Clienții băncilor din România, ținte ale infractorilor cibernetici

Analiza unui atac cibernetic complex și eficient

Angheluș Alexandru – Prodefence
Oana Buzianu - Wintech

Societatea digitală actuală are nevoie de o disponibilitate continuă a serviciilor și de o protecție eficientă a datelor sensibile. Activele informaționale și serviciile online sunt foarte importante pentru toate organizațiile și sunt vitale pentru crearea unei economii digitale sigure.

Deși atacurile cibernetice vizează fiecare industrie, sectorul financiar este afectat în mod disproporționat, fiind vulnerabil la foarte multe amenințări din ce în ce mai sofisticate, deoarece infractorii cibernetici știu că au acces la sume mari care le autofinanțează activitățile criminale. Securitatea cibernetică în organizațiile din sectorul bancar a devenit din ce în ce mai critică.

Mizele cresc atunci când vorbim despre confidențialitatea, integritatea și disponibilitatea activelor informaționale, precum și despre implementarea unor servicii și aplicații de ultimă generație(Fintech, Blockchain), care conduc la îmbunătățirea rezistenței împotriva amenințărilor cibernetice. Sectorul financiar recunoaște evoluția amenințărilor și riscurilor cibernetice, precum și ritmul accelerat al tehnologiei în permanentă schimbare.

Ca și în cazul altor infrastructuri informaționale, o parte din deciziile și soluțiile adoptate de conducere nu se pot baza strict pe politici și proceduri, ci au la bază incidente de securitate cibernetică cu impact asupra propriilor instituții, sau analize/ rapoarte ale experților în securitate cibernetică.

Toate acestea subliniază necesitatea de a proteja datele și tranzacțiile cu date sensibile și, prin urmare, de a (re)asigura încrederea în sectorul financiar.

Această analiză are ca subiect un atac cibernetic extrem de complex și cu o activitate infracțională foarte ridicată, deși totul pleacă de la o simplă informație găsită pe una dintre platformele monitorizate de echipa Prodefence.

Așa cum se poate înțelege din figura 1, atacul cibernetic are ca țintă sistemul bancar, urmărind compromiterea conturilor de utilizator ale clienților unor bănci din România. Cuvântul ”unicredit” fiind cel care a declanșat ”alarma”.

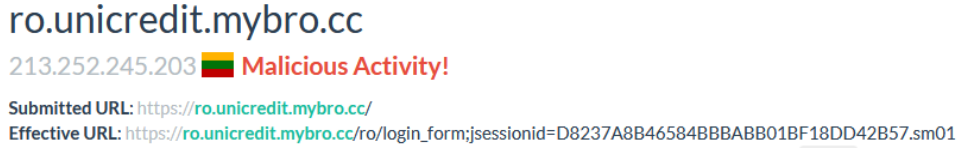


Fig1 : urlscan.io

În cache-ul platformei sursă am găsit stocată varianta online a sesiunii de acces în pagina falsă. Acest aspect este important, deoarece validează modalitatea de atac,

aparent fiind un atac cibernetic de tip Phishing. Un atac phishing care crează o sesiune unică, pentru victimă. Ceea ce ne poate duce cu gândul la furtul sesiunilor de access, prezentate în articolul ”Phishing-ul bancar” (https://sigurantaonline.ro/phishing-ul-bancar/), unde puteți vedea modul de funcționare a atacului cibernetic de tip phishing sau este modalitatea de identificare individuală a victimelor la accesarea aplicației false.

