Cyber attack by UAC-0010 (Armageddon) on state institutions of the European Union (CERT-UA # 4334)

General Information

At the end of March 2022, the Government Team for Response to Computer Emergencies of Ukraine CERT-UA discovered several RAR archives named "Assistance.rar", "Necessary_military_assistance.rar". Each of these archives contained malicious shortcut files entitled "List of necessary things for the provision of military humanitarian assistance to Ukraine.lnk", "Providing military humanitarian assistance to Ukraine.lnk". In addition, it was found that the method of delivery was e-mails with links to the mentioned RAR-archives.

The use of English in the names of the files and the text of the e-mail, as well as the fact that the letter was sent to the Latvian government, clearly indicates the UAC-0010 (Armageddon) attacks on government agencies in the European Union.

Indicators of compromise

Files:

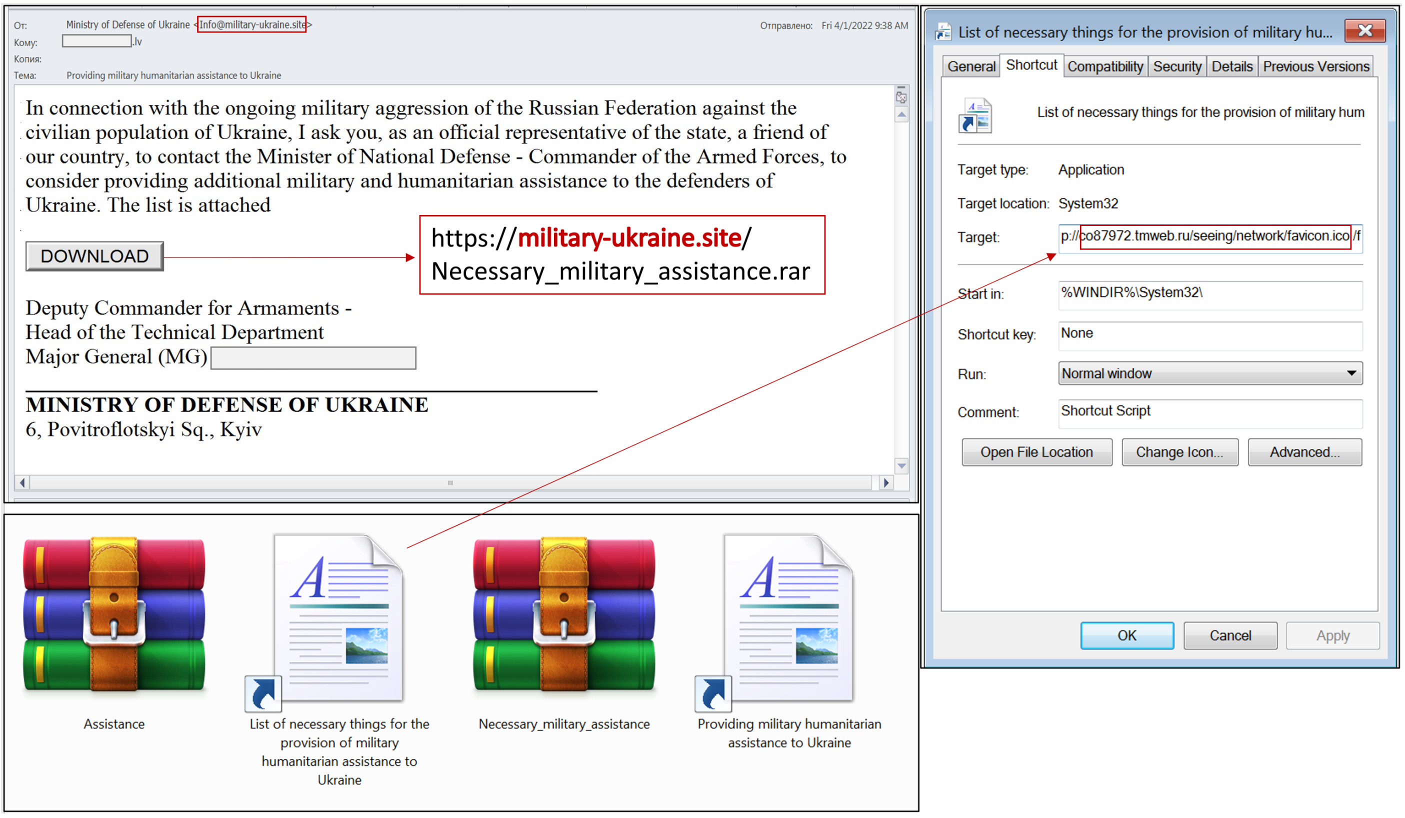
```
6ac4153b9ca93b8eefd83e304d2e5f5b
b73314087130fe98896add3430787744de7310d3342b219bd668cdce79368f91 Providing
military humanitarian assistance to Ukraine.eml
c0d3a0ab9b47ab9bc81cf5d831053431
596acbbfd7bc54dcc06123b7adfb7337f8ceab736004ce930d8286c8914b8e25
Assistance.rar
6c4e8c4880e388a49681cc169ccd4032
fa7bbc46a7b062a5828380b7c70a67cb47ba10c2ef127fd2348647313f65aa11 Providing
military humanitarian assistance to Ukraine.lnk
a4fad68e152a0f63cc525ae770e31a66
7052cef3936c29707da0dd0d4696863b63971eefa1b0e7db611df2ce26b73f50
Necessary_military_assistance.rar
7208e37192ad6f1d970a94d29ff02073
8f429996f5be9d59d86ba4346de535a25b9a2c3e89cf2e29dbc053d13ae99269 List of
necessary things for the provision of military humanitarian assistance to
Ukraine.lnk
7b20e3ac2a4ebf507f6c8358245d5db5
ae3fabbbb2e2297e31435b7a57c486f0eaf0f01738da8d0ab68214dc92373666
Assistance.rar
```

```
ab8bb3c1ff0c19358b5cd9867dbf2206
cf7570cbbca779c755729484792208900a89564669785cb26e88442278ac52b2 Providing
military humanitarian assistance to Ukraine.lnk
284aab4eada2fd522740315ee90efeed
0b63f6e7621421de9968d46de243ef769a343b615978166152223887c45df80ae
Necessary_military_assistance.rar
fb69fdb35859be1141a85a2af804340b
303abc6d8ab41cb00e3e7a2165ecc1e7fb4377ba46a9f4213a05f764567182e5 List of
necessary things for the provision of military humanitarian assistance to
Ukraine.lnk
e1fe781714ecb763ccd1568f7fa11443
a0a39c06f56d63b9d37f7e72c24ec0768fe0aff497870ef879d7ae813d84bf1e
Necessary_military_assistance.rar
872ef25c5c544b277b6185d75f33f9fb
09472d6bfb1c142a3b02f73175254a5e961f91e792dc9b347b099944bcfeab6f List of
necessary things for the provision of military humanitarian assistance to
Ukraine.lnk
```

