Кібератака на державні організації з використанням тематики іранських дронів-камікадзе Shahed-136 та шкідливої програми DolphinCape (CERT-UA#5683)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA 08.12.2022 від фахівців підрозділу кібербезпеки АТ "Укрзалізниця" отримано інформацію щодо розсилання електронних листів з темою "Як розпізнати дрон-камікадзе." з адреси "morgunov.a@dsns.com[.]ua", начебто, від імені Державної служби України з надзвичайних ситуацій. Для цього, серед іншого, 08.11.2022 зареєстровано відповідне доменне імя.

У вкладенні до листа знаходиться RAR-архів "shahed-136.rar", що містить PPSX-документ "shahed.ppsx", який, у свою чергу, містить VBScript-код, призначений для створення запланованого завдання, а також дешифрування, створення на ЕОМ та запуску PowerShell-скрипта. При цьому, криптографічне перетворення даних здійснюється за допомогою алгоритму RC4, а в якості ключа виступає рядок, що є результатом конкатенації значення властивості "Manager" та назви документу ("Трігубенко Сергій Георгійович|shahed.ppsx").

Згаданий PowerShell-скрипт за допомогою командлету BitsTransfer (Background Intelligent Transfer Management) здійснить завантаження виконуваних файлів "WibuCm32.dll", "CodeMeter.exe" (легітимна програма), а також створення запланованого завдання для запуску останнього. При цьому, буде використана техніка DLL Side-Loading.

Файл "WibuCm32.dll" класифіковано як шкідливу програму DolphinCape, що розроблена з використанням мови програмування Delphi та основним функціоналом якої є збір інформації про ЕОМ (ім'я хоста, ім'я користувача, розрядність, версія ОС, значення змінних середовища), запуск EXE/DLL файлів, відображення списку файлів та їх вивантаження, а також створення та ексфільтрація знімків екрану.

Активність відстежується за ідентифікатором UAC-0140.

Індикатори компрометації

Файли:

```
247997c2b4431585f9355d3324410298
460244cbf353b15b52c69952dd3b2549de79c590c56807bc25d4896dd0016655    shahed-136.rar
241e4285a84be65cf16778462f06b9a8
5137a888271b08f388d863433e5f0f1b129e15d4c812b95c831e93e27ec45bd6
```

```
shahed.ppsx
3444e86aefa7bc2dbce34903f805400d
6ee62645cd97fb0b41fdf219b9a2a8211324ded110b5c7f09b3d9881abb2a594
SearchEmbdIndex.ps1
142893c48b76b7e9d0f7ce74e16aaf1f
2c1a2fe3fb418601f3adc9256e1ff2c509178483fdbb0e964f52fb6b30be1129
CodeMeter.exe
98c3d5347842743bfb4ade50b39226c1
772654b186ad9fbd0a80f03ceae7d327b45c8944452cc39048160b1f6d8f2672
WibuCm32.dll    (2022-09-24 06:09:32) (DolphinCape)
```

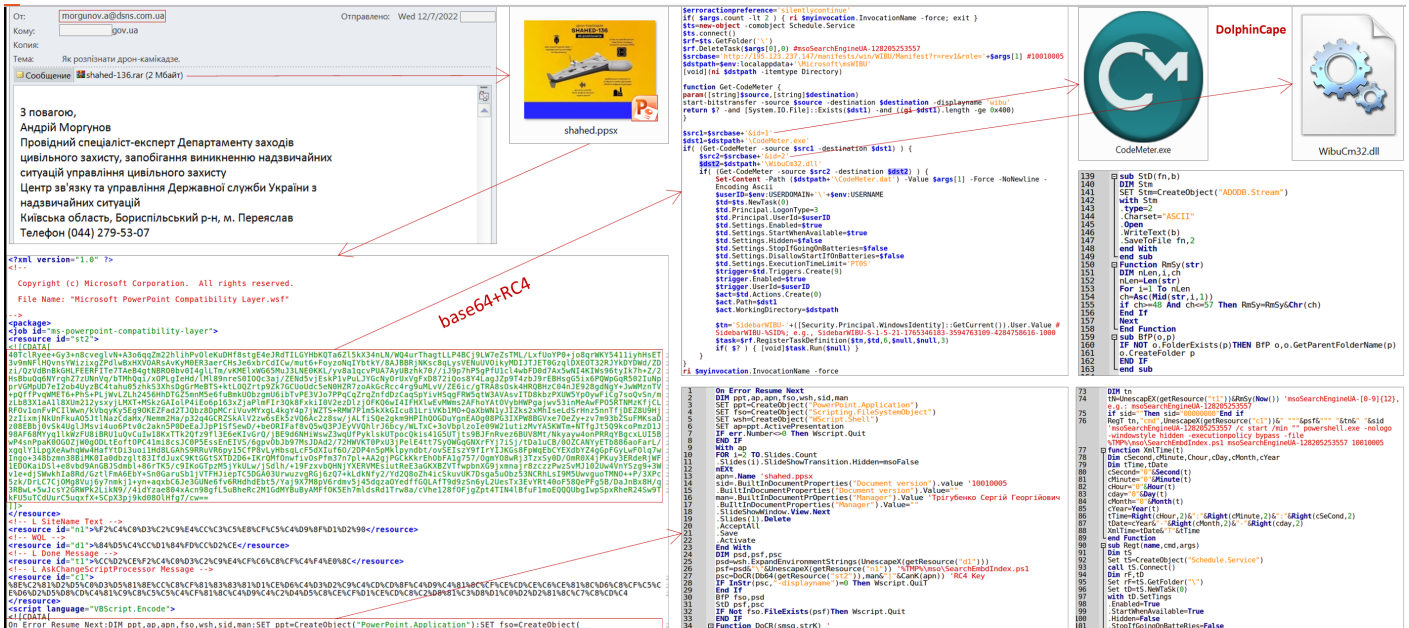
Мережеві:

```
morgunov.a@dsns.com.ua
195[.]123.237.147
202[.]157.187.190
Mozilla/3.0 (compatible; Indy Library)
dsns.com[.]ua
hXXp://195[.]123.237.147/manifests/win/WIBU/Manifest?r=rev1&role=
hXXp://202[.]157.187.190/cgi-
bin/rarcheckcert[.]cgi/http/20221208011644645.stc
".cda|.cda|.stk|.stc|.stt|.stf" (суфікси URI)
```

Хостові:

```
%LOCALAPPDATA%\Microsoft\msWIBU\
%LOCALAPPDATA%\Microsoft\msWIBU\CodeMeter.dat
%LOCALAPPDATA%\Microsoft\msWIBU\CodeMeter.exe
%LOCALAPPDATA%\Microsoft\msWIBU\WibuCm32.dll
%TMP%\mso\SearchEmbdIndex.ps1
{CVS_87963304_MN.0.3.4_227e} (M'ютекс)
SidebarWIBU- (частина назви запланованого завдання)
msoSearchEngineUA- (частина назви запланованого завдання)
```

Графічні зображення


base64+RC4
DolphinCape
shahed.ppsx
CodeMeter.exe
WibuCm32.dll