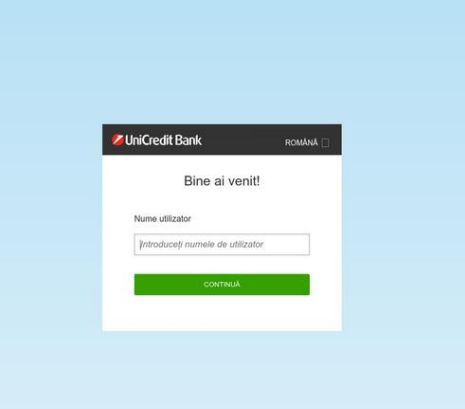
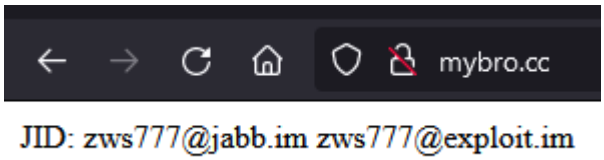


Fig2 : urlscan.io

Pentru început vom accesa domain-ul principal ”mybro.cc”, în încercarea de a aduna cât mai multe informații despre domain, subdomain și informațiile deținătorului.



JID: zws777@jabb.im zws777@exploit.im

```
1 <html>
2 <body>
3 JID: zws777@jabb.im zws777@exploit.im<br>
4 </body>
5 </html>
6
```

Fig3 : Analiză Prodefence

Pagina principală deține informațiile de contact ale deținătorului și cam atât. Nu există alte informații vizibile, nici măcar în codul sursă.

Adăugăm câteva cuvinte cheie în Google search, dar nu există informații relevante. Și totuși, folosind ”intext:mybro.cc” avem parte de informații despre o analiză care face referire la subiectul nostru.

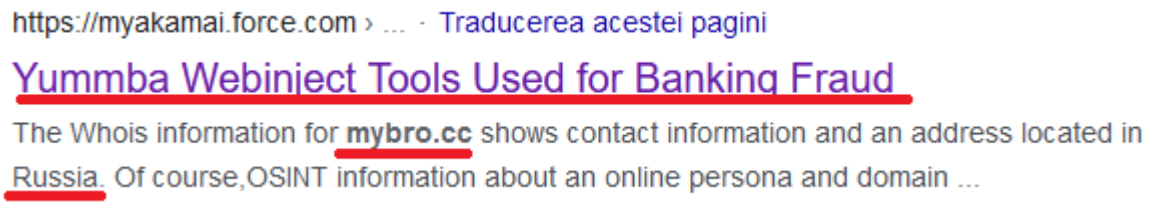


Fig4 : Google search engine

https://myakamai.force.com/customers/s/article/Yummba-Webinject-Tools-Used-for-Banking-Fraud?language=en_US

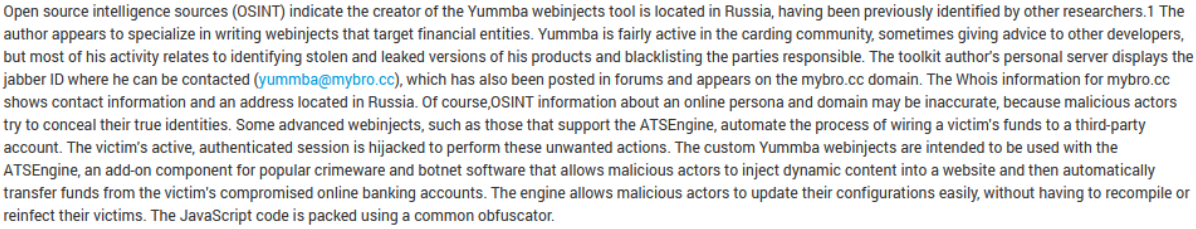

Open source intelligence sources (OSINT) indicate the creator of the Yummba webinjects tool is located in Russia, having been previously identified by other researchers.1 The author appears to specialize in writing webinjects that target financial entities. Yummba is fairly active in the carding community, sometimes giving advice to other developers, but most of his activity relates to identifying stolen and leaked versions of his products and blacklisting the parties responsible. The toolkit author's personal server displays the jabber ID where he can be contacted (yummba@mybro.cc), which has also been posted in forums and appears on the mybro.cc domain. The Whois information for mybro.cc shows contact information and an address located in Russia. Of course,OSINT information about an online persona and domain may be inaccurate, because malicious actors try to conceal their true identities. Some advanced webinjects, such as those that support the ATSEngine, automate the process of wiring a victim's funds to a third-party account. The victim's active, authenticated session is hijacked to perform these unwanted actions. The custom Yummba webinjects are intended to be used with the ATSEngine, an add-on component for popular crimeware and botnet software that allows malicious actors to inject dynamic content into a website and then automatically transfer funds from the victim's compromised online banking accounts. The engine allows malicious actors to update their configurations easily, without having to recompile or reinfect their victims. The JavaScript code is packed using a common obfuscator.

