nevoia, fără precedent, de adaptare a activității angajaților din sectorul financiar-bancar, în special prin extinderea semnificativă a forței de lucru mobile. De asemenea, au fost accelerate procesele de adoptare de noi tehnologii necesare facilitării accesului clienților la servicii financiare, de automatizare accelerată a unor procese de business, precum și de digitalizare a fluxurilor de documente necesare înrolării/ accesului la servicii.

Pe acest fond, suprafața de atac și riscurile de securitate cibernetică la adresa instituțiilor care activează în domeniul financiar-bancar au crescut, securitatea cibernetică devenind o prioritate investițională pentru majoritatea jucătorilor de pe piața de profil.

Moreover, in addition to the theft of banking data and the manipulation of transactions, by means of such attacks on banking institutions, cyber actors seek to extract personal data of customers, which they can later use for blackmail or marketing on cybercrime forums. Thus, an attack on the infrastructure of a banking institution can lead to financial losses in the entire managed cash flow, as well as image damage.

In 2020, the activity of financially motivated cyber actors intensified, the threat being amplified in the context of efforts made in order to manage the COVID-19 pandemic. Cybercrime groups saw the social context as an opportunity to ensure the success of their activities, diversifying and adapting the TTPs and tools used to exploit the pandemic context.

They also exploited both the population's need for information on the evolution of the pandemic and the use of the „work from home" model, as part of social distancing measures.

In this context, the landscape of cybercrime threats to the financial - banking system was marked by campaigns high in frequency and magnitude, among the most common malware applications used while exploiting the pandemic context in 2020 being Agent Tesla, Cerberus, Emotet, Qbot, Trickbot, Lokibot.

TYPES OF CYBER THREATS FACED BY INSTITUTIONS IN THE FINANCIAL - BANKING SECTOR

1. THREATS TO BANKING INSTITUTIONS

Over the last year, there has been an unprecedented need to adapt the activity of employees in the financial - banking compartment, especially through the significant expansion of the mobile workforce. Also, the processes of adopting new technologies necessary to facilitate customers' access to financial services were accelerated, as well as the automation of business processes and the digitization of document flows necessary for enrollment/ access to services.

Upon this background, the attack area and cyber security risks against institutions operating in the financial - banking field have increased, cyber security becoming an investment priority for most players in the market.

Pe parcursul anului 2020, la nivelul CEC Bank a fost înregistrată o dublare cantitativă a numărului de incidente de securitate cibernetică detectate și gestionate prin intermediul platformelor tehnologice de care banca dispune. Creșterea în volum a incidentelor identificate nu este cauzată exclusiv de contextul pandemic, care a creat un mediu propice evoluției acestui fenomen, ci și extinderii și modernizării arhitecturii de securitate cibernetică.

Din perspectiva complexității incidentelor de securitate cibernetică, nu au fost înregistrate modificări semnificative față de perioada anterioară. Tehnicile, tacticile și procedurile utilizate de actorii cibernetici nu au înregistrat o evoluție relevantă, care să genereze riscuri majore la adresa infrastructurilor IT&C utilizate. Cu toate acestea, au fost observate eforturi de adaptare ale actorilor cibernetici la contextul pandemic și de exploatare a acestuia.

Majoritatea incidentelor de securitate cibernetică la adresa infrastructurii CEC Bank la nivelul anului 2020 au exploatat vulnerabilități cunoscute, iar principalul vector de atac a fost reprezentat de email-uri de tip phishing adresate angajaților.
O evoluție relevantă identificată de către Bitdefender, CEC Bank și Centrul Național CYBERINT, pe lângă creșterea semnificativă a volumului campaniilor de phishing care au ca obiective distribuirea de malware pe sistemele informatice ale angajaților instituțiilor financiar-bancare și furtul credențialelor de acces (nume de utlizator, parole), a fost adaptarea tehnicilor de inginerie socială utilizate de atacatori la specificul pandemiei COVID-19. A fost vizat, în special, interesul public în raport cu evoluția epidemiei și adaptarea conținutului mesajelor phishing în raport cu acestea (evoluții ale cazurilor de infectare, tratamente „minune", date despre vaccinuri, oferte de materiale de protecție la prețuri avantajoase, informații despre condițiile de călătorie/carantină, măsuri dispuse de autorități, etc.).

