CERT-UA

cert.gov.ua/article/37626

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA виявлено файл "довідка.zip", який містить файл контекстної довідки (Microsoft Compiled HTML Help) "dovidka.chm". Згаданий CHM-файл, у свою чергу, містить зображення-приманку "image.jpg" (довідка про порядок дій під част артилерійських обстрілів) та HTA-файл "file.htm" зі шкідливим програмним кодом на мові VBScript. Виконання останнього призведе до створення на комп'ютері і запуску дропера "ignit.vbs", який забезпечить декодування .NET-лоадеру "core.dll", а також файлів "desktop.ini" (виконує запуск "core.dll" за допомогою regasm.exe) і "Windows Prefetch.lNk", який забезпечує запуск раніше згаданого "desktop.ini" за допомогою wscript.exe.

Насамкінець, .NET-лоадер здійснить декодування і виконання шкідливої програми MicroBackdoor. Зауважимо, що дати компіляції бекдору та лоадеру - 28.01.2022 і 31.01.2022, відповідно; крім того, домен, що використовується сервером управління, створено 12.01.2022. Слід додати, що окрім стандартних команд ("id", "info", "ping", "exit", "upd", "uninst", "exec", "shell", "flist", "fget", "fput"), в цій версії бекдору додатково реалізовано команду "screenshot".

Активність асоційовано з діяльністю групи UAC-0051, також відомою як unc1151 (за даними Mandiant).

Індикатори компрометації

Файли:

```
e34d6387d3ab063b0d926ac1fca8c4c4  довідка.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 - публічно доступна програма-бекдор, розроблена з використанням мови програмування C++. Автор: cr4sh (aka Dmytro Oleksiuk). Функціонал: id, info, ping, exit, upd, uninst, exec, shell, flist, fget, fput, screenshot (реалізовано окремо членами групи UAC-0051/unc1151). Серверна частина розроблена з використанням мови програмування Python та надає простий веб-інтерфейс для управління ботами. Персистентність: ключ Run реєстру Windows. Комунікація між ботом та сервером зашифрована за допомогою RC4.

Графічні зображення

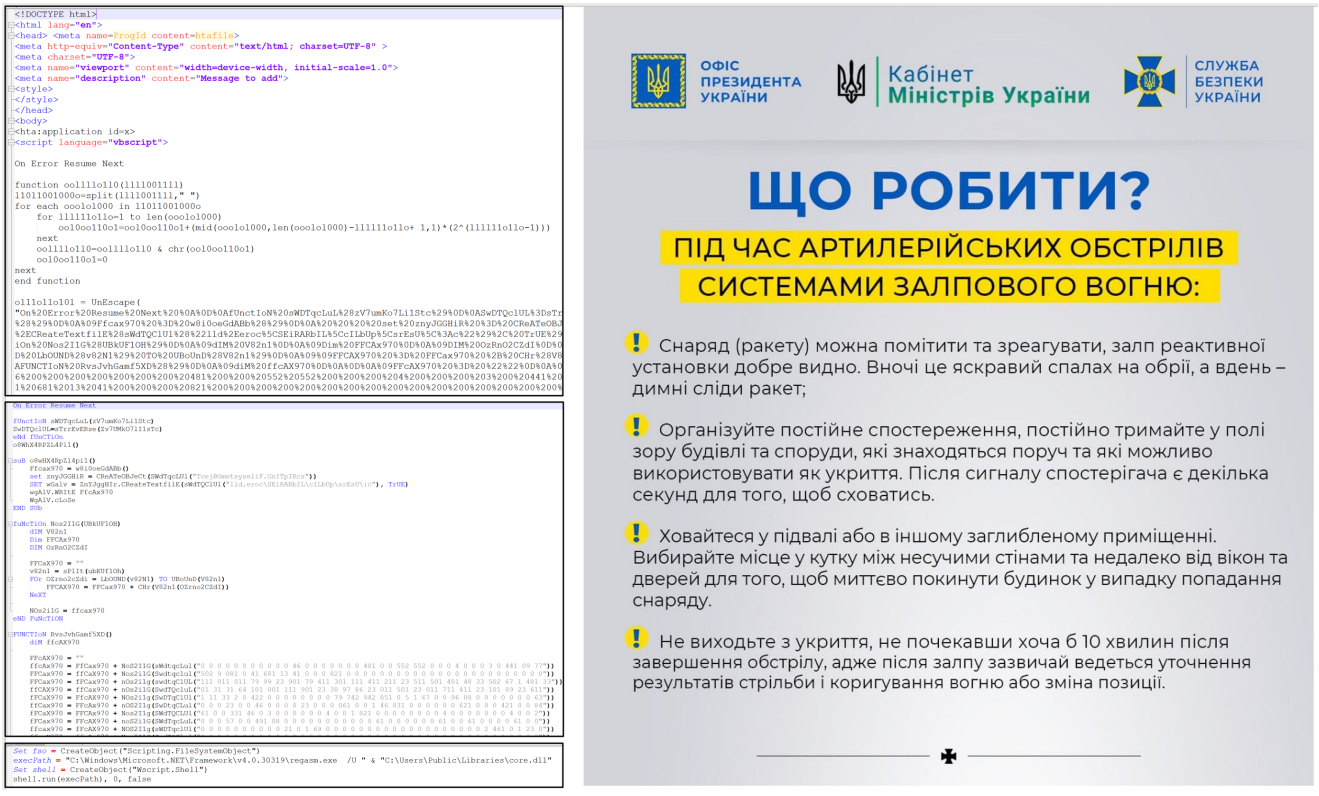

Рис. 1 Приклад шкідливих файлів та зображення-приманки

Попередня

Вразливості в Zabbix (CVE-2022-23131, CVE-2022-23134)