Cyber Threats in the context of COVID-19

2020

Ransomware attacks

Encrypt and / or block access to data and request a virtual currency ransom

Use of **spear-phishing** techniques to infect targets

Use of COVID-19 specific **impersonation** elements (email addresses, titles, text content etc.)

Targets - government institutions in key areas for COVID-19 crisis management, especially in the field of **Health**

Recommendations:

- **avoid opening email** attachments that apparently contain info related to COVID-19 or that come from unknown addresses
- **avoid accessing links and opening email attachments** (eg .doc, .docx, .pdf)
- use of updated **Antivirus** solutions
- make daily **backups**
- update all **operating systems**
- use low level of **privileges**
- **avoid providing personal data**

Website defacement attacks

Attack that consists in the unauthorized replacement of a web page interface, by exploiting **cyber security vulnerabilities**

Targets - government institutions in key areas for COVID-19 crisis management, especially in the field of **Health**

They affect both **the ability of institutions to communicate online** the measures and decisions taken, and the functionality of the websites used

Recommendations:

- **investigate the web server**, to identify signs of compromise and unauthorized access;
- **update** to the latest version of the server and web applications
- **define an access policy** by blocking ports at the level of specific servers, except for strictly necessary ports (e.g HTTP, HTTPS etc.)
- **make daily backups**
- **set access credentials with a high degree of security**

Cyber attacks that use banking Trojan malware

- Distribution of malware to **steal online banking credentials** from mobile terminals
- Use of social engineering techniques, **spear-phishing and smishing**, which exploit elements specific to COVID-19
- **Targets - individual users**
- Malware campaign identified in the context of COVID-19: **Cerberus Android Banker**

Recommendations:

- **check bank accounts** to detect possible unauthorized accesses
- **reset the mobile device** to the factory settings
- **change access credentials for device and application authentication**
- **avoid accessing links or attachments** from unknown sources

Cerberus Android Banker

"In the context associated with the SARS-CoV-2 pandemic, a malware distribution campaign has been identified aimed at stealing online banking credentials from users' mobile terminals.
From a technical perspective, the illegal action is based on the distribution of a text message containing a new version of the Trojan Cerberus Android Banker. The message is written in Romanian and invites users to access a link to download information on SARS-CoV-2. The phrase used in the content of the message is "Secret details! (COVID-19) ".
The main danger is that the Trojan provides illegal access to data from banking applications. Cerberus Android Banker can also extract data about messaging and email applications installed on the targeted device (e.g Telegram, WhatsApp or Gmail), as well as key logging

Awareness: Campanie *malware* de furt de credențiale bancare

24 aprilie 2020

În contextul asociat pandemiei de SARS-CoV-2 a fost identificată o campanie de distribuire de *malware* care vizează furtul de credențiale bancare de pe terminalele mobile ale utilizatorilor.

Din punct de vedere tehnic, acțiunea ilicită are la bază distribuirea unui mesaj tip text care conține o versiune nouă a troianului *Cerberus Android Banker*. Mesajul este redactat în limba română și invită utilizatorii să acceseze un link pentru descărcarea de informații privind SARS-CoV-2. Sintagma utilizată în conținutul mesajului este „Detalii secrete! (COVID-19)". Link-ul inițiază descărcarea unui fișier denumit *File.apk* care infectează cu respectivul troian dispozitivele mobile cu sisteme de operare Android, versiunile cuprinse între 4.0 și 10. Funcționalitățile *Cerberus Android Banker* împiedică atât detectarea acestuia de către serviciul Play Protect specific Android, cât și dezinstalarea ulterioară a aplicației de către utilizator.

Principalul pericol este acela că troianul oferă acces ilicit la date din aplicațiile bancare. De asemenea, *Cerberus Android Banker* poate extrage date despre aplicațiile de mesagerie și poștă electronică instalate pe dispozitivul vizat (spre exemplu, Telegram, WhatsApp sau

Qbot

"In April 2020, a cyber-attack campaign was identified being conducted by a cybercrime group using the Qbot banking trojan (QakBot, Plinkslipbot, QuakBot). In the various variants identified, the Trojan mainly targets customers of financial-banking organizations in the US, Romania, Canada and Greece. To a lesser extent, Qbot also targeted customers of technology, commercial and telecom organizations.

In Romania, the campaign targeted customers of platforms that use internet banking services through browsers (Chrome, FireFox, Microsoft Edge) and not through dedicated applications."

RO / EN

Cyber Awareness: Troian bancar infectează soluțiile de Internet Banking prin browser

28 aprilie 2020

În luna aprilie a anului în curs a fost identificată o campanie de atacuri cibernetice a unei grupări de criminalitate cibernetică care utilizează troianul bancar Qbot (QakBot, Plinkslipbot, QuakBot). În diferitele variante identificate, troianul vizează preponderent clienții organizațiilor din domeniul financiar-bancar din SUA, România, Canada și Grecia. Într-o măsură mai redusă, Qbot a vizat și clienți ai organizațiilor din domeniul tehnologic, comercial și al telecomunicațiilor.

În România, campania a vizat clienții unor platforme care utilizează servicii de *internet banking* prin *browser* (Chrome, FireFox, Microsoft Edge) și nu prin aplicații dedicate.

