CERT-UA

cert.gov.ua/article/37626

general information

The government team for responding to computer emergencies in Ukraine CERT-UA found the file "dovidka.zip", which contains the contextual help file (Microsoft Compiled HTML Help) "dovidka.chm". The mentioned CHM-file, in turn, contains the bait image "image.jpg" (information on the procedure for frequent artillery shelling) and HTA-file "file.htm" with malicious code in VBScript. Execution of the latter will lead to the creation on the computer and run the dropper "ignit.vbs", which will decode the .NET loader "core.dll", as well as files "desktop.ini" (run "core.dll" using regasm .exe) and "Windows Prefetch.lNk", which provides the launch of the previously mentioned "desktop.ini" using wscript.exe.

Finally, the .NET loader will decode and execute the MicroBackdoor malware. Note that the compilation dates of backdoor and loader are 28.01.2022 and 31.01.2022, respectively; in addition, the domain used by the management server was created on 12.01.2022. It should be added that in addition to the standard commands ("id", "info", "ping", "exit", "upd", "uninst", "exec", "shell", "flist", "fget", "fput "), this version of the backdoor additionally implements the" screenshot "command.

The activity is associated with the activities of the UAC-0051 group, also known as unc1151 (according to Mandiant).

Indicators of compromise

Files:

```
e34d6387d3ab063b0d926ac1fca8c4c4 reference.zip
2556a9e1d5e9874171f51620e5c5e09a dovidka.chm
bc6932a0479045b2e60896567a37a36c file.htm
bd65d0d59f6127b28f0af8a7f2619588  ignit.vbs
fb418bb5bd3e592651d0a4f9ae668962  Windows Prefetch.lNk
a9dcaf1c709f96bc125c8d1262bac4b6  desktop.ini
d2a795af12e937eb8a89d470a96f15a5  core.dll (.NET-лоадер)
65237e705e842da0a891c222e57fe095  microbackdoor.dll (MicroBackdoor)
```

Мережеві:

```
xbeta[.]online:8443
185[.]175.158.27
```

Хостові:

```
%PUBLIC%\ignit.vbs
%PUBLIC%\Favorites\desktop.ini
%PUBLIC%\Libraries\core.dll
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Windows Prefetch.lNk
wscript.exe //B //E:vbs C:\Users\Public\Favorites\desktop.ini
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U
C:\Users\Public\Libraries\core.dll
```

Додаткова інформація

MicroBackdoor is a publicly available backdoor program developed using the C ++ programming language. Author: cr4sh (aka Dmytro Oleksiuk). Functional: id, info, ping, exit, upd, uninst, exec, shell, flist, fget, fput, screenshot (implemented separately by members of the group UAC-0051 / unc1151). The server part is designed using the Python programming language and provides a simple web interface for managing bots. Persistence: Run Windows Registry Key. Communication between the bot and the server is encrypted using RC4.

Graphic images

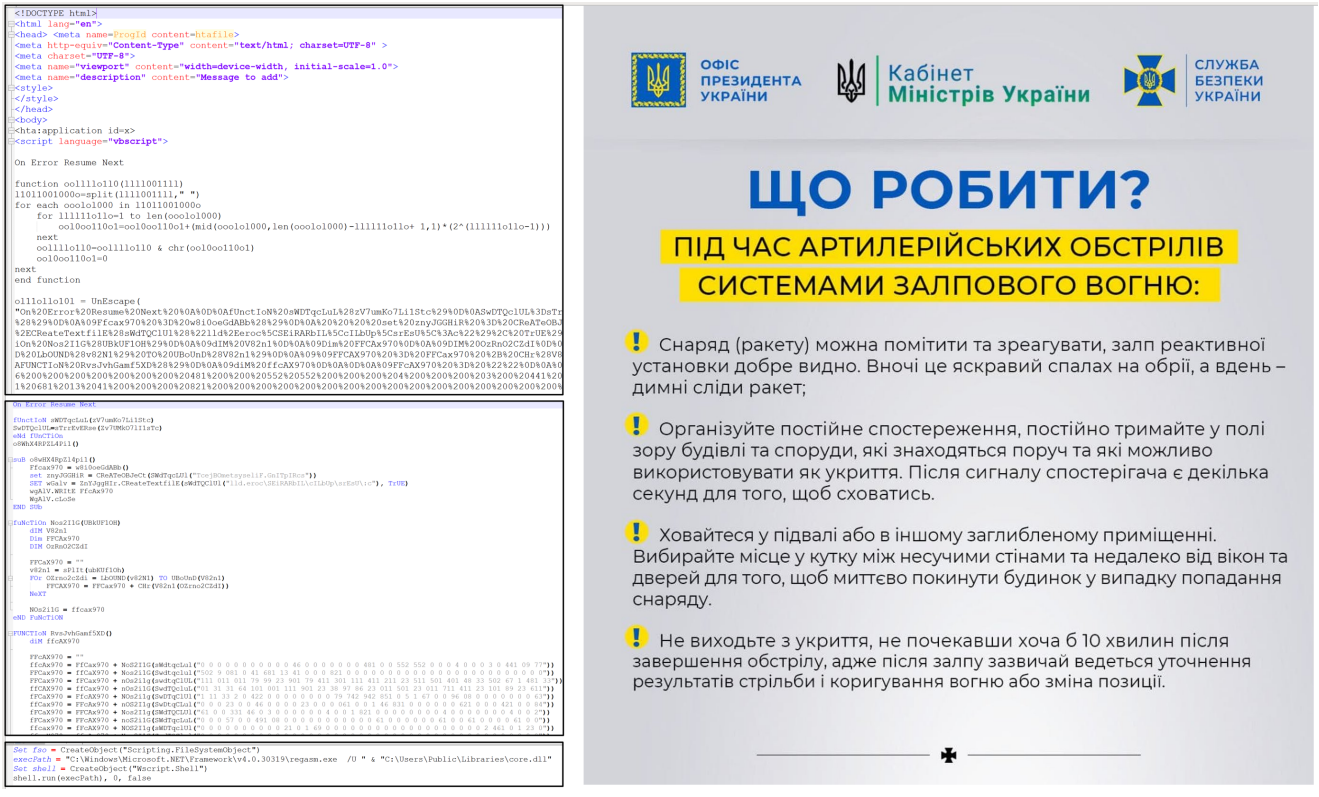

Fig. 1 Example of malicious files and image baits