

CERT-UA

Archived: 2026-04-05 16:02:49 UTC

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 СНМ-файл, у свою чергу, містить зображення-приманку "image.jpg" (довідка про порядок дій під час артилерійських обстрілів) та НТА-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 ладеру - 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-0057, 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:

