# Romanian banks customers, targets of cybercriminals

## Analysis of a complex and effective cyber-attack

Angheluș Alexandru – Prodefence
Oana Buzianu - Wintech

Nowaday’s digital society needs continued availability of services and effective protection of sensitive data. Information assets and online services are very important for all organisations and vital for creating a secure digital economy.

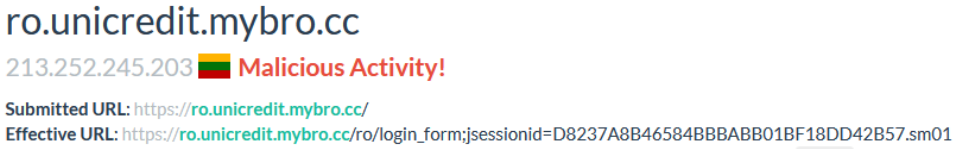
Although cyberattacks target every industry, the financial sector is disproportionately affected, being vulnerable to many increasingly sophisticated threats, as cybercriminals know that they have access to large sums that self-finance their criminal activities. Cybersecurity in banking organizations has become increasingly critical.

The stakes rise when we talk about the confidentiality, integrity and availability of information assets, as well as the implementation of state-of-the-art services and applications (Fintech, Blockchain), which lead to improved resilience against cyber threats. The financial sector recognises the evolution of cyber threats and risks, as well as the ever-changing pace of technology.

As with other information infrastructures, some of the decisions and solutions adopted by the management cannot be based strictly on policies and procedures, but are based on cybersecurity incidents with an impact on their own institutions, or analyzes / reports of cybersecurity experts.

All this underlines the need to protect data and transactions in sensitive data and therefore to (re)ensure trust in the financial sector. This analysis is about an extremely complex cyberattack with a very high criminal activity, although everything starts from a simple information found on one of the platforms monitored by the Prodefence team.

As can be understood from Figure 1, the cyber-attack targets the banking system, aiming at compromising the user accounts of the clients of some banks in Romania. The word "unicredit" being the one that triggered the "alarm".



ro.unicredit.mybro.cc

213.252.245.203 🇱🇹 Malicious Activity!

**Submitted URL:** https://ro.unicredit.mybro.cc/
**Effective URL:** https://ro.unicredit.mybro.cc/ro/login_form;jsessionid=D8237A8B46584BBBABB01BF18DD42B57.sm01

*Fig1 : urlscan.io*

In the cache of the source platform we found stored the online version of the access session in the fake page. This is important because it validates the mode of attack, apparently a Phishing cyberattack. A phishing attack that creates a unique session for the victim.

Which can lead us to think about the theft of access sessions, presented in the article "Bank Phishing" (https://sigurantaonline.ro/phishing-ul-bancar/), where you can see how the phishing cyber attack works, or is the way to individually identify the victims when accessing the fake application.

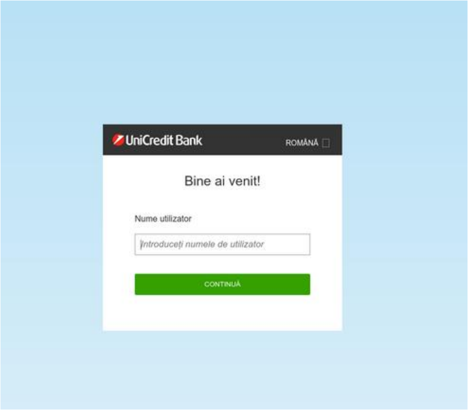
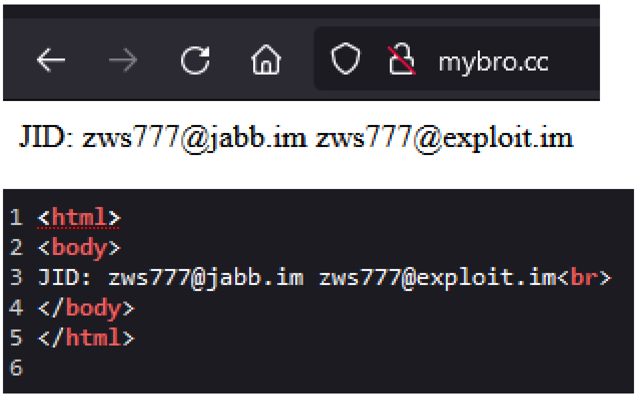


*Fig2 : urlscan.io*

To begin with, we will access the main domain "mybro.cc", in an attempt to gather as much information as possible about the domain, subdomain and the owner's information.