De asemenea, tehnicile de transmitere a unui număr mare de email-uri de tip phishing au evoluat, prin adaptarea mecanismelor de transmitere, astfel încât să permită ocolirea unora dintre filtrele antiphishing utilizate și să asigure șanse mai mari de deschidere a mesajelor de către angajați, utilizarea unor nume de domenii actualizate (necunoscute în primele ore ale atacului de firmele furnizoare de date tehnice). De asemenea, în cadrul mesajelor s-a remarcat utilizarea corectă a limbii române, precum și nume de expeditori, persoane fizice si firme autohtone.

Over 2020, at the level of CEC Bank, the number of cyber security incidents detected and managed through the technological platforms available to the bank has doubled. The increase in volume of the identified incidents is not caused exclusively by the pandemic context, which created an environment conducive to the evolution of this phenomenon, but also to the expansion and modernization of cyber security architecture.

With respect to the complexity of cyber security incidents, no significant changes were recorded compared to the previous period. The techniques, tactics and procedures used by cyber actors have not evolved in a relevant way, so as to generate major risks to the IT&C infrastructures used. However, efforts have been made by cyber actors to adapt to the pandemic context and exploit it.

Most of the cyber security incidents against the CEC Bank infrastructure at the level of 2020 exploited known vulnerabilities, and the main attack vector was represented by phishing emails addressed to employees.
A relevant evolution identified by Bitdefender, CEC Bank and Cyberint National Center, in addition to the significant increase in the volume of phishing campaigns aimed at distributing malware on the computer systems of employees of financial - banking institutions and theft of access credentials (username, passwords), was the adaption of the social engineering techniques used by the attackers to the specifics of the COVID-19 pandemic. The attackers targeted mainly the public interest in relation to the evolution of the epidemic and the adaptation of content of phishing messages in relation to them (evolutions of cases of infection, „miracle" treatments, data on vaccines, offers of protective materials at convenient prices, information on the conditions of travel/ quarantine, measures taken by the authorities, etc.)

At the same time, the techniques of sending phishing e-mails have evolved, by adapting the transmission mechanisms so as to bypass some of the anti-phishing filters and ensure greater chances of success in getting employees to open messages, as well as the use of updated domain names (unknown in the first hours of the attack to the companies providing technical data). Also, in the messages, the correct use of the Romanian language was noticed, as well as the names of senders, individuals and local companies.

2. AMENINȚĂRI LA ADRESA CLIENȚILOR INSTITUȚIILOR BANCARE

Contextul pandemic a determinat actorii cibernetici să își adapteze și diversifice tehnicile de inginerie socială utilizate pentru a asigura succesul campaniilor derulate asupra clienților băncilor. Obiectivul principal al acestora este de a determina țintele să transmită date cu caracter personal, fie ca răspuns la unul sau mai multe email-uri, fie prin accesarea unor atașamente sau link-uri din corpul mesajelor.

Majoritatea clienților instituțiilor bancare sunt interesați de gestionarea cu ușurință a bunurilor financiare deținute și a operațiunilor derulate, și mai puțin de securizarea acestora, considerând, adesea, că aspectele privind securitatea sunt exclusiv responsabilitatea instituțiilor bancare. Din acest considerent, clienții devin ținte predilecte ale actorilor cybercrime, care își pot îndeplini scopul cu eforturi reduse.

În perioada martie 2020 – aprilie 2021, campaniile de phishing care au vizat clienții instituțiilor bancare au avut forme diverse. Mesajele de tip phishing primite de clienți ai instituțiilor bancare sau recepționate la nivelul acestora nu au avut un nivel de complexitate ridicat. Acestea au utilizat sigla instituției și au creat aparența unei comunicări legitime din partea băncii. În majoritatea situațiilor, clienții au avut capacitatea de a identifica mesajul ca fiind suspect, fie pe fondul unor greșeli gramaticale sau de exprimare prezente în textul mesajului, fie identificând adresa de email a expeditorului și constatând că aceasta nu este legitimă.