Fig5 : myakamai.force.com

Sunt informații despre deținătorul domain-ului mybro.cc și face referire la o aplicație folosită în furtul sesiunilor de acces, Yummba webinjects tool.

Deci avem noi cuvinte cheie de căutare și descoperim suficiente informații despre Yummba tool.

O analiză foarte bună este ”THE EVOLUTION OF WEBINJECTS” a lui Jean-Ian Boutin, unde face referire la mybro.cc, la activitățile din spatele acestui domain și explicații despre injectarea web.

Injectarea web este modalitatea de a include elemente malițioase în codul paginii web sau includerea în adresa paginii a unor parametri care să permită atacatorului monitorizarea activităților victimei.

Analiza celor de la Virus Bulletin scoate în evidență informații relevante.

https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Boutin.pdf

Figura 11 din analiză face referire la domain-ul în cauză, printr-o captură a unui articol din 2013, unde utilizatorul *yummba* oferă spre vânzare o injectare web capabilă să intercepteze mesajele SMS (mesaje folosite la dubla autentificare). Dacă dăm suficientă atenție acestei informații realizăm că interceptarea dublei autentificări prin SMS este posibilă de mult timp.

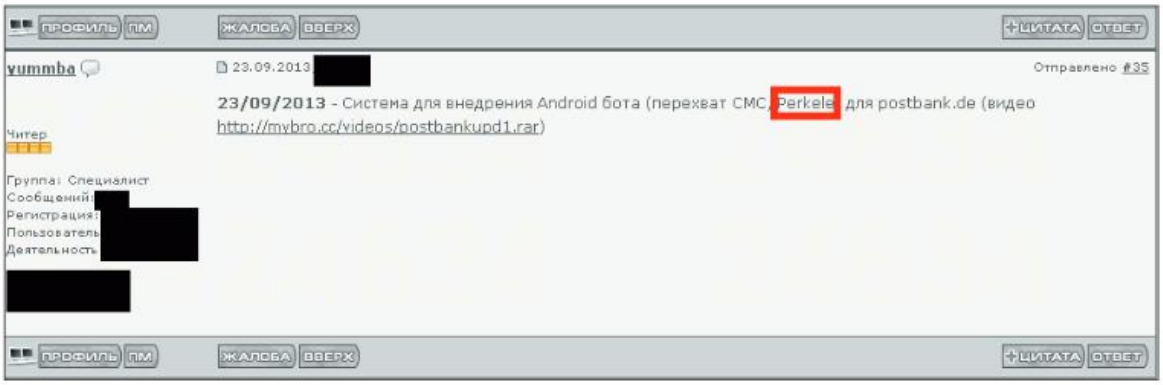


Figure 11: Webinject coder bundling Perkele, a mobile component able to intercept SMS messages, as part of a webinject offering.

Fig5: THE EVOLUTION OF WEBINJECTS

Interesant ar fi să vedem dacă în afară de ro.unicredit.mybro.cc mai există și alte subdomenii.

