Pandemia COVID-19 – factor potențator al activităților de criminalitate cibernetică

-Sectorul Financiar-Bancar-

CRIMINALITATEA CIBERNETICĂ ÎN PANDEMIA COVID-19

Contextul generat de pandemia COVID-19 a fost exploatat de grupările de criminalitate cibernetică pentru intensificarea derulării de atacuri cibernetice împotriva entităților publice și private, inclusiv asupra instituțiilor cu atribuții în domeniul financiar-bancar.

Caracteristici:

- **Adoptarea modelului *work from home* de către entități publice și private**
- **Gradul de utilizare al aplicațiilor bancare dedicate terminalelor mobilelor sau desktop a crescut semnificativ**
- **Atacurile cibernetice s-au intensificat (troian bancar, infostealer, ransomware)**

ATACURI CIBERNETICE ÎN CONTEXTUL COVID-19

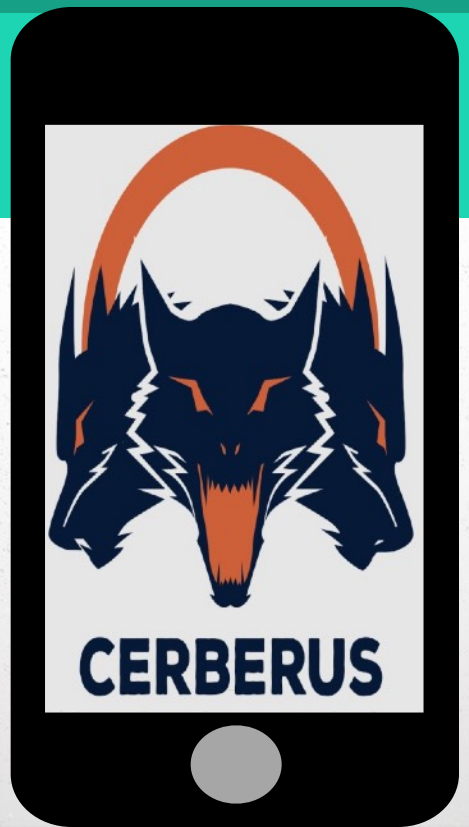
CERBERUS ANDROID BANKER

QBOT

EMOTET

CERBERUS ANDROID BANKER

- Mesaje redactate în limba română
- Mesajele fac referitoare la contextul pandemic: "**Detalii secrete! (COVID-19**)"
- Infectează dispozitivele mobile cu sisteme de operare ***Android***, versiunile cuprinse între 4.0 și 10



- Poate accesa datele aplicațiilor bancare
- Exfiltrează datele din aplicațiile de mesagerie și email
- Are funcție de keylogger

EMOTET

- Distribuit prin intermediul email-urilor de tip *phishing/spear-phishing*
- Scopul acestuia este exfiltrarea datelor financiare, dar și lansarea altor aplicații *malware*
- Infecția se realizează prin descărcarea unor fișiere *Microsoft Office* atașate email-urilor, acestea conținând *macro-uri* care descarcă malware-ul
- Vizează atât utilizatori individuali, cât și entități publice sau private
- Targetează sistemele informatice care utilizează sistemul de operare ***Microsoft Windows***
- Experții în securitate cibernetică au dezvoltat instrumente de detectare a infecției cu EMOTET, disponibile online