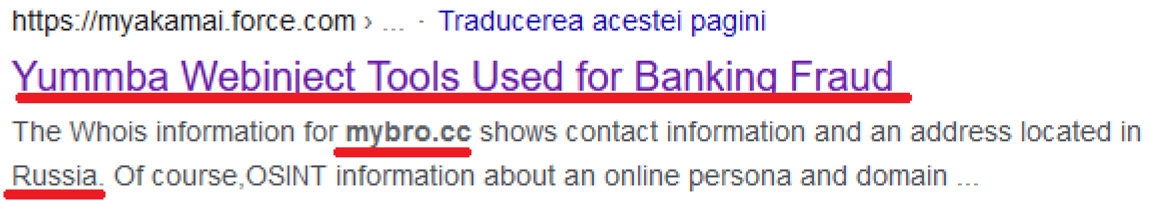
JID: zws777@jabb.im zws777@exploit.im

```
<html>
<body>
JID: zws777@jabb.im zws777@exploit.im<br>
</body>
</html>

```

*Fig3: Prodefence Lab. Analysis*

The main page has the owner's contact information and that's about it. There is no other visible information, not even in the source code. We're adding some keywords to Google search, but there's no relevant information. And yet, using "intext:mybro.cc" we get information about an analysis that references our topic.



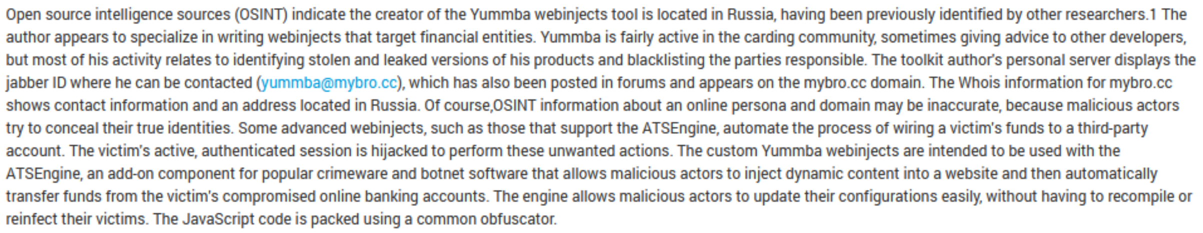
https://myakamai.force.com › ... · Traducerea acestei pagini

Yummba Webinject Tools Used for Banking Fraud

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 ...

*Fig.4: 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.

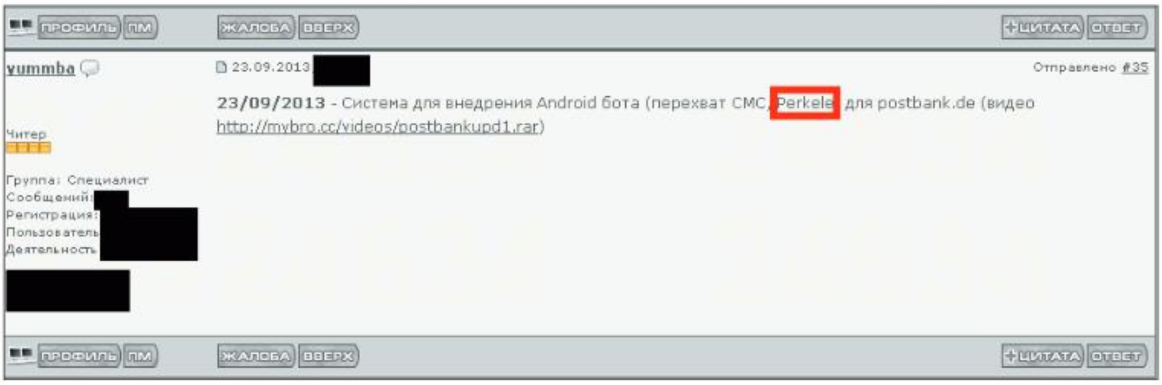
*Fig5 : myakamai.force.com*

It is information about the domain owner mybro.cc and refers to an application used in the theft of access sessions, Yummba webinjects tool. So we have new search keywords and we discover enough information about Yummba tool.

