CERT-UA

Archived: 2026-04-02 11:06:54 UTC

Загальна інформація

Наприкінці березня 2022 року Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA виявлено декілька RAR-архівів з іменами "Assistance.rar", "Necessary_military_assistance.rar". Кожен з таких архівів містив шкідливі файли-ярлики з назвами "List of necessary things for the provision of military humanitarian assistance to Ukraine.lnk", "Providing military humanitarian assistance to Ukraine.lnk". Крім того, з'ясовано, що способом доставки були електронні листи з посиланнями на згадані RAR-архіви.

Використання англійської мови в назвах файлів та тексті електронного листа, а також той факт, що лист надіслано на адресу державного органу Латвії, однозначно свідчить про здійснення атак групою UAC-0010 (Armageddon) на державні органи країн Європейського Союзу.

Індикатори компрометації

Файли:

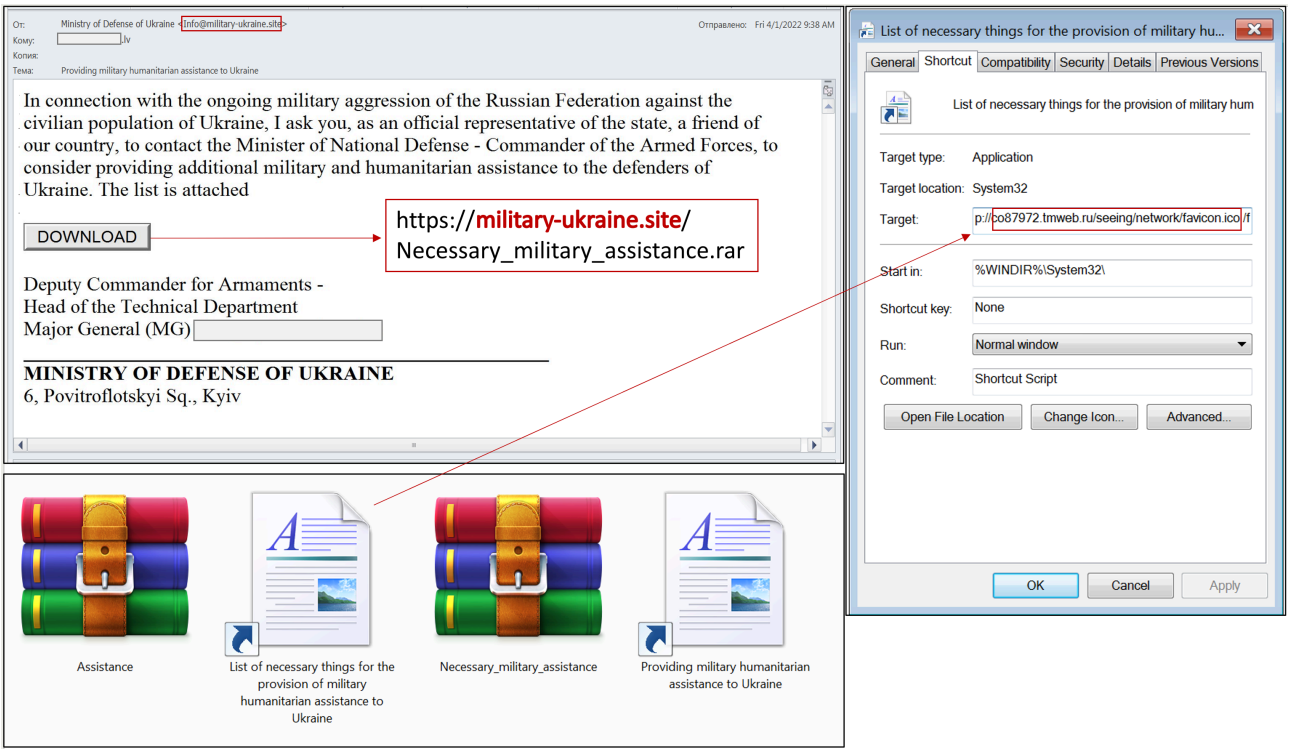
```
6ac4153b9ca93b8eefd83e304d2e5f5b    b73314087130fe98896add3430787744de7310d3342b219bd668cdce79368f91
c0d3a0ab9b47ab9bc81cf5d831053431    596acbbfd7bc54dcc06123b7adfb7337f8ceab736004ce930d8286c8914b8e25
6c4e8c4880e388a49681cc169ccd4032    fa7bbc46a7b062a5828380b7c70a67cb47ba10c2ef127fd2348647313f65aa11
a4fad68e152a0f63cc525ae770e31a66    7052cef3936c29707da0dd0d4696863b63971eefa1b0e7db611df2ce26b73f50
7208e37192ad6f1d970a94d29ff02073    8f429996f5be9d59d86ba4346de535a25b9a2c3e89cf2e29dbc053d13ae99269
7b20e3ac2a4ebf507f6c8358245d5db5    ae3fabbbb2e2297e31435b7a57c486f0eaf0f01738da8d0ab68214dc92373666
ab8bb3c1ff0c19358b5cd9867dbf2206    cf7570cbbca779c75572948479220890 0a89564669785cb26e88442278ac52b2
284aab4eada2fd522740315ee90efeed    0b63f6e7621421de9968d46de243ef769a343b61597816615222387c45df80ae
fb69fdb35859be1141a85a2af804340b    303abc6d8ab41cb00e3e7a2165ecc1e7fb4377ba46a9f4213a05f764567182e5
e1fe781714ecb763ccd1568f7fa11443    a0a39c06f56d63b9d37f7e72c24ec0768fe0aff497870ef879d7ae813d84bf1e
872ef25c5c544b277b6185d75f33f9fb    09472d6bfb1c142a3b02f73175254a5e961f91e792dc9b347b099944bcfeab6f
```

Мережеві:

```
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
```

Графічні зображення



Source: https://cert.gov.ua/article/39086