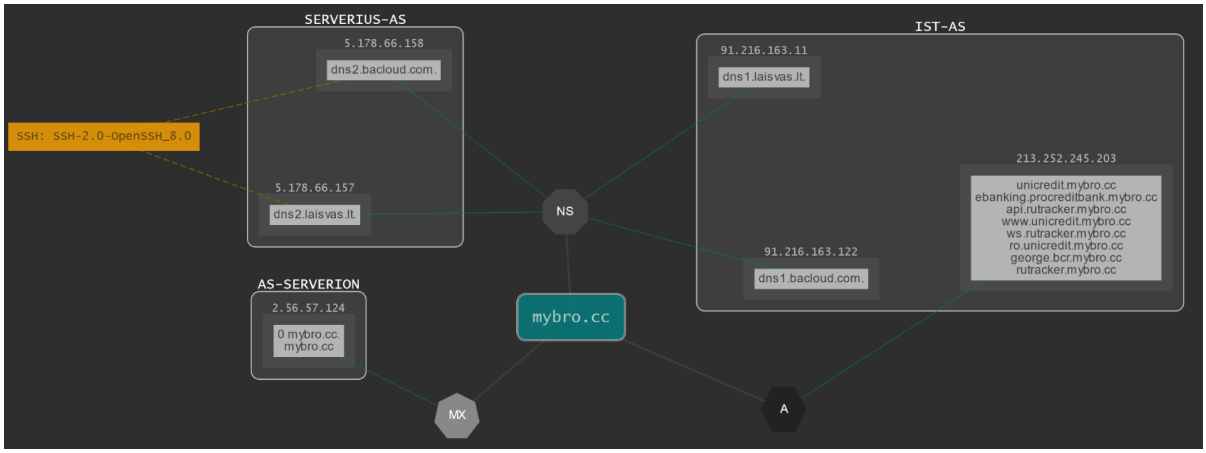


Fig6 : dnsdumpster.com

Fig7 : dnsdumpster.com

Informațiile colectate complică analiza noastră, deoarece se pare că țintă sunt clienții mai multor bănci din România, dar se pare că din tot sistemul bancar global, doar aceste bănci sunt ținta infractorilor. Clienții băncilor Unicredit, Procredit și BCR au fost/ sunt vizați în mod direct de aceste atacuri.

unicredit.mybro.cc
ebanking.procreditbank.mybro.cc
ro.unicredit.mybro.cc
george.bcr.mybro.cc

În momentul analizei, indiferent de dispozitivul folosit, subdomeniile nu pot fi accesate sau se permite accesul dacă dispozitivele vin cu o anumită redirecționare/ sesiune.

Vom analiza puțin serverul

Ip-ul alocat la data începerii acestei analize era 213.252.245.203, găzduit pe un server din Lituania

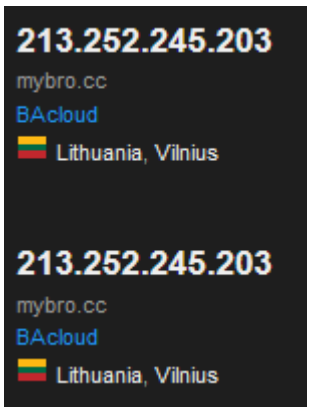


Fig8 : shodan.io

Porturi vizibile:

22(OpenSSH8.2p1 Ubuntu-4ubuntu0.4),
80(Apache httpd2.4.41),
443(Apache httpd2.4.41),
4369(Erlang Port Mapper Daemon name ejabberd at port 37282),
5269(stream:stream id='7676721247852660454)

De asemenea în timpul analizei inițiale pe una dintre platformele de identificare a deținătorilor apărea informația că domain-ul este în curs de transfer și se pare că noul server are alocat IP-ul 69.49.245.42, US.