A very good analysis is Jean-Ian Boutin's "THE EVOLUTION OF WEBINJECTS", where he refers to the mybro.cc, the activities behind this domain and explanations about web injection. Web injection is the way to include malicious elements in the code of the web page or the inclusion in the address of the page of parameters that allow the attacker to monitor the activities of the victim. Virus Bulletin's analysis reveals relevant information.

[https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Boutin.pdf](https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Boutin.pdf)

Figure 11 of the analysis refers to the domain in question, through a capture of a 2013 article, where the yummba user offers for sale a web injection capable of intercepting SMS messages (messages used for double authentication). If we pay enough attention to this information we realize that intercepting double authentication by SMS is possible for a long time.



yummba

23.09.2013 [redacted]

Отправлено #35

23/09/2013 - Система для внедрения Android бота (перехват СМС, Perkele для postbank.de (видео http://mybro.cc/videos/postbankupd1.rar)

Читер

Группа: Специалист
Сообщений: [redacted]
Регистрация:
Пользователь
Деятельность [redacted]

[redacted]

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

*Fig6: THE EVOLUTION OF WEBINJECTS*

It would be interesting to see if apart from ro.unicredit.mybro.cc there are other subdomains.

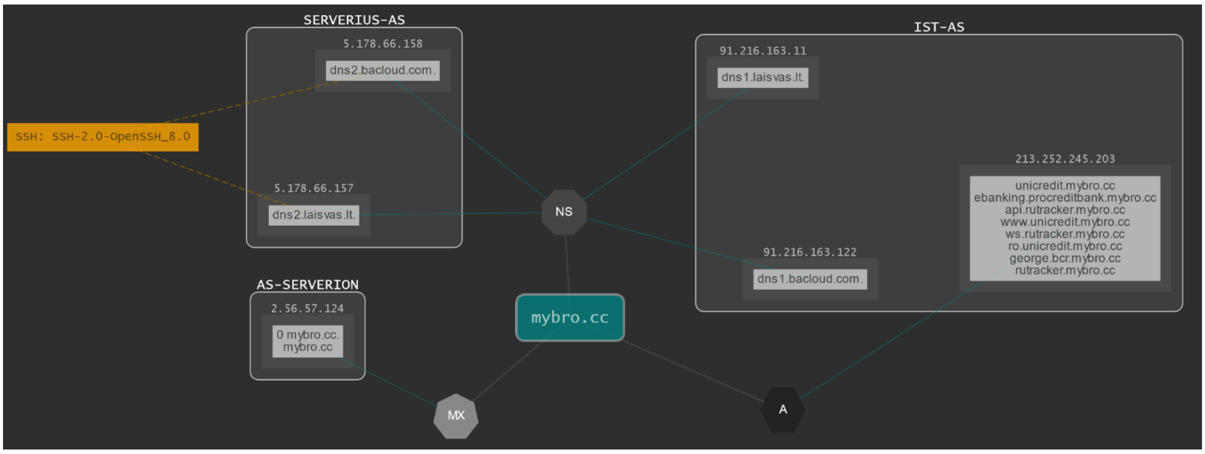
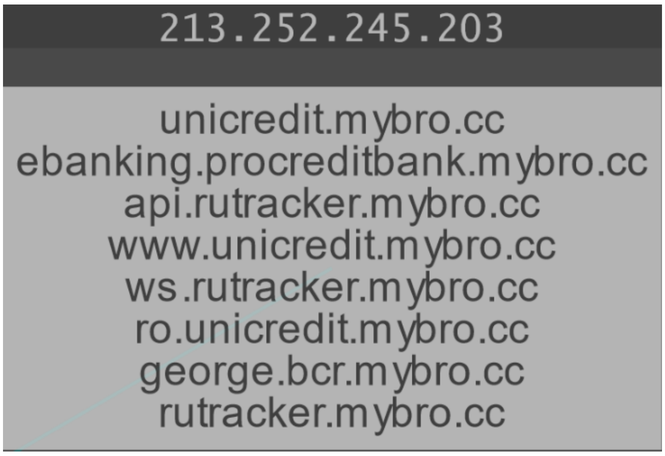


