Точковий сплеск активності UAC-0057 (CERT-UA#10340)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA у період з 12 по 18 липня 2024 року зафіксовано сплеск активності угрупування UAC-0057, що полягала в розповсюдженні документів з макросами, призначеними для запуску на ЕОМ шкідливої програми PICASSOLOADER з метою доставки на комп'ютер жертви Cobalt Strike Beacon.

Вміст виявлених файлів ("oborona.rar", "66_oborona_PURGED.xls", "trix.xls", "equipment_survey_regions_.xls", "accounts.xls", "spreadsheet.xls", "attachment.xls", "Податок_2024.xls") стосувався реформи органів місцевого самоврядування (проєкт USAID/DAI "HOVERLA"), оподаткування, а також тематики фінансово-економічних показників.

З огляду на зазначене доцільно припустити, що об'єктами зацікавленості UAC-0057 могли бути як фахівці проєктних офісів, так й їхні "контрагенти" з числа співробітників відповідних органів місцевого самоврядування України.

У випадку виявлення подібної активності просимо невідкладно інформувати CERT-UA.

Індикатори кіберзагроз

Файли:

```
f7d09dd6a214d5c5be9c17a833665d1f
313f2078fa0abb4452daa061ed98eccbfb956dfc76fdb6870cf9ec2a4b534f5a
313f2078fa0abb4452daa061ed98eccbfb956dfc76fdb6870cf9ec2a4b534f5a
3e25bf86d491cb4b7cd454c5aaaf8587
478c650401b6ea7d68f649fab17a8eb9581b81607b49e1cff0f61d65df29d1da
runbll32.dll
95fe77c5028c5713dac53efa97b50be1
72721f96599ab1191d2588e1a8001cc76f9bd8968fa4708dff153b1383b37aeb    mens-
freeze.html
2440bb07a338603b0b1f5fa4682c5ed4
9479ff59794cbf5f26996eb702f027e700bdbb13858463b7d2537a3fdff4af64
attachment.xls
363b9c08efb795a088694706fdc771c2
720df41451f9de8d863fce8c90310cd9f14dabe2519f98580c963784628eea55
spreadsheet.xls
1cc4bdaa3ef0f00a71bf74fb9c320694
d0dccd3a46392875b480c3666e2da62d12fdb0b4e5557185d4116344ed73110d
```

Loader.dll
07feb6b34198e1a8aec598e8dca8f42e
912e8f6d71d556c6def42cb01e8c17e7bd6e46bd3f90eba0c8e8f83937d362f0
ResetEngine.dll
235ddb7a47a2733b36ac7e312590548b
e32f016fe347dd29e263c026c680b9044dcf75340b6fa72b43f1a73a4d7605cf
CobaltStrikeBeacon.shellcode
db6030e4845eb8aa76f5a1803f95ca56
042de780112ef6d50b37a3f57e5a8f1e9910ad986fbba984be8fea3a18f39d59
virus_12.07.2024.rar
8fbc386b46ab18f35564536e7e6b3b68
2feb0bc8dec293ac19246cc0ecc05a1bc606ddac9aa57e677ade4cfac4e94d20
equipment_survey_regions_.xls
7ab58eb9b1c6b6e43a8606b9785d7352
7f29c3ea5b8fbd8b8ab6f7b508b6f8b6fa68fdebfec928f57f203bdef63b1c08
accounts.xls
618c22c74c0bfa60b7232751f90ddc2d
eca4273d922a66eb943a4bd1fd73ee4bd196289e32fe629cfe4ecf99e4cfadd3
eca4273d922a66eb943a4bd1fd73ee4bd196289e32fe629cfe4ecf99e4cfadd3
c98afaa61bc1a9a985e679b273509912
02d15669996853594424e5e7f957e12b2042b7775535bd2160953b4e84bb61cd
66_oborona_PURGED.xls
1ff1d1f4a91704cf011019c772801e8a
8932a95c10b088874bfb3471c352d2a7d64757ce77b226f19133301c481d9d03
accounts.xls
5799bccc0140492483ac53354f29577d
b7ef3c08cea0c50a43a7e3904f386189bd92f5da2920f026febc9f42c4de109d
b7ef3c08cea0c50a43a7e3904f386189bd92f5da2920f026febc9f42c4de109d
59a5ac6c2dc0ec90966e2064962e4fd6
22ba7234715ec7d99656fc6e16c2d75cbb5465c0fb2e5063c6d02baa4837a602
22ba7234715ec7d99656fc6e16c2d75cbb5465c0fb2e5063c6d02baa4837a602
0990df4c6805f1ababcc17eb4640395c
eaf3fd4dd5f6ea621ddc1bbccd5626cfa47bd3f8370c254866d9540dfda24374
eaf3fd4dd5f6ea621ddc1bbccd5626cfa47bd3f8370c254866d9540dfda24374
e32c23f357514d18c398ba393b74b603
bea3df5f788e60d324f1623a4328dafd9eaa6bb01d0a93343176def708bc002f
bea3df5f788e60d324f1623a4328dafd9eaa6bb01d0a93343176def708bc002f
9c498e1a3f5cb89f236c8b8fe9274d2c
e89612f017334f1bea536095abda92ded478a56ea4dce5e293222ce99a3e0c91
e89612f017334f1bea536095abda92ded478a56ea4dce5e293222ce99a3e0c91
e5b36154cd6c6c013633af2b64aecaa8
d8aba4e6904e03daac2c154a1b6b6a9ebe351e4af9b59b44a8ed442f4e67abcf
spreadsheet.xls
ef5b01f2c5800b29d67560a84c41a832

