CERT-UA

Archived: 2026-04-05 19:03:35 UTC

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA від суб’єкту координації (Кіберцентр Державної прикордонної служби України) отримано інформацію щодо розповсюдження, начебто, від імені ДП «Адміністрація морських портів України», електронних поштових повідомлень із вкладенням у вигляді RAR-архіву «порти APK.rar».

Згаданий RAR-архів містить шкідливі DOCX-документи «Щодо заходження суден під іноземним прапором в порти АР Крим на 27.01.2022.docx» і «Щодо заходження суден під державним прапором в порти АР Крим на 27.01.2022.docx», кожен з яких, у свою чергу, містить вбудовану URL-адресу.

У разі відкриття документів буде завантажено і відкрито DOC-файл з макросом. Останній забезпечить виконання шкідливого VBA-коду, що призведе до ураження комп’ютера шкідливою програмою GammaLoad.

Атаку асоційовано з діяльністю групи Armageddon (відслідковується CERT-UA за ідентифікатором UAC-0010).

Індикатори компрометації

Файли:

```
9fe8203b06c899d15cb20d2497103dbb        порти APK.rar
178b0739ac2668910277cbf13f6386e8        Щодо заходження суден під  державним прапором в порти
fd4de6bb19fac13487ea72d938999fbd        Щодо заходження суден під  іноземним прапором в порти
8644a34af1bf278d4cbe28022f77fd69        derg.gif
```

Мережеві:

```
hxxp://surname192.temp.swtest[.]ru/prapor/su/derg.gif
hxxp://surname192.temp.swtest[.]ru/prapor/su/ino.gif
hxxp://<IP-адреса>/concession.mot
surname192.temp.swtest[.]ru
coagula[.]online
tortunas[.]ru
phymateus[.]online
stopcovid@email[.]cz
```

Хостові:

```
%USERPROFILE%\Downloads\<назва_файлу>.exe
```

Додаткова інформація

GammaLoad – шкідлива програма, розроблена з використанням мови програмування VB Script; основний функціонал – ідентифікація комп’ютера (визначення %COMPUTERNAME% і %SYSTEMDRIVE%) і подальше завантаження та запуск додаткових шкідливих програм. Персистентність забезпечується за допомогою запланованого завдання (Scheduled Task).

