CERT-UA

Archived: 2026-04-05 15:41:21 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено XLS-документи "PerekazF173_04072023.xls" та "Rahunok_05072023.xls", що містять як легітимний макрос, так і макрос, який здійснить декодування, забезпечення персистентності та запуск шкідливої програми **PicassoLoader**.

При цьому, окремо реалізовано перевірку встановленого засобу захисту: у випадку, якщо на ЕОМ виявлено продукти Avast, FireEye, Fortinet (назви процесів: "AvastUI.exe", "AvastSvc.exe", "xagt.exe", "fcappdb.exe", "FortiWF.exe") шкідливу програму створено не буде.

На момент дослідження PicassoLoader забезпечував завантаження, дешифрування (AES) та запуск шкідливої програми njRAT.

Активність здійснюється угрупуванням UAC-0057.

Принагідно інформуємо, що "GhostWriter" є назвою інформаційної операції, що була проведена угрупуванням UNC1151 (UAC-0057) про яку публічно інформувала компанія Mandiant у 2020 році [1]. Проте, для спрощення сприйняття в інформаційних повідомленнях CERT-UA назва "GhostWriter" може ототожнюватися із назвою/ідентифікатором загрози UAC-0057.

Індикатори кіберзагроз

Файли:

```
6e6c39f498d0231417f6fa75e27b3008    4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65
6857da89a25728b066dcf7f47d25455b    0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32
f09420169a24a54eff0fc35cd15d68bc    7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
4e23e56fb247e92980331ca23a1b7300    6dd40ea5e53754a7160801aa5e378089c7dcd9b76429c2536d115c022e3484e8
c0dc96834b07ec32bc67d3bce7b60a28    3b7702a3c2434f8677dddcd44b8ab09bd23129df98ce76929d5731d156398c32
5bf951438305f16e42f6a85b81d6c5d7    b27ec1a0d4e122765abbecc5e66742f4ed546adfda208b4320fbf277d37a38f5
192e12e92dd0fe7a838e104eb65665ef    97894351c3c0728f3c2c740b0ea60af7bd9db955f2d3dc1a97668227956c89f3
552d020c3c090c7b297a8f23f7c48648    4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829
6857da89a25728b066dcf7f47d25455b    0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32
f09420169a24a54eff0fc35cd15d68bc    7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
a85c94825f1420dd15cd80851e89efb1    5061bf0d671aacb5fc8e89918c6e5dc5e0b8cb14020422ca73ca5941a7f34b98
4d8bc51e52067f4b983e4f60d5618a15    7f89ec40687564ad7bae34c3f9cddcea28624b3ecf4807e3cef9911d850aecf8
1d3f26e8b8f0a145d752bc089e5904e5    32cf2acd3300d5c0cf7aadc70f07d137d705f379e35510e25018578e3ee40f42
d43e0c177c7de3d311706609fecdabb8    1de7d03db87618e20b85c4e30e040168f26e4a0bdc98943736ef9a2c5f648e23
```

```
4f173e82336aec538124bc1f6a8435b2    52fe07167694935a5a6441c1e6de73b08f786f736057034de766a7fa3866e576
f09420169a24a54eff0fc35cd15d68bc    7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
```

