Кібератака на державні організації України з використанням шкідливої програми RomCom. Можлива причетність Cuba Ransomware aka Tropical Scorpius aka UNC2596 (CERT-UA#5509)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA 21.10.2022 виявлено факт розповсюдження електронних листів, начебто, від імені Пресслужби Генштабу ЗСУ з посиланням на сторонній веб-ресурс для завантаження "наказу". На згаданій веб-сторінці розміщено повідомлення про необхідність оновлення програмного забезпечення (PDF Reader). У випадку натискання на кнопку "ЗАВАНТАЖЕННЯ" на комп'ютер буде завантажено виконуваний файл "AcroRdrDCx642200120169_uk_UA.exe".

Запуск згаданого файлу, в результаті, призведе до декодування та запуску файлу "rmtpak.dll". Останній класифіковано як шкідливу програму RomCom.

Зважаючи на використання бекдору RomCom, а також інші особливості пов'язаних файлів, вважаємо за можливе асоціювати виявлену активність з діяльністю групи Tropical Scorpius (Unit42) aka UNC2596 (Mandiant), що відповідальна за розповсюдження Cuba Ransomware; CERT-UA відстежує активність за ідентифікатором UAC-0132.

Індикатори компрометації

Файли:

```
62d99110a03c33157a2c844ed5ddec11
a2511c5c2839bfbdf9c0f84f415d5eae168456e5d3f77f1becdbcd69fba4daa4
Наказ_309.pdf
879a0684646a0fe6897b2b5637abaf8a
bd46cdd2f058697f7f13cfd958c2be9d132d72844c8d2cf1c76463087f785187
_309_002.pdf (документ-приманка)
32b4d8b58dde0bdc372dbb41a856c46c
c116a0aafdc2765e38b4f5efdf89960997abf0db81daa8f5380ce3c893e9af96
AcroRdrDCx642200120169_uk_UA.exe (2022-10-20 09:29:58)
05eaab1fb0ef4a9f22e9d21439e9bd90
03965aeccf475029ea06ff400b34dfd0e19bcf04403bfd539e11c60aaab11343
AcroRdrDCx642200120169_uk_UA_payload.exe (2022-10-21 08:25:02)
f31620e7e22a30f408e5d683922f5029
068117b406940ac510ed59efd1d7c7651f645a31bd70db6de16aba12c055aae6    VSSVC.exe
```

(2022-10-21 08:24:45)
5f5c18e98e5c8a5a50a1e122221f61dd
4fc9202ff84ef84b8c5e6140b66ac3d04570daf886a7f1ae31661ade882f963e
WinApp.dll (2022-10-21 08:23:22)
a785462b81ad66922c7128b0fe40b448
494b43198db467f506e9857f39ebe8f8bf6d871776eba092a7e2f2140046e16d
rmtpak.dll (2022-10-21 08:22:59) (RemCom)

Пов'язані файли:
(18.10.2022)
c78f9b945b91fee7b2d9d4d41e7dade5
59f0c3b7890f11217ad37764f225cd1c9d27747495d80dadde40b78edfbfa21e
PDFFiller.zip (2022-10-18 13:26:28)
6d7a47c27cf381cf386e311e6363020f
ac800a17dced2dcaa6be68dd0ac09e38b10c5e1c7ac0623bcb923cb17e447c55 setup.exe
(2022-10-18 13:26:28)
04972228302e569da856e4fa45f679ed
e80d80521238008bf6f429e072eaf6030c06e2d3123d03ea9b36f5a232a1ec90 hlpr.dat
(2022-10-18 13:25:16)
ef2483810ed58dbfee7568be65a48872
61e349518ca3f10d1e7aae0be95bc43dc23843c8acf177831cdfd48f26a07c72
rtmpak.dll (2022-10-18 13:24:33) (RemCom)
(12.10.2022)
f77af383bbec2e637e1d42efea742e8f
997e54360fdc3d45f8fb2612b2936394d20e8ae84a0dd073562ba9d6ea5825ad setup.exe
(2022-10-12 14:51:55)
(27.07.2022)
2896c334f4ef21aec24596ae13f9b692
3e3a7116eeadf99963077dc87680952cca87ff4fe60a552041a2def6b45cbeea
advancedipscanner.msi (2022-07-23 07:41:25)
f206e4c4c0b21ea47fb51d4f04c42d61
983833334d168cd4274467f48171489e019b86b51e687738565a93dd3f58d0aa
MSI9C7D.tmp (2022-07-27 10:18:38)
de239ac43508c4fd4c9069a9b6a4a3f8
05681ff7cae6b28f5714628a269caa5115da49c94737ce82ec09b4312e40fd26
combase32.dll (2022-07-27 10:17:34) (RemCom)
(20.07.2022)
3d9022126f8e43eb0e9d041b05c7fa54
892d7725d798a0bea0a80245057183dbf53dceb729985de2d1653316b72b3fde
Advanced_IP_Scanner_V2.5.4594.1.zip
e699ff001dad735130cca18d832442a3
f59b81fda6ba719cefa74145e15d7044fb9da1faa8f09ce912e83a8a7ae60bb6 setup.exe
(2022-07-20 16:25:03)
66ecb729fd1993d3f54e2e0936eb3515