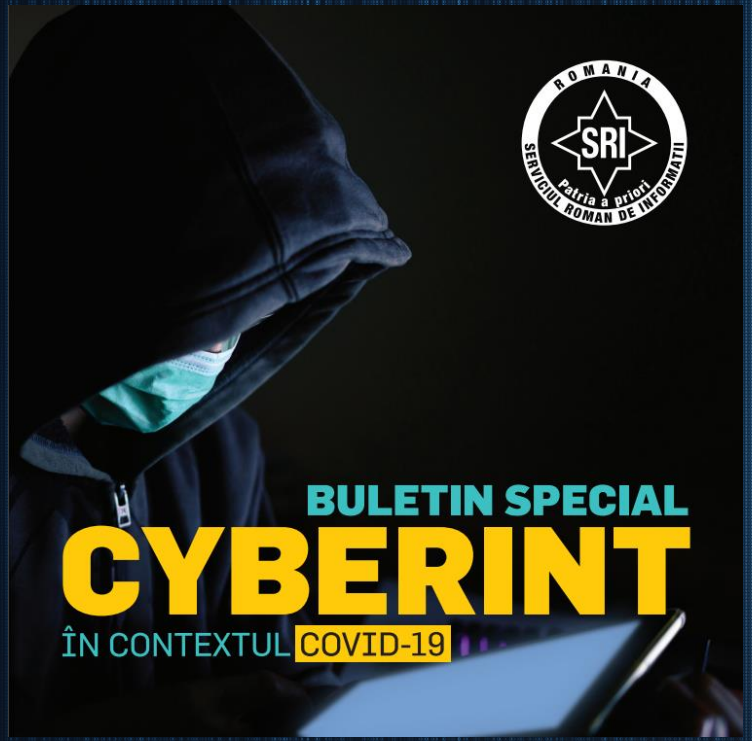
Prin transmiterea unor *e-mail*-uri capcană (*spear-phishing*), Qbot este programat să sustragă credențiale de acces pentru platforme specifice companiilor financiar-bancare și serviciilor de *e-mail* și date financiare.

Aceste mesaje pot avea fie un *link* în conținut, fie un atașament. Atașamentul este un fișier de tip *zip*, care conține un document *MS Word* ce rulează un *macro* prin care se descarcă troianul și se realizează infectarea dispozitivului. Odată instalat, Qbot verifică existența unui anti-virus, își asigură persistența în sistem și utilizează certificate de securitate valide pentru a evita detecția. Ulterior, troianul extrage credențiale de acces și date finanaciare de pe dispozitivul infectat. De asemenea, Qbot are capabilități prin care pot fi infectate și alte dispozitive dintr-o rețea cu un dispozitiv deja compromis.

Pentru a diminua riscul de infectare cu troianul bancar Qbot, recomandăm:

- utilizarea de soluții anti-virus și actualizarea constantă a semnăturilor acestora;
- evitarea deschiderii atașamentelor sub formă de arhivă dacă proveniența acestora este incertă și dacă nu au fost verificate în prealabil cu soluții de detecție anti-virus;
- evitarea deschiderii atașamentelor sau *link*-urilor din cadrul mesajelor e-mail suspecte;
- actualizarea sistemului de operare și evitarea utilizării sistemelor de operare care nu mai primesc suport din partea producătorului;
- notificarea băncii atunci când observați tranzacții bancare care nu vă aparțin;
- dezactivarea executării automate a unor rutine din MS Office (*macro*-uri);
- evitarea executării manuale a *macro*-urilor.

Cyber security culture in the context of COVID-19



"In the context of the COVID-19 crisis, hostile activities in cyberspace have intensified globally. Cyber actors use the current social context, both by conducting cyber attacks based on social engineering techniques and by attempting to affect services in key areas (health, public administration, education etc.) for the management of the COVID-19 crisis . Thus, ransomware and web defacement cyber campaigns were identified, including in Romania, as well as attacks with banking Trojan applications, in accordance with the motivations of the cyber actors involved."

Work from home

Remote access to the networks of public institutions has become a necessity, by implementing the "work from home" concept.

Recommendations for working from home

- Network administration will not be performed remotely
- The network will be accessed by users through the use of secure VPN connections
- Services accessed from the network (remote desktop, file servers etc.) will not be exposed directly to the Internet
- Creating security policies in firewall equipment
- Differentiate users at the logical level of the network and based on available resources, depending on needs
- For accessing the network, only computer systems provided by the organization will be used

The importance of ensuring cyber security in the context of COVID-19

Recommendations for ensuring a high level of cyber security of web platforms used:

- Ensure the ability to handle a large volume of applications
- Use an encrypted connection
- Use highly complex passwords across all services (authentication, database, server etc.)
- **Permanently update the modules/plugins installed, using only official sources**
- Provide protection against Distributed Denial of Service (DDoS) attacks

- **Avoid distributing documents on unofficial channels** (e.g. email, instant messaging services)
- **Access official sources of information** to eliminate the risk of infection with malware and to avoid exposure to false information
- **Institutions and organizations with key roles in the COVID-19 context** need to adopt preventive cyber security measures and to comply with security policies


Thank You!