Registrar Status	pendingTransfer
Dates	509 days old Created on 2021-01-31 Expires on 2025-01-31 Updated on 2022-06-20
Name Servers	DNS1.BACLOUD.COM (has 2,154 domains) DNS1.LAISVAS.LT (has 92 domains) DNS2.BACLOUD.COM (has 2,154 domains) DNS2.LAISVAS.LT (has 92 domains)

Fig9: whois

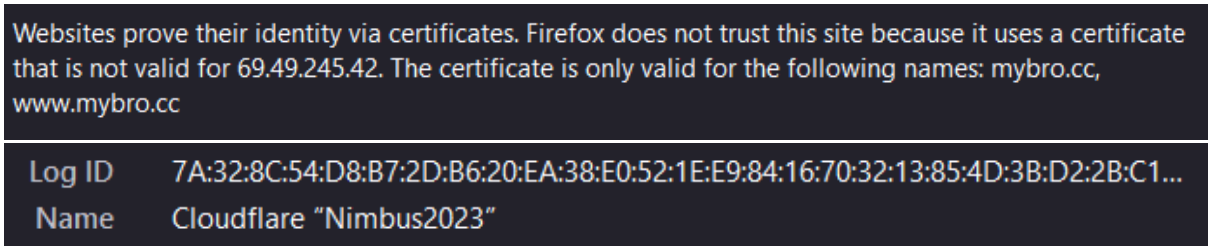


Fig10: whois

Foarte multe porturi deschise, dar lipsesc cele de pe serverul anterior: 4369 și 5269

Figura 5 include și o adresă spre o arhivă rar, iar la accesare este cerută o parolă. După includerea după domain a unor cuvinte random realizăm că indiferent de ceea ce căutăm vom avea același răspuns cu fereastra de acces, ceea ce denotă faptul că acele fișiere nu mai există pe server.

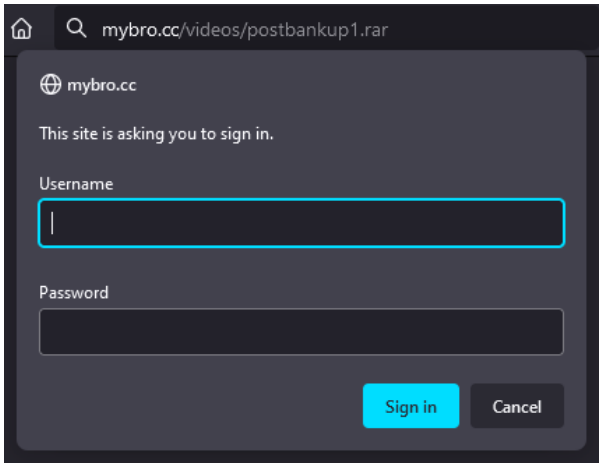


Fig11: urlscan.io

În arhivele stocate de Google apare o captură cu fișierele existente, acestea find modificate în anul 2014.

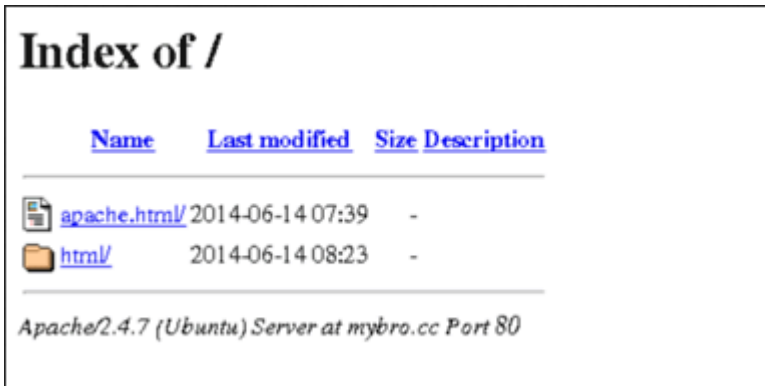


Fig12 : Google search engine

Ne întoarcem la subdomain-ul găsit inițial și reușim să găsim câteva informații extra.