28950cff484550312f2c91e17d7da89300981f17b19a7cd9c5432a4b76e281d2
instlib.dat (2022-07-20 16:25:03)
dba03c29dd6099af5aae7a1163a8fd5e
28b2a0f5441a5c50c73bb2044e48c7e404b848b84da9d1043771c783e17647d8 hlpr.dat
(2022-07-20 16:25:03)
2630e8d2216a99e91fd5247decba3127
64a4a5d818fa030b5f2c4e1babaee4c58d2677e9ef3a0ecf1d99070f186e041f
winver.dll (2022-07-20 12:14:14) (RemCom)
(16.09.2022)
74d9ecec3c02370b5606ab354893d7b3
4f4949f7203b1d0b93adfabde5ef9d86cd8921f8524534fb4f2c1d5cd5cd10b4
explore.exe (2022-09-13 13:53:34)
a5d08548d5a1d72f5c42dfd3275efe39
c149474f97140c3381bda3ad2451f253e08e7ad4be76a68ac3a6f15bc4bd4e63
a5d08548d5a1d72f5c42dfd3275efe39.dll (2022-09-16 07:00:55)
ef96b8c7139d6014dc84a21b433f504a
40c29c2e691f28844092da318ef557f518b2e34b80529c4a12affad2e49958b0
combase32.dll (2022-09-16 07:00:34) (RemCom)
71d0715284a402aaf5dc2a1158d2188e
71b83ad71745cd7bf5a367694dbecff620367d9019c6baabbf794376360f9a06 a.exe
(2022-04-21 11:57:29) (cve-2022-24521)
4c1579c6a14bb8f3985be8a1a83c731c
f94998b90a28c678e4ed6bdf851f339e02a58369435b20ad62858e0ea5bc8eba
winrun.exe (2022-04-21 11:57:29) (cve-2022-24521)

Мережеві:

45[.]158.38.74 (Received)
45[.]87.155.99 (@stark-industries.solutions)
69[.]49.231.103
hXXp://notfiled[.]com:4444/
hXXps://www.get.adobe.com.aspx[.]io/reader/download.php
hXXps://gov.mil.ua.aspx[.]io/mail/attachment/Наказ_309.pdf
www.get.adobe.com.aspx[.]io
gov.mil.ua.aspx[.]io
mil.ua.aspx[.]io
ua.aspx[.]io
aspx[.]io (2022-10-15)
mill.co[.]ua (2022-10-14)
notfiled[.]com (2022-09-03)
WinHTTP Example/1.0 (User-Agent)
s.l.sinkewitch@ukr.net (електронна адреса відправника)