Pe parcursul anului 2020, a fost identificată o serie de campanii cibernetice care au targetat inclusiv clienți ai instituțiilor financiar-bancare, cele mai întâlnite utilizând aplicațiile:

■ **Cerberus Android Banker** – a vizat utilizatori individuali prin distribuirea unui mesaj tip text redactat în limba română, care conține sintagma „Detalii secrete! (COVID-19)”. Troianul oferă acces ilicit la date din aplicațiile bancare, având totodată capabilități de extragere de date despre aplicațiile de mesagerie și poștă electronică instalate pe dispozitivul vizat (ex. Telegram, WhatsApp, Gmail), precum și de captarea șirurilor de caractere tastate și de exfiltrare a datelor astfel obținute.

■ **Qbot** – a vizat utilizatori individuali prin transmiterea unor emailuri de tip spear-phishing, pentru a obține acces la date financiare. Mesajele aveau fie un link în conținut, fie un atașament cu conținut malware.

2. THREATS TO CUSTOMERS OF BANKING INSTITUTIONS

The pandemic context has led cyber actors to adapt and diversify the social engineering techniques used to ensure the success of their campaigns on bank customers. Their main objective is to convince the targets to disclose personal data, either in response to one or more e-mails, or by accessing attachments or links located in the body of the messages.

Most customers of banking institutions are more interested in the easy management of their financial assets and operations, and less in securing them, often deeming the banks as the sole responsible for security issues. For this reason, clients become favorite targets of cybercrime actors, who can achieve their goal with little effort.

Between March 2020 and April 2021, the phishing campaigns that targeted the clients of the banking institutions were of great variety. Phishing messages received by customers of banking institutions or by banks did not have a high level of complexity. They used the institution's logo and created the appearance of a legitimate communication from the bank. In most cases, customers succeeded in identifying the message as suspicious, either on the basis of grammar or lexical errors present in the text of the message, or by identifying the sender's e-mail address and finding that it was not legitimate.

During 2020, a series of cyber campaigns was identified, targeting customers of financial-banking institutions, the most common of them using the following apps:

■ **Cerberus Android Banker** – targeted individual users by distributing a text message written in Romanian, which contained the phrase “Secret details! (COVID-19)”. The Trojan provides illegal access to data from banking applications, while also having the ability to extract data about messaging and e-mail apps installed on the target device (for example Telegram, WhatsApp, Gmail), as well as capturing the strings of typed letters and exfiltrating data thus obtained.

■ **Qbot** – targeted individual users by sending spear-phishing emails to gain access to financial data. The messages had either a link in the content or an attachment with malware content. The attachment is a zip file that contains a Microsoft Word document that runs a macro through which the Trojan is downloaded and thus is spreading the infection.

Atașamentul este un fișier de tip zip, care conține un document Microsoft Word ce rulează un macro prin care se descarcă troianul și se realizează infecția.

Strategia adoptată la nivelul CEC Bank cu privire la atacurile cibernetice și comunicarea permanentă cu clienții au permis ca, în perioada martie 2020 – aprilie 2021, să nu fie înregistrat niciun caz de furt de date personale aparținând clienților băncii.

STUDIU DE CAZ - EMOTET

În anul 2020, Emotet a fost una dintre cele mai prolifice aplicații de tip malware, atât pe fondul numărului mare de victime, cât și al utilizării sale în campanii cu alte aplicații, respectiv al capabilităților tehnice avansate și strategiei de lucru implementate de dezvoltatori.
Emotet este o aplicație malware de tip troian care infectează sistemele informatice pe care rulează sistemul de operare Microsoft Windows. Acesta este distribuit prin campanii de phishing/ spearphishing, email-urile utilizate conținând link-uri sau atașamente cu conținut malware.

Emotet targetează utilizatori individuali, companii publice și private, organizații financiar-bancare și instituții de stat, având ca scop furtul de date personale și financiare.

În principal, infecțiile cu Emotet au fost realizate prin descărcarea unor fișiere Microsoft Office Word sau Excel atașate email-urilor, acestea conținând elemente macro care descarcă aplicația malware.
Emotet este o aplicație modulară, ceea ce a permis actualizarea permanentă și dezvoltarea capabilităților deținute. Malware-ul deține funcționalități de brute force asupra parolelor, utilizând un dicționar de parole încorporat, precum și credențiale exfiltrate anterior.