Network:

```
Info @ military-ukraine [.] Site (envelope-from)
194 [.] 58.104.86 (Received from)
hxxps: // military-ukraine [.] site / Necessary_military_assistance.rar
hxxp: // military-ukraine [.] site / Assistance.rar
hxxp: // military-ukraine [.] online / predicate / images / favicon.ico
hxxp: // military-ukraine [.] online / headstone / images / favicon.ico
hxxp: //co87972.tmweb [.] ru / select / guarded / favicon.ico
hxxp: //co87972.tmweb [.] ru / intent / quick / favicon.ico
hxxp: //co87972.tmweb [.] ru / seeing / network / favicon.ico
military-ukraine [.] site
military-ukraine [.] online
co87972.tmweb [.] ru
```

Graphic images



От: Ministry of Defense of Ukraine <Info@military-ukraine.site> Отправлено: Fri 4/1/2022 9:38 AM
Кому: [redacted].lv
Копия:
Тема: Providing military humanitarian assistance to Ukraine

In connection with the ongoing military aggression of the Russian Federation against the civilian population of Ukraine, I ask you, as an official representative of the state, a friend of our country, to contact the Minister of National Defense - Commander of the Armed Forces, to consider providing additional military and humanitarian assistance to the defenders of Ukraine. The list is attached

https://military-ukraine.site/
Necessary_military_assistance.rar

Deputy Commander for Armaments -
Head of the Technical Department
Major General (MG) [redacted]

MINISTRY OF DEFENSE OF UKRAINE
6, Povitroflotskyi Sq., Kyiv

List of necessary things for the provision of military hu...

List of necessary things for the provision of military hum

Target type: Application
Target location: System32
Target: p://co87972.tmweb.ru/seeing/network/favicon.ico/f
Start in: %WINDIR%\System32\
Shortcut key: None
Run: Normal window
Comment: Shortcut Script

Assistance

List of necessary things for the provision of military humanitarian assistance to Ukraine

Necessary_military_assistance

Providing military humanitarian assistance to Ukraine