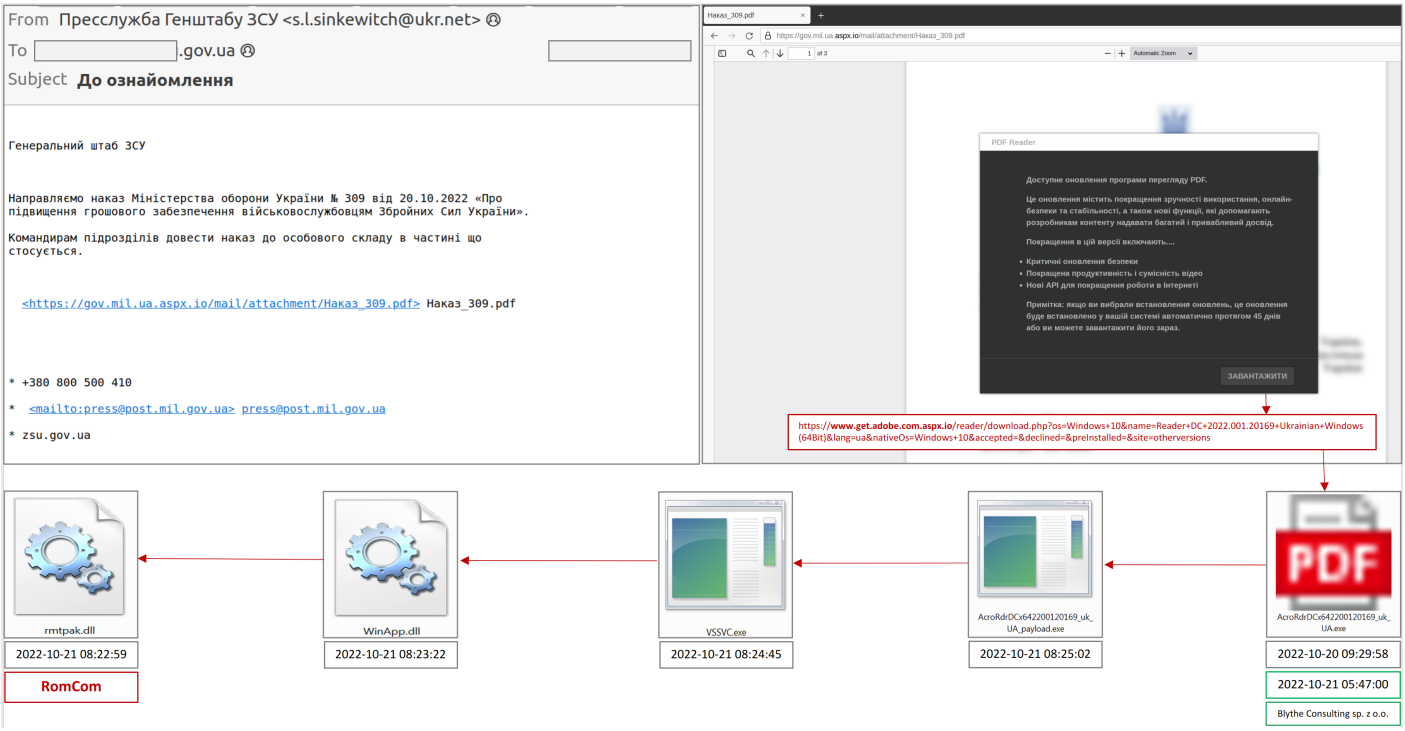
```
Пов'язані мережеві індикатори:
hXXp://advanced-ip-scanners[.]com/advancedipscanner.msi
hXXps://advanced-ip-scaner[.]com/download/
hXXp://combinedresidency[.]org:4444
hXXp://4qzm[.]com:4444
4qzm[.]com (2022-08-12)
combinedresidency[.]org (2022-02-28)
advanced-ip-scaner[.]com (2022-07-13)
advanced-ip-scanners[.]com (2022-07-20)
```

Хостові:

```
%PUBLIC%\Libraries\VSSVC.exe
%PUBLIC%\Libraries\WinApp.dll
%PUBLIC%\Libraries\rtmpak.dll
%PUBLIC%\Наказ_309.pdf
rundll32.exe %PUBLIC%\Libraries\WinApp.dll,fwdTst
Blythe Consulting sp. z o.o. (назва сертифікату для цифрового підпису)

Пов'язані хостові індикатори:
rundll32.exe hlpr.dat,fwdTst
C:\Users\123\source\repos\ins_asi\Win32\Release\setup.pdb (PDB-шлях)
C:\Users\123\source\repos\cve_2022_24521
(1)\CVE_2022_24521\x64\Release\CVE_2022_24521_clfs.pdb (PDB-шлях)
Wechapaisch Consulting & Construction Limited (назва сертифікату для
цифрового підпису)
```

Графічні зображення


From Пресслужба Генштабу ЗСУ <s.l.sinkewitch@ukr.net>
To .gov.ua
Subject До ознайомлення
Генеральний штаб ЗСУ
Направляємо наказ Міністерства оборони України № 309 від 20.10.2022 «Про підвищення грошового забезпечення військовослужбовцям Збройних Сил України».
Командирам підрозділів довести наказ до особового складу в частині що стосується.
<https://gov.mil.ua.aspx.io/mail/attachment/Наказ_309.pdf> Наказ_309.pdf
* +380 800 500 410
* <mailto:press@post.mil.gov.ua> press@post.mil.gov.ua
* zsu.gov.ua
Наказ_309.pdf
PDF Reader
Доступне оновлення програми перегляду PDF.
Це оновлення містить покращення зручності використання, онлайн-безпеки та стабільності, а також нові функції, які допомагають розробникам контенту надавати багатий і привабливий досвід.
Покращення в цій версії включають....
Критичні оновлення безпеки
Покращена продуктивність і сумісність відео
Нові API для покращення роботи в Інтернеті
Примітка: якщо ви вибрали встановлення оновлень, це оновлення буде встановлено у вашій системі автоматично протягом 45 днів або ви можете завантажити його зараз.
ЗАВАНТАЖИТИ
https://www.get.adobe.com.aspx.io/reader/download.php?os=Windows+10&name=Reader+DC+2022.001.20169+Ukrainian+Windows (64Bit)&lang=ua&nativeOs=Windows+10&accepted=&declined=&preInstalled=&site=otherversions
rmtpak.dll
2022-10-21 08:22:59
RomCom
WinApp.dll
2022-10-21 08:23:22
VSSVC.exe
2022-10-21 08:24:45
AcroRdrDCx642200120169_uk_UA_payload.exe
2022-10-21 08:25:02
AcroRdrDCx642200120169_uk_UA.exe
2022-10-20 09:29:58
2022-10-21 05:47:00
Blythe Consulting sp. z o.o.