Emotet conține metode de protecție în ceea ce privește eludarea soluțiilor antivirus și a mecanismelor de securitate, precum și pentru îngreunarea procesului de analiză malware: componente polimorfice, zone de cod criptate, criptarea locației serverului de comandă și control. Pe lângă capabilitățile tehnice avansate ale Emotet, ceea ce a determinat succesul campaniilor derulate a fost utilizarea unor adrese de email ce par a fi legitime, personificând indivizi sau instituții, precum și a unor adrese de email legitime, compromise anterior. Astfel, după compromiterea unui sistem informatic, Emotet exfiltrează lista de contacte a email-urilor prezente la nivelul acestuia,

The strategy adopted by CEC Bank regarding the cyber attacks and the permanent communication with the clients resulted, between March 2020 and April 2021, in zero cases of theft of personal data belonging to the bank's clients.

CASE STUDY - EMOTET

In 2020, Emotet was one of the most prolific malware applications, both due to the large number of victims and its use in campaigns along with other applications, respectively the advanced technical capabilities and work strategy implemented by the developers.
Emotet is a Trojan-type malware application that infects computer systems running the Microsoft Windows operating system. It is distributed through phishing/ spear-phishing campaigns, the emails used containing links or attachments with malware content.

Emotet targets individual users, public and private companies, financial organizations and state-owned institutions, for the purpose of stealing personal and financial data.

Most of the Emotet infections were achieved by downloading Microsoft Office Word or Excel files attached to e-mails, which contained macro elements that downloaded the malware.
Emotet is a modular application, which enables its permanent updating and development of capabilities. The malware has password brute force functionality, using a built-in password dictionary, as well as previously exfiltrated credentials.

Emotet contains protection mechanisms whose role is to help the malware evade detection by antivirus solutions and security systems and to hinder the malware analysis process: polymorphic components, encrypted code areas, encryption of the location of the command and control server. In addition to Emotet's advanced technical capabilities, the success of the campaigns was also attributable to the use of seemingly legitimate e-mail addresses, apparently originating from familiar individuals or institutions, as well as legitimate e-mail addresses, which had been previously compromised. In other words, after compromising a computer system, Emotet exfiltrates the contact list of e-mail addresses and sends the application via e-mail to all such contacts.

Emotet is also used as a loader for the distribution of applications such as

distribuind aplicația, prin email, către toate acestea.

De asemenea, Emotet este utilizat și cu funcție de loader, inclusiv pentru distribuirea aplicațiilor Trickbot și Ryuk. Scenariul utilizat de actorii cibernetici în derularea de atacuri cibernetice cu un nivel de complexitate ridicat presupune utilizarea capabilităților Emotet pentru realizarea infecției inițiale, ulterior fiind livrat malware-ul Trickbot, care exfiltrează date de interes despre victimă. Ca parte finală a atacului, este descărcat și executat ransomware-ul Ryuk, care criptează datele utilizatorului, fiind solicitată plata unei răscumpărări pentru recăpătarea accesului la acestea.

Perspectiva SRI/CNC

În toamna anului 2020, prin intermediul Sistemului Național de Protecție a Infrastructurilor IT&C de Interes Național împotriva Amenințărilor provenite din Spațiul Cibernetic (Țițeica), Centrul Național CYBERINT a identificat o intensificare a alertelor asociate Emotet. Perioada de creștere semnificativă a alertelor, septembrie – noiembrie 2020, coincide cu momentul în care atât utilizatorii individuali, cât și instituții publice și private au fost ținte ale unor valuri succesive de campanii de phishing prin care era distribuit Emotet.

Astfel, în luna octombrie 2020, Centrul Național CYBERINT a analizat, în medie, 4800 de alerte malware la nivelul Sistemului Țițeica, de 4.6 ori mai mult față de luna precedentă.

Trickbot and Ryuk. The scenario used by cyber actors to carry out highly complex cyber attacks entails the use of Emotet's capabilities to achieve the initial infection and the subsequent delivery of the Trickbot malware, which exfiltrates data of interest about the victim. As a final part of the attack, the Ryuk ransomware is downloaded and executed, encrypting the user's data and requesting a ransom to regain access to such data.