*Fig7 : dnsdumpster.com*



213.252.245.203

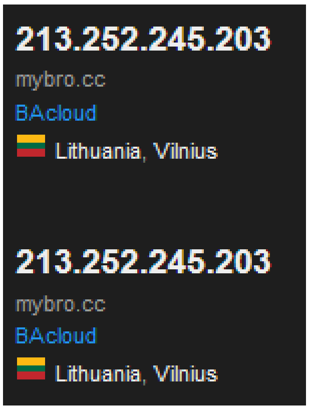
unicredit.mybro.cc
ebanking.procreditbank.mybro.cc
api.rutracker.mybro.cc
www.unicredit.mybro.cc
ws.rutracker.mybro.cc
ro.unicredit.mybro.cc
george.bcr.mybro.cc
rutracker.mybro.cc

*Fig8 : dnsdumpster.com*

The information collected complicates our analysis, because it seems that the target is the customers of several banks in Romania, but it seems that out of the entire global banking system, only these banks are the target of criminals. The clients of Unicredit, Procredit and BCR banks were/are directly targeted by these attacks.

http://ebanking.procreditbank.mybro.cc

At the time of analysis, regardless of the device used, the subdomains cannot be accessed or access is allowed if the devices come with a certain redirection / session. We'll take a little look at the server The IP allocated at the time of starting this analysis was 213.252.245.203, hosted on a server in Lithuania.



**213.252.245.203**

mybro.cc

BAcloud

🇱🇹 Lithuania, Vilnius

**213.252.245.203**

mybro.cc

BAcloud

🇱🇹 Lithuania, Vilnius

*Fig9 : shodan.io*

Visible ports:

22(OpenSSH8.2p1 Ubuntu-4ubuntu0.4),

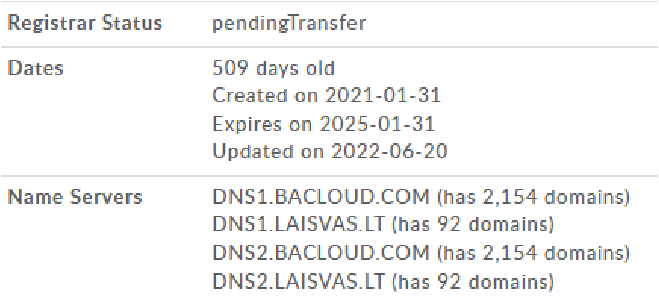
80(Apache httpd2.4.41),

443(Apache httpd2.4.41),

4369(Erlang Port Mapper Daemon  name ejabberd at port 37282),

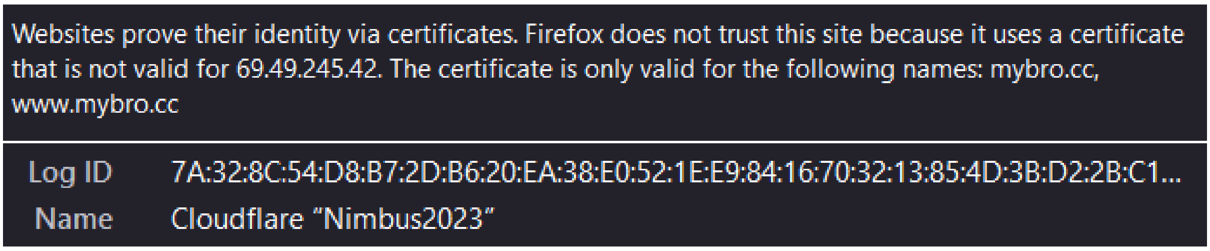
5269(stream:stream id='7676721247852660454)

Also, during the initial analysis on one of the platforms for identifying the owners appeared the information that the domain is in the process of being transferred and it seems that the new server has allocated the IP 69.49.245.42, US.



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

*Fig10: whois*

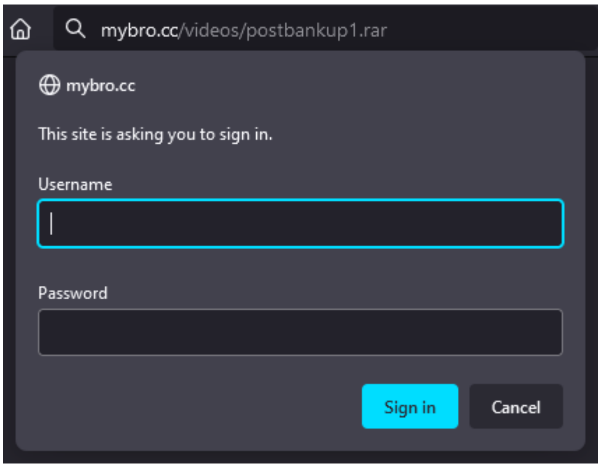


Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 69.49.245.42. The certificate is only valid for the following names: mybro.cc, www.mybro.cc

| | |
|---|---|
| Log ID | 7A:32:8C:54:D8:B7:2D:B6:20:EA:38:E0:52:1E:E9:84:16:70:32:13:85:4D:3B:D2:2B:C1... |
| Name | Cloudflare "Nimbus2023" |

