CERT-UA

Archived: 2026-04-05 13:56:34 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA вживаються організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки.

Так, 07.12.2023 виявлено факт масового розповсюдження електронних листів з темою "судових претензій" і "заборгованості" та додатками у вигляді вкладених RAR-архівів, захищених паролем.

У випадку відкриття такого архіву та запуску виконуваних файлів ЕОМ може бути уражена програмами RemcosRAT (ідентифікатор ліцензії: 3DBAF89B8E287E6A5221436A08EAA6B8, ідентифікатор кампанії: "DaVinci") або MeduzaStealer. При цьому, зокрема, застосовано Autoit-інжектор.

Типово для UAC-0050 сервери управління RemcosRAT розміщено на технічному майданчику малайзійського хостинг-провайдера Shinjiru.

Зауважимо, що для розсилання електронних листів використано легітимні скомпрометовані облікові записи, в т.ч. в домені gov.ua. Крім того, виявлено електронні листи, що свідчать про спрямування кібератаки проти органів державної влади Польщі.

Вкотре рекомендуємо елетронні листи з додатками, що захищені паролями (як архіви так і документи), фільтрувати на рівні поштових шлюзів.

CERT-UA вжито заходів з протидії кіберзагрозі.

Індикатори кіберзагроз

Файли:

```
573806ca8fe46711550de2e961e09145   3c99a4a03bd7c9b54ef6c2262dad042bb04f3f61f2453d336201c8e086606085
6ce55c5384d54141bf6cd97787fce9a0   7d6133584418f2aeb1ae3147731c78806f93004d62beecaeb3ced5b0d8a4a727
fad0fac025dc107d194710bf4d71fe93   4cc6fb5b5f416527296a4b2a84a6da92ce97dcca7db03f9e1c526048443453d2
26c885bd7a28236a8f82ce795ed1c21d   d6028c7ed3324a01614e2697f4cf0d095170eff8f36fae7e6e66aa5412d08b45
5e27454611915cbe6a898e0b1223c7e2   fcbc9b3b79c1ff1ca5c5d6c858b90a62be9f6c52093ebc6e6b10d743fee02019
e9bda9a2099a3517fa87fbc8627d06e3   e9c848a14f2cafcf90d912d0af0530bb3075559ba134f39483d55f462941fcb8
848164d084384c49937f99d5b894253e   f58d3a4b2f3f7f10815c24586fae91964eeed830369e7e0701b43895b0cefbd3
f92ba75d9b1576587eac561324236965   ad87af966492f5d7c6b4ccd2a08a5adcb3dd66be1a8b8eff44f57dc3c52b7126
5ae2b6a47e6fce919b191ecfe2d74b71   109a78347a8ef06775ebdab96979377aee6bb5325452754234d90955f0daf4eb
e9616499683400fa97dc8e8cb466bdcb   778231490899e006025bfb14f720c8faeacac7c7c1ee7bdd607cd458804a2944
502264acd60a5f84bfd6d1dad03f8862   ac5401906cefc2ecfda5a84f272c1289f5660c74753c35bfcc84ea49f13f8e41
33f28845863fa59c79b3ac8669722b68   8a244379c63cf5ae11f1c79cb7834374f76fd1c6ebed293d0569102d5d6308aa
00736ba8ccd459a131dda33a6563b66d   d20ef93dcd262985040f049c4df26c26b8bfcd4a97afa6cff41f5b4e92baf3fc
```

Мережеві:

```
(tcp)://101[.]99.75.140:8080
(tcp)://101[.]99.75.142:8080
(tcp)://101[.]99.75.145:465
(tcp)://101[.]99.75.145:8080
(tcp)://101[.]99.75.147:465
(tcp)://101[.]99.75.148:8080
(tcp)://101[.]99.75.156:465
(tcp)://101[.]99.75.159:465
(tcp)://101[.]99.75.233:465
(tcp)://101[.]99.75.233:8080
(tcp)://101[.]99.92.100:80
(tcp)://101[.]99.92.100:8080
(tcp)://101[.]99.92.101:80
(tcp)://101[.]99.92.102:80
(tcp)://101[.]99.92.102:8080
(tcp)://101[.]99.92.103:80
(tcp)://101[.]99.92.104:80
(tcp)://101[.]99.92.104:8080
(tcp)://101[.]99.92.105:80
(tcp)://101[.]99.92.106:80
(tcp)://101[.]99.92.107:80
(tcp)://101[.]99.92.108:80
(tcp)://101[.]99.92.108:8080
(tcp)://101[.]99.92.110:8080
(tcp)://101[.]99.92.230:8080
(tcp)://101[.]99.92.252:8080
(tcp)://79[.]137.205.201:15666
101[.]99.75.140
101[.]99.75.142
101[.]99.75.145
101[.]99.75.147
101[.]99.75.148
101[.]99.75.156
101[.]99.75.159
101[.]99.75.233
101[.]99.92.100
101[.]99.92.101
101[.]99.92.102
101[.]99.92.103
101[.]99.92.104
101[.]99.92.105
101[.]99.92.106
101[.]99.92.107
101[.]99.92.108
101[.]99.92.110
```

```
101[.]99.92.230
101[.]99.92.252
79[.]137.205.201
journal@ndibk.gov.ua (скомпрометований обліковий запис)
kl@aten.ua (скомпрометований обліковий запис)
ms-service@ndibk.gov.ua (скомпрометований обліковий запис)
o.slavgorodska@bdf.gov.ua (скомпрометований обліковий запис)
petrochenko@ndibk.gov.ua (скомпрометований обліковий запис)
zakupivli@trnvk.gov.ua (скомпрометований обліковий запис)
```