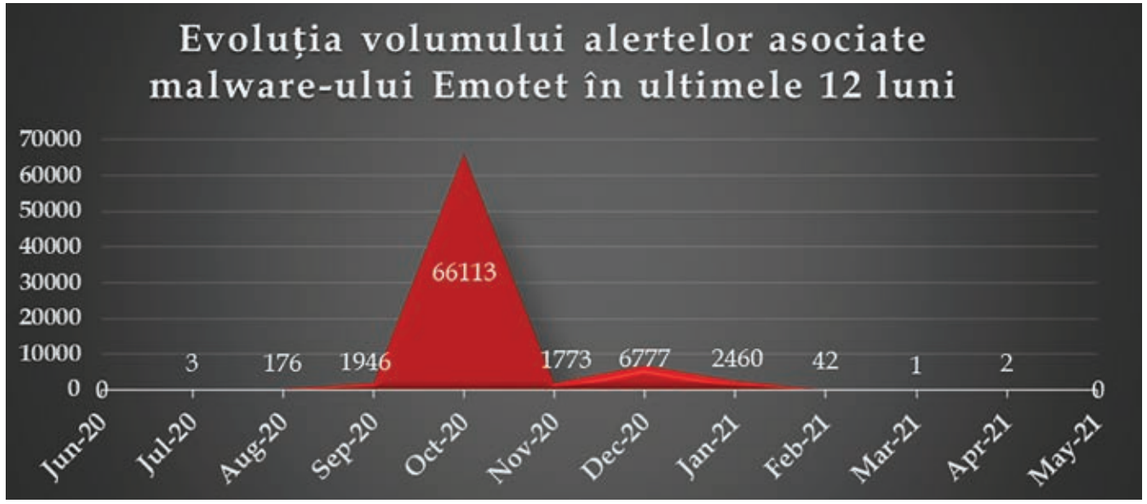
The outlook of SRI/CNC

In the fall of 2020, through the National System for the Protection of IT&C Infrastructures of National Interest against Cyber Threats (Țițeica), the National CYBERINT Center identified an increased number of alerts associated with Emotet.

The period when the number of alerts grew significantly, namely September-November 2020, is consistent with the time frame when individual users, as well as public and private institutions, were targeted by successive phishing campaigns by means of which the Emotet malware was distributed.

In October 2020, the National CYBERINT Center analyzed about 4800 malware alerts by means of the Țițeica System, a number which is 4.6 higher than the previous month.