*Fig11: whois*

Too many ports open, but missing those on the previous server: 4369 and 5269 Figure 5 also includes an address to a rare archive, and a password is required when accessing it. After including random words after the domain we realize that no matter what we are looking for we will have the same answer with the access window, which denotes that those files no longer exist on the server.



mybro.cc/videos/postbankup1.rar

mybro.cc

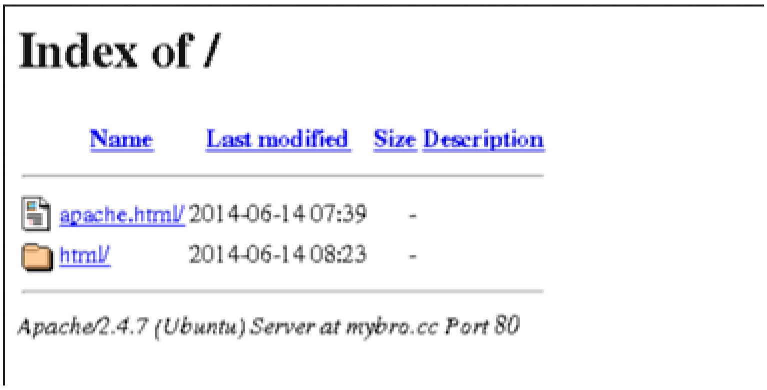
This site is asking you to sign in.

Username

Password

*Fig12: urlscan.io*

A capture of the existing files appears in the archives stored by Google, which were modified in 2014.



Index of /

| Name | Last modified | Size | Description |
|---|---|---|---|
| apache.html/ | 2014-06-14 07:39 | - | |
| html/ | 2014-06-14 08:23 | - | |

*Apache/2.4.7 (Ubuntu) Server at mybro.cc Port 80*

*Fig13 : Google search engine*

We go back to the subdomain originally found and we manage to find some extra information.

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

These are the resources of the fake page, which gave the visitor a very close image to that of the official banking pages. It should be noted that cyber attackers are of at least two categories:

1. Owners of these malicious applications, who extract the information of the victims and can act by:
- Selling the app to other criminals,
- Sale of collected banking information,
- Extracting funds from victims' accounts.

2. Cybercriminals who buy the app or bank information, with the aim of extracting funds. For legislative reasons, the analysis of these crimes can only be done through methods that do not act on the server or the web page, not having the possibility to find or extract information that is not visible, but that may exist and shape the idea behind the financial cyber-attacks.

Transferring the domain to another server and maintaining the subdomains denotes that the attacks will continue, may be more advanced, may include other banks in Romania... everything being possible. At the moment we cannot do much, but we continue to monitor the field and its activities, with the hope that we will discover the next targets and attacks in time.

Phishing is a major issue that everyone needs to focus on and we hope this will help you understand why education on manipulating users through phishing is vital to staying safe both at work and at home.

As previously mentioned, in order to understand the way of stealing the sessions and handling them, we recommend the document "Bank phishing", taken over by the National Cyber Security Directorate, the Association of Banks in Romania and the Romanian Police, being hosted at the address: https://sigurantaonline.ro/phishing-ul-bancar/ , this being a way to learn to be more vigilant when we are targeted by a cyberattack of this type.

What are the conclusions of this analysis:

We have been, are and will continue to be the targets of financial cyber-attacks because they are a way of funding for cybercriminals. Cybersecurity being a shared responsibility, each of us must be responsible for monitoring the compliance of cybersecurity controls and managing risks in this area.

1. Experts to help by exposing knowledge,

2. Banks to continue to protect their clergy,

3. Let customers not rely on those from the previous points and give themselves time for cyber education, because technology and online data transmission are part of our lives.

That is why it is important to follow the cyber education courses prepared by us. They are free of charge, contain information that can help you identify a cyber attack and will help you mitigate the risk you take in using the technology.

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

And following the cyber warnings provided by the National Directorate of Cyber Security and ProWin Group must become a daily routine!

Stay safe!

@ProWin Group