QBOT

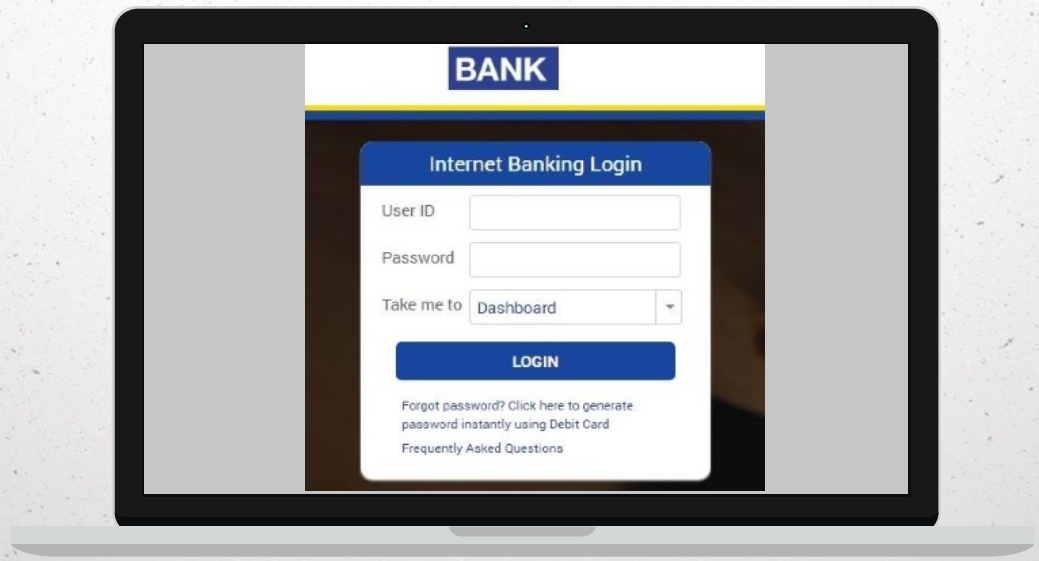
- Distribuit prin intermediul email-urilor de tip *spear-phishing*
- A targetat clienții instituțiilor financiar-bancare din România, SUA, Canada și Grecia
- A vizat clienții unor platforme de *internet banking* prin *browser* și nu prin aplicații dedicate
- Exfiltrează datele din cadrul platformelor financiar-bancare
- Deține capabilități pentru a-și asigura persistența în sistem și pentru a evita detecția
- Deține capabilități de mișcare laterală în cadrul unei rețele

IMPERSONAREA UNOR BĂNCI DIN ROMÂNIA

1. Utilizarea serviciilor de promovare platită din cadrul Google

2. Replicarea platformelor web ale bancilor și solicitarea acelorași tipuri de date de autentificare ca în cazul celor legitime (username, parolă, cod autentificare)

3. Redirecționarea către domeniul legitim pentru a face operațiuni bancare în numele clientului



IMPERSONAREA UNOR BĂNCI DIN ROMÂNIA

[redacted]

Produs/Serviciu

Trimite mesaj

Acasă Recenzii Fotografii Comunitate Mai multe Îmi place

Cronologie Despre Prieteni Fotografii Mai multe

ÎL CUNOȘTI PE BANCA?

Pentru a vedea ce le distribuie prietenilor, trimite-i o cerere de prietenie.

Adaugă

credit[redacted]
20 Tweets

Follow

credit[redacted]
@credit[redacted]

Credit[redacted] Comunitatea de lupta impotriva abuzurilor Bancii [redacted]
Credit[redacted]

Romania [redacted] Joined August 2010

4 Following 2 Followers

Not followed by anyone you're following

PROVOCĂRI WORK FROM HOME

Accesarea de la distanță a rețelelor instituțiilor a devenit o necesitate

Administrare necorespunzătoare

În unele situații, administrarea rețelelor destinate modelului *work from home* a fost realizată defectuos.

Echipamente necorespunzătoare

Resursele tehnice puse la dispoziția angajaților nu sunt în totalitate conforme cu necesitățile digitale actuale..

Neglijența utilizatorilor

În foarte multe situații, pregătirea utilizatorilor ce lucrează de la distanță nu a fost realizată corespunzător.

Expunere

Multe entități publice sau private și-au mutat activitatea în spațiul virtual.

Carențe de securitate

Multe entități publice sau private nu au implementat politici de securitate potrivite.

Exploatarea vulnerabilităților

Grupările de criminalitate cibernetică au profitat de condițiile impuse de pandemie pentru a exploata diverse vulnerabilități.

STRATEGII PENTRU ASIGURAREA SECURITĂȚII CIBERNETICE

Nivelurile securității cibernetice în cadrul unei organizații

Nivelul angajaților

Pregătirea și testarea angajaților pentru prevenirea incidentelor de securitate cibernetică

Nivelul administratorilor IT

Implementarea unor politici de securitate complexe și actualizate

Nivel instituțional

Cooperarea cu alte entități publice sau private specializate în securitate cibernetică

VĂ MULȚUMESC!