1234
567
89
10
HACKING DETECTED
01010101110000
01010101

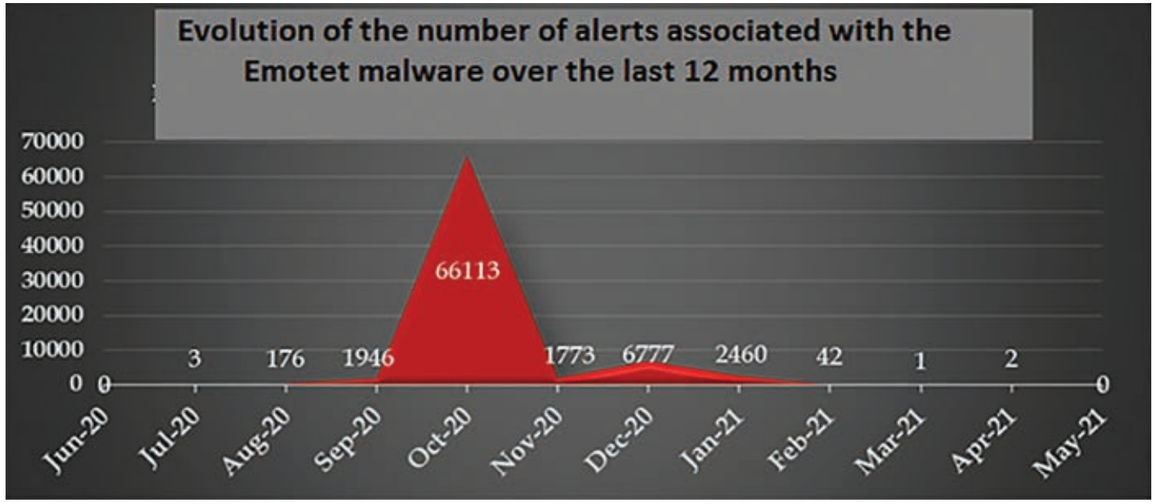


Perspectiva CEC Bank

În perioada 15 septembrie – 30 octombrie 2020, CEC Bank a fost vizată de un număr semnificativ de mesaje de tip phishing transmise pe adresele de email ale angajaților, situație care a impus adaptarea rapidă a mecanismelor tehnice și procedurale de protecție anti-phishing. De asemenea, a fost resimțită necesitatea creșterii resursei umane alocate în cadrul Centrului Operațional de Securitate (SOC) pentru asigurarea monitorizării incidentelor de securitate cibernetică și asigurării răspunsului la acestea.
La nivelul CEC Bank s-a reușit gestionarea cu succes a campaniilor Emotet datorită automatizărilor la nivelul SOC, implementării unor mecanisme tehnice care să permită identificarea unor elemente de comportament anormal în fluxul de mesaje electronice recepționate și filtrării cu succes a mesajelor transmise către angajați.

În urma campaniilor cibernetice în care a fost utilizat Emotet, specialiștii în securitate cibernetică au dezvoltat o soluție software prin intermediul căreia este detectată infecția. Tool-ul poate fi descărcat de la adresa de GitHub https://github.com/JPCERTCC/EmoCheck.

Suplimentar, a fost dezvoltat un instrument online pentru verificarea și identificarea compromiterii cu Emotet a adreselor de email și a domeniilor web. Acesta este disponibil la adresa https://www.haveibeenemotet.com.



The outlook of CEC Bank

Between September the 15th and October the 30th, 2020, CEC Bank was targeted by a significant number of phishing messages sent to the employees' e-mail addresses and this situation required the rapid adaptation of technical and procedural anti-phishing mechanisms. The need to increase the human resources allocated to the Operational Security Center (OSC) was also felt, in order to ensure the monitoring of cyber security incidents and the response to such events.
Within CEC Bank the Emotet campaigns were successfully thwarted due to the automation of processes within the OSC, to the implementation of technical mechanisms designed to identify abnormal behavior in the flow of incoming e-mails and to the successful filtering of the messages sent to employees.

Following the cyber campaigns where Emotet was used, cyber security specialists developed a software solution which detects the infection. The tool can be downloaded from the GitHub address https://github.com/JPCERTCC/EmoCheck.

In addition, an online tool was developed, which checks e-mails and Web domains and identifies the ones compromised by Emotet. It is available at https://www.haveibeenemotet.com.

Moreover, given their scale, Emotet campaigns drew the attention of public

Mai mult, dată fiind anvergura lor, campaniile cu Emotet au atras atenția instituțiilor publice cu responsabilități în domeniul securității cibernetice. Astfel, în urma eforturilor susținute ale autorităților competente din Olanda, Germania, Statele Unite ale Americii, Regatul Unit al Marii Britanii și Irlandei de Nord, Franța, Lituania, Canada și Ucraina, sub coordonarea Europol și Eurojust, activitatea Emotet a fost sistată brusc în data de 25.01.2021.

Ca urmare a acestui demers, autoritățile au obținut control asupra infrastructurii de comandă și control utilizată de Emotet, distribuind către toate sistemele infectate fișiere binare al căror rol a fost de a dezinstala componentele malware în data de 25 aprilie 2021. Ulterior acestei date, s-a observat că toate serverele de comandă și control ale Emotet cunoscute în mediul online au devenit inactive.
Cu toate acestea, nu putem afirma că Emotet a dispărut din sfera amenințărilor cibernetice criminale. În trecut, actorii cibernetici care operaționalizează aplicația malware au avut perioade lungi de inactivitate, revenind de fiecare dată cu capabilități inovatoare și de complexitate ridicată. Este posibil ca aceștia să își diversifice și de această dată tehnicile, tacticile și procedurile, adăugând funcționalități superioare, atât din punct de vedere tehnic, cât și din punct de vedere al tehnicilor de inginerie socială utilizate.

Cazul destructurării de către instituții abilitate a infrastructurii de atac utilizată în atacurile derulate cu Emotet este un succes real, dar și o excepție la nivelul ecosistemului cybercrime. De cele mai multe ori, astfel de investigații au rezultate minimale, atacatorii cibernetici afectați dezvoltând o nouă infrastructură, precum și noi instrumente și aplicații malware.