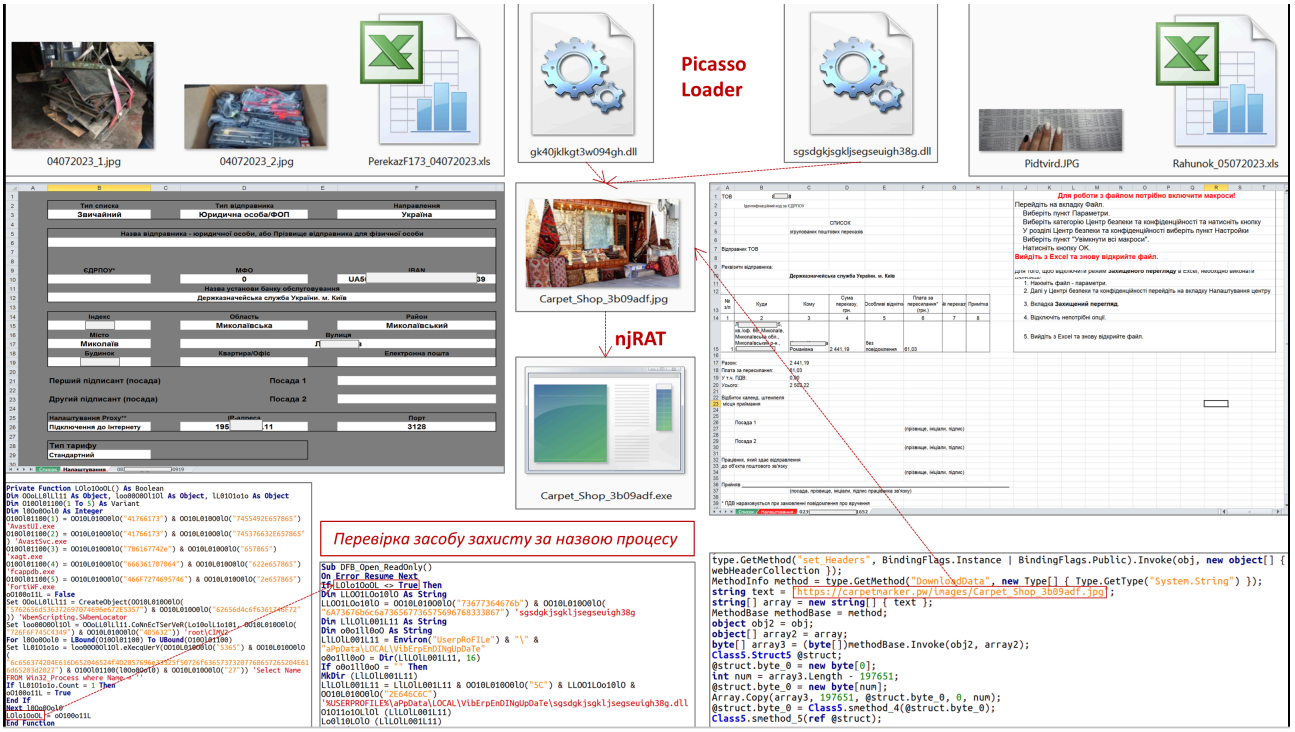
Хостові:

```
%APPDATA%\Microsoft\Windows\Start Menu\ADhk GKs h09k.lnk
%APPDATA%\Microsoft\Windows\Start Menu\Ganmk2 Gk3o ADk30.lnk
%LOCALAPPDATA%\VibErpEnDINgUpDaTe\sgsdgkjsgkljsegseuigh38g.dll
%LOCALAPPDATA%\WhatsAppPendingUpdate\gk40jklkgt3w094gh.dll
%WINDIR%\System32\rundll32.exe %LOCALAPPDATA%\WhatsAppPendingUpdate\gk40jklkgt3w094gh.dll,IETracking
%WINDIR%\System32\rundll32.exe %LOCALAPPDATA%\viberpendingupdate\sgsdgkjsgkljsegseuigh38g.dll,IETrac
RunDLL32.EXE shell32.dll,ShellExec_RunDLL "%APPDATA%\Microsoft\Windows\Start Menu\ADhk GKs h09k.lnk"
RunDLL32.EXE shell32.dll,ShellExec_RunDLL "%APPDATA%\Microsoft\Windows\Start Menu\Ganmk2 Gk3o ADk30.
```

Мережеві:

```
(tcp)://everything-everywhere.at.ply[.]gg:50709
hXXps://carpetmarker[.]pw/images/carpet_shop_3b09adf.jpg
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.78.109.7
carpetmarker[.]pw
everything-everywhere.at.ply[.]gg
```

Графічні зображення



Посилання

[1] https://www.mandiant.com/resources/blog/ghostwriter-influence-campaign

Source: https://cert.gov.ua/article/5098518