027e50b96e1683f22c448f9c7157f518d7d8f887c22862df3837fcfee558a6f2 trix.xls
2f61b89c56bdc5fa3818bcb2ebf23d34
f4a434dd2ac33ffe67575a61c1048d8c9c7f75363727dae9af578a943e9e512a trix.xls
1fd4b7f97551c1df0403b2c7280b8bd9
a032348d09c21894b14e9accee0bfd4a14b9dfda6f113cfc1476f45bec500135
attachment.xls
6908e1c1616271efba5b7c811b998c76
2b3617ae3fb743eaf604d0d3d36b68cf249dbeb180f06c8d0f3d60ccc3cc4b43
ruhbll32.dll
36b293e93b9b3fd4aaa98de8ab31d244
5f590fbd8307c7568737b62379a1fc0559308c7f29cb31920aa64097ffc0ca56
spreadsheet.xls
1724a8b1abb30612eceeb983809a3945
9a5a37b16350da20f86553df67eb7edf2142e1d36da1fcf99cacc6a74cc03730
9a5a37b16350da20f86553df67eb7edf2142e1d36da1fcf99cacc6a74cc03730
7fb55ab462fbcbd218682f1386ed94d4
411f088c3f997fdddec7a3b153d9526bd2d2d7c55ea25bae32d7b41f36514e04
411f088c3f997fdddec7a3b153d9526bd2d2d7c55ea25bae32d7b41f36514e04
86ab1d8dff4c828f232ff848ff497610
b1997a5bb5da44e05e05935ebe79d44f11358b8d8da7d4a99ad3e0367b5c567e trix2.xls
7bbc1d438ddb10a6b0893dc9a53aa868
ce5481496b58ef0bdf43d650bc8b70db5a2e03b1f8f42e30002bc95d9be8fe03 trix.xls
4218f95313a57ea6173bd8590f9a5c50
2cde8de330a874020340f2110bd1fd013fab7e93ef884c9006a646b49b567a75
Податок_2024.xls
47de94cd457149fac309abdd1c48d1bd
d7edb2ef6e95cbd77368ba5f5644d67c4de23feea9336bd324146b8abd63eab1
ruhbll32.dll
06faea7df39635f60feab8eaf663589c
b2434817428c6e38e435343db0d758498ba73952703c9d835f8ba62cbd36763d
b2434817428c6e38e435343db0d758498ba73952703c9d835f8ba62cbd36763d
fef3d4c960f97c113762e1b9f253c3ca
67e282aeadd040e14519a3755e526228a0e91472520728d258568cf61e68097f
accounts.xls
9d83e1af2727e271261fd5f31a966f9f
51f6b8dfcbe757f5df935203369da894c45727028d972b1207e449d0a592f7e2
51f6b8dfcbe757f5df935203369da894c45727028d972b1207e449d0a592f7e2
a6d1d556cd53d1ccd01a7ad3fd496a39
a7694687ac179a48f07d306ed1b08cd60e9aa7063ee91ab64b0a50ddd7371378
a7694687ac179a48f07d306ed1b08cd60e9aa7063ee91ab64b0a50ddd7371378
edb6cfca036c1a183d532fe78f1e23e0
477c198d257a738c945a866b176d9ecf922e3145f86f26154065818be5623fd5
477c198d257a738c945a866b176d9ecf922e3145f86f26154065818be5623fd5
8d6948d9e974d8f513e398713dfd6398

```
4a00b428a6513ea69a7185903f773bf8008e862ac295be86ef26536001ba17ef
accounts2.xls
d350a490f31df7a6efb86b2403a5d8e9
651e551854a4d949c4168efd6ae374f20e7951ad09fbea0e7d03456072644a99    trix2.xls
52cab62df14c0ea5f5532283ea2376a4
22af576e3c9ff82d2ddf45701e9f0db5ec6320ab9837d39d5d9d76d15a084f16    trix.xls
```

Мережеві:

```
backstagemerch[.]shop
empoweringparents[.]shop
lauramcinerney[.]shop
hXXps://backstagemerch[.]shop/the-simpsons/mens-freeze.html
hXXps://empoweringparents[.]shop/voorraad/hyundai/ioniq-6
hXXps://empoweringparents[.]shop/voorraad/peugeot/408
hXXps://lauramcinerney[.]shop/a-cumulatively-effective-way-of-dealing-with-
worries.html
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 Safari/537.36
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/98.0.4758.80 Safari/537.36 Edg/98.0.1108.62

backstagemerch.shop
empoweringparents.shop
lauramcinerney.shop
https://backstagemerch.shop/the-simpsons/mens-freeze.html
https://empoweringparents.shop/voorraad/hyundai/ioniq-6
https://empoweringparents.shop/voorraad/peugeot/408
https://lauramcinerney.shop/a-cumulatively-effective-way-of-dealing-with-
worries.html
```

Хостові:

```
%APPDATA%\Microsoft\runbll32.dll
%AppData%\Microsoft\ruhbll32.dll
%ProgramData%\Windows\Containers\BaseImages\a9cr29d6-89e4-430a-b193-
b23aba9bd6df\Files\Windows\System32\ResetEngine.dll
System service    (запланованe завдання)
```

Графічні зображення

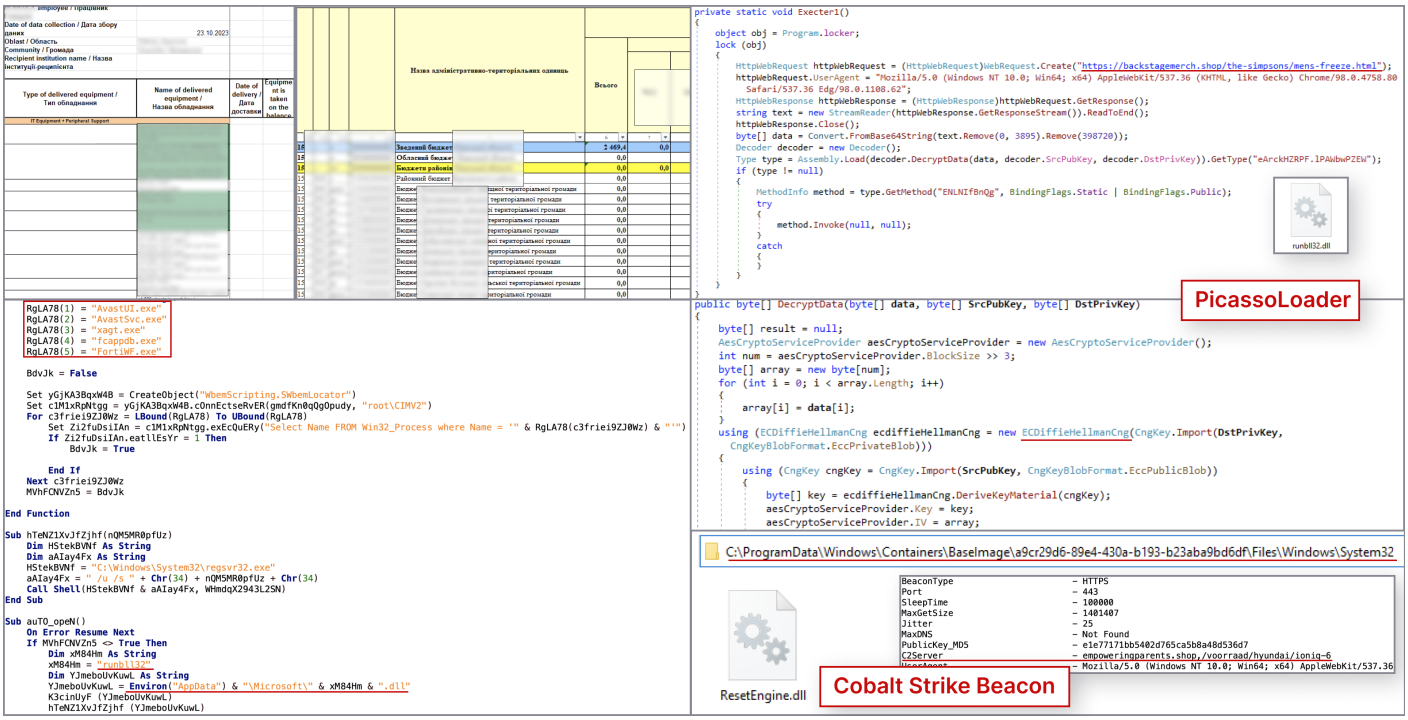

Рис.1 Приклад ланцюга ураження