Графічні зображення

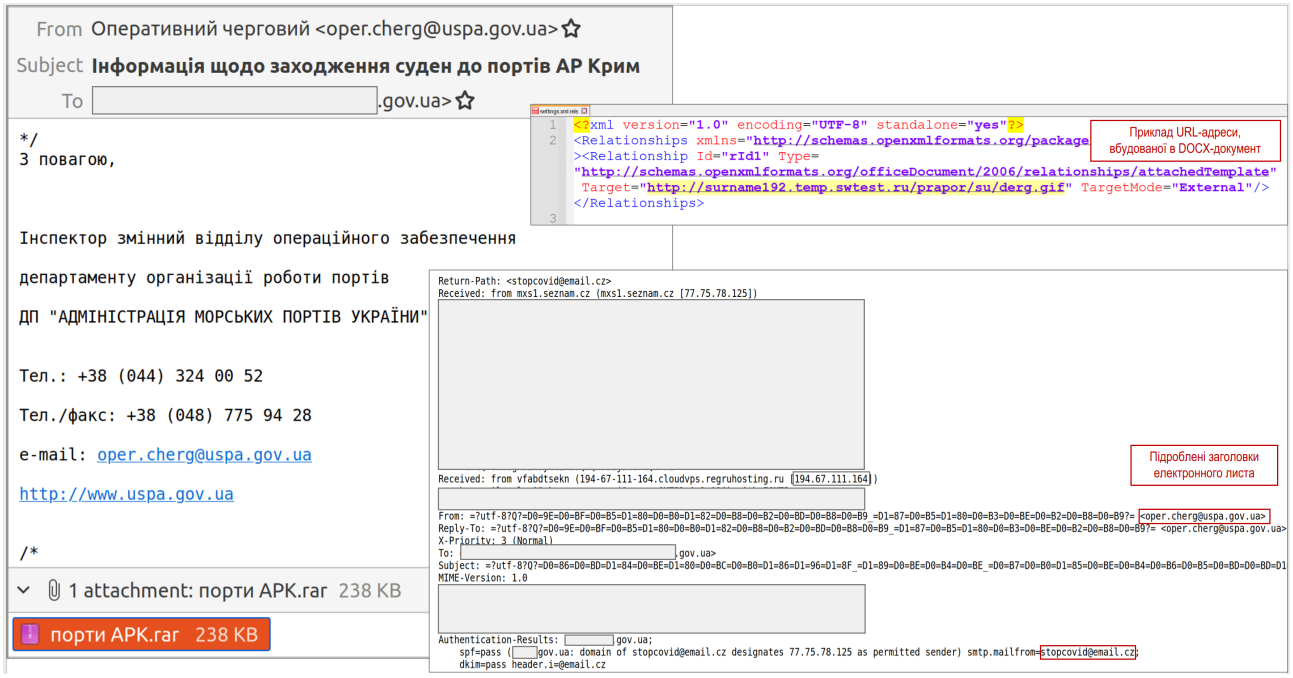

Рис. 1 Приклад шкідливого електронного листа та вбудованої URL-адреси

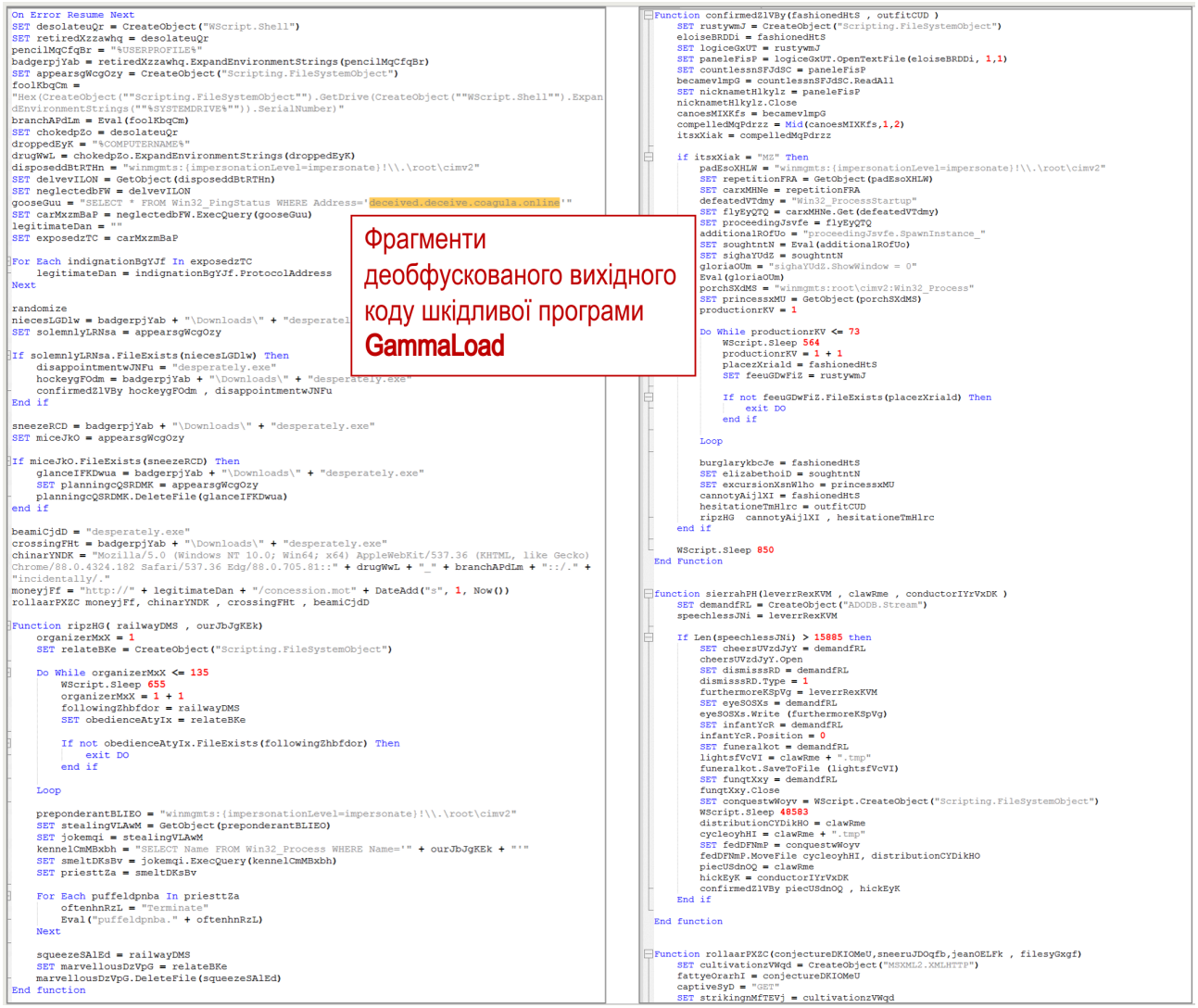

Рис. 2 Приклад програмного коду шкідливої програми GammaLoad

Source: https://cert.gov.ua/article/18365