Хостові:

```
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\VideoMagic.url
%LOCALAPPDATA%\MagicMedia Studios\A
%LOCALAPPDATA%\MagicMedia Studios\VideoMagic.js
%LOCALAPPDATA%\MagicMedia Studios\VideoMagic.pif
%LOCALAPPDATA%\MagicMedia Studios\VideoMagic.pif %LOCALAPPDATA%\MagicMedia Studios\A
cmd /k echo [InternetShortcut] > "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Program
```

Графічні зображення

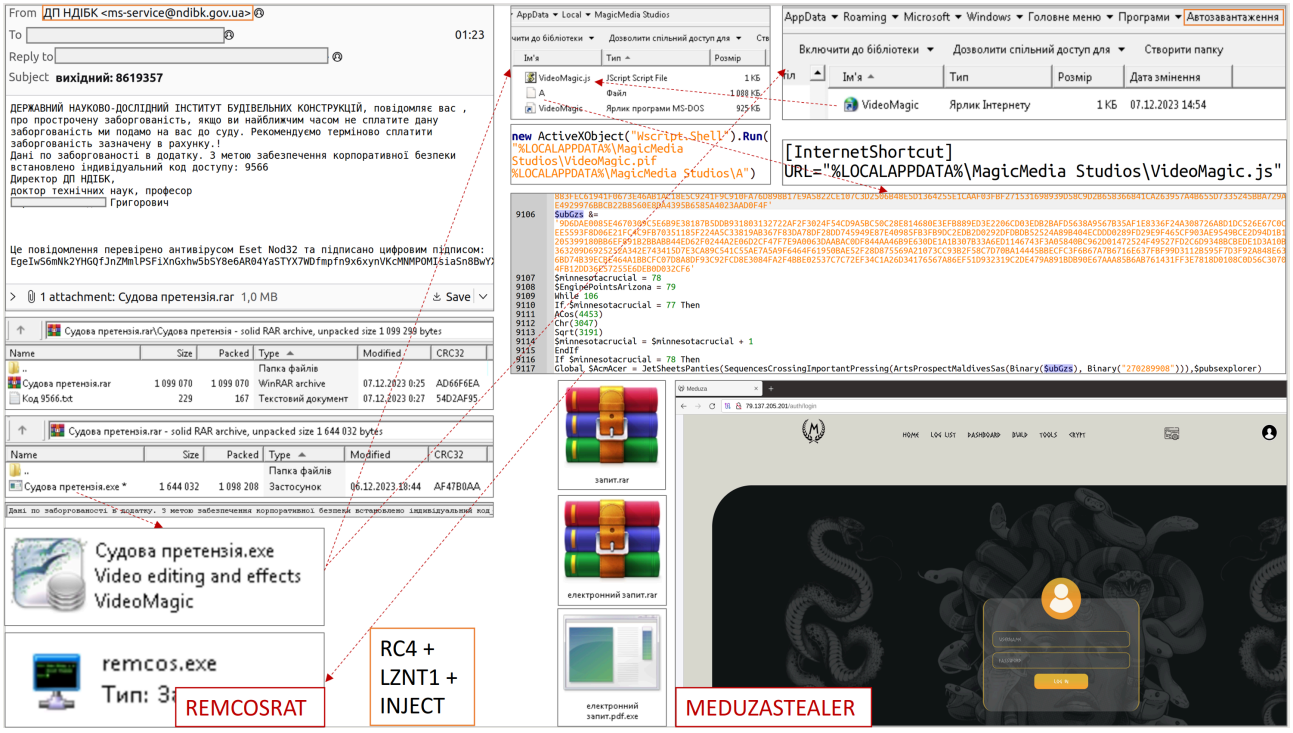

Рис.1 Приклад ланцюга ураження