Perspectiva BITDEFENDER

În cazul campaniilor cu Emotet a fost prima oară când a fost observată utilizarea unor conversații legitime compromise anterior și modificarea acestora astfel încât să-și păstreze veridicitatea, având ca scop inducerea în eroare a altor victime. Chiar dacă gruparea a fost destructurată, ne așteptăm ca această metodă să înceapă sa fie folosită și de alte grupări, fiind dovedit că funcționează în majoritatea cazurilor. În acest context, recomandăm acordarea unei atenții sporite conversațiilor purtate prin intermediul serviciilor de email, indiferent dacă, în aparență, vin din partea unei persoane cu care am schimbat emailuri în trecut.

institutions with responsibilities in cyber security. Thus, after the sustained efforts of competent authorities in the Netherlands, Germany, the United States of America, the United Kingdom of Great Britain and Northern Ireland, France, Lithuania, Canada and Ukraine, under the coordination of Europol and Eurojust, the Emotet activity was terminated abruptly on January 25th, 2021.

Thanks to this endeavor, the authorities got control of the command and control infrastructure used by Emotet, by distributing to all infected systems binary files the role of which was to uninstall the Malware components on April 25th, 2021. After that date, it was noted that all Emotet command and control servers known online became inactive.
Nevertheless, we cannot state that Emotet was eliminated from the range of criminal cyber threats. In the past, cyber actors that operate the Malware application have had long periods of inactivity, but have always re-emerged with innovative and highly complex capabilities. It is likely that they will once more diversify their techniques, tactics and procedures, by adding superior functionalities, both technical and in terms of social engineering techniques.

The competent authorities disrupting the attack infrastructure used in the attacks carried out with Emotet is a real success, but it is also an exception in the cybercrime ecosystem. Most of the times, such investigations register minimal results, the affected cyber attackers developing a new infrastructure as well as new Malware tools and applications.

The outlook of BITDEFENDER

In the case of Emotet campaigns, the use of legitimate conversations that had been compromised beforehand and their alteration so that they kept their veracity with the purpose of misleading other victims was noted for the first time. Even if the group was disbanded, we expect this method to start being used by other groups, since it has already been proven to work in most of the cases. In this context, we recommend that particular attention be paid to conversations carried out by e-mail, in spite of the fact that they apparently come from a person with whom we have previously exchanged e-mails.

Evaluare și trenduri ale amenințărilor cibernetice la adresa sectorului financiar-bancar

Ținând cont de atractivitatea sectorului financiar-bancar pentru actorii cibernetici care derulează activități subsumate cybercrime, amenințările cibernetice asupra acestuia vor continua să se mențină la un nivel ridicat.
Contextul global generat de pandemia COVID-19 a evidențiat capacitatea actorilor cibernetici de a-și adapta și diversifica activitatea în sensul maximizării câștigurilor financiare. Aceștia vor căuta să mențină acest trend, targetând atât platformele și angajații instituțiilor financiar-bancare, cât și contractorii și clienții acestora.

În fapt, un lucru este cert – actorii cibernetici criminali nu își vor înceta activitatea. Pentru aceștia, atractivitatea domeniului financiar-bancar se va menține permanent. Importantă pentru diminuarea riscurilor și înlăturarea amenințărilor este adoptarea, la nivelul instituțiilor bancare, a unui comportament pro-activ în fața acestor amenințări, manifestat atât prin implementarea unei strategii proprii, cât și prin cooperare cu instituții publice cu atribuții în domeniul securității cibernetice, respectiv cu companii din domeniu.

Cyber Threats to the Financial - Banking Sector - Assessment and Trends

Given its attractiveness to the cyber actors that carry out activities falling under cybercrime, the cyber threats against the financial and banking sector will continue to remain high.
The global context generated by the COVID-19 pandemic has emphasized the cyber actors' ability to adapt and diversify their activity in order to maximize their financial gains. They will work to maintain this trend, targeting both financial and banking platforms and employees, as well as their contractors and clients.

In fact, one thing is certain - criminal cyber actors will not cease their activity. To them, the attractiveness of the financial and banking sector will remain permanent. The important thing in order to mitigate the risks and eliminate the threats is for banking institutions to adopt a pro-active behavior when faced with these threats, both by implementing their own strategies, and by cooperating with public institutions with responsibilities in cyber security, and with companies operating in this field respectively.

WWW.SRI.RO/CYBERINT