Cyber attack of UAC-0010 group (Armageddon) on state organizations of Ukraine (CERT-UA # 4378)

General Information

The government team for responding to computer emergencies in Ukraine CERT-UA revealed the fact of distribution of e-mails on "Information on war criminals of the Russian Federation" among government agencies of Ukraine. The e-mail contains the HTML-file "War criminals of the Russian Federation.htm", the opening of which will lead to the creation of a computer RAR-archive "Viyskovi_zlochinci_RU.rar". The mentioned archive contains a file-label "War criminals destroying Ukraine (home addresses, photos, phone numbers, pages on social networks) .lnk", the opening of which will download an HTA-file containing VBScript-code, which, in its turn to download and run the powershell script "get.php" (GammaLoad.PS1). The task of the latter is to determine the unique identifier of the computer (based on the name of the computer

The activity is associated with the activities of the group UAC-0010 (Armageddon).

We draw your attention to the need for additional verification of e-mails with attachments in the form of HTM-files, because, at present, the level of their detection is low.

Indicators of compromise

Files:

```
c1c62da5a36fed274f7777d5b8d111ae
ad03c5f2add8c629f4294b2a7df440cbae213f466e18f98af66db0b82a4e4142 Information
on war criminals of the Russian Federation [REDACTED] 2022-04-03 1459.eml
602e39a47a531b3f2b394a7176d6c87d
452a89dd1c760881e0066a5f6c0fc7b5f936a90a197859a4f3ee74b39f705da0 War
criminals of the Russian Federation.htm
35323ab59c094f3742a60998be6d0a27
ded51c96d161e9ac22782d7f9df37fe4816eae13be9369f9c