ro.unicredit.mybro.cc/ro/
ro.unicredit.mybro.cc/ro/private
ro.unicredit.mybro.cc/ro/login_form;jsessionid=D8237A8B46584BBBABB01BF18DD42B57.sm01 1
ro.unicredit.mybro.cc/noastatics/css/framework/framework-1.10.43.4.css?ts=1655250572
ro.unicredit.mybro.cc/comp!cwbuicore/static/js/react/cwb-js-common-core-react.jsx.js?ts=1655250572 2
ro.unicredit.mybro.cc/comp!cwbuicore/static/js/react/login-flow-core-react.jsx.js?ts=1655250572 3
ro.unicredit.mybro.cc/comp!cwbuicore/static/js/react/cwb-generic-menu-core-react.jsx.js?ts=1655250572
ro.unicredit.mybro.cc/cms/!root!/etc/designs/cee2020-ib-core/static/images/logo_uc.png
ro.unicredit.mybro.cc/comp!loginflowcore/-2139274127/controller!login_state_controller/checkLoginBgSource 4

Acestea sunt resursele paginii false, care ofereau vizitatorului o imagine foarte apropiată de cea a paginilor bancare oficiale.

De precizat faptul că atacatorii cibernetici sunt de cel puțin două categorii:

1.Deținători ai acestor aplicații malițioase, care extrag informațiile victimelor și pot acționa prin:

- Vânzarea aplicației către alți infractori,
- Vânzarea de informații bancare colectate,
- Extragerea de fonduri din conturile victimelor.

2.Infractori cibernetici care cumpără aplicația sau informațiile bancare, având ca scop extragerea de fonduri.

Din motive legislative, analizarea acestor infracțiuni se poate face doar prin metode care nu acționează asupra serverului sau a paginii web, neavând posibilitatea de a găsi sau extrage informații care nu sunt vizibile, dar care posibil să existe și să contureze ideea din spatele atacurilor cibernetice financiare.

Transferul domeniului pe alt server și menținerea subdomeniilor denotă faptul că atacurilor vor continua, pot fi mai avansate, pot include și alte bănci din România... totul fiind posibil. La momentul actual nu putem face prea multe, dar continuăm monitorizarea domeniului și al activităților acestuia, cu speranța că vom descoperi la timp următoarele ținte și atacuri.

Phishing-ul este o problemă majoră pe care trebuie să se concentreze toată lumea și sperăm că acest lucru vă va ajuta să înțelegeți de ce educația privind manipularea utilizatorilor prin phishing este vitală pentru a rămâne în siguranță atât la serviciu, cât și acasă.

Așa cum am precizat anterior, pentru a înțelege modalitatea de furt al sesiunilor și manipularea acestora, vă recomandăm documentul *”Phishing-ul bancar”*, preluat de Directoratul Național de Securitate Cibernetică, Asociația Băncilor din România și Poliția Română, fiind găzduit la adresa: https://sigurantaonline.ro/phishing-ul-bancar/, aceasta fiind o modalitate de a învăța să fim mai vigilenți atunci când suntem vizați de un atac cibernetic de acest tip.

Care sunt concluziile aceastei analize:

Am fost, suntem și vom continua să fim țintele atacurilor cibernetice financiare, deoarece acestea constituie o modalitate de finanțare pentru infractorii cibernetici.

Securitatea cibernetică fiind o responsabilitate comună, trebuie ca fiecare dintre noi să fie responsabil de monitorizarea conformității controalelor de securitate cibernetică și de gestionarea riscurilor în acest domeniu.

1. Experții să ajute prin expunerea cunoștințelor,
2. Băncile să își protejeze în continuare clenții,
3. Clienții să nu se bazaze pe cei de la puncele anterioare și să își ofere timp pentru educație cibernetică, deoarece tehnologia și transmiterea datelor online sunt parte din viața noastră.

De aceea este important să urmăriți cursurile de educație cibernetică pregătite de noi. Acestea sunt gratuite, conțin informații care vă pot ajuta să identificați un atac cibernetic și vă vor ajuta să diminuați riscul asumat în folosirea tehnologiei.

https://www.cyberaid.eu/cursuri-educatie-cibernetica/

Iar urmărirea avertizărilor cibernetice oferite de Directoratul Național de Securitate Cibernetică și de ProWin Group, trebuie să devină o rutină zilnică!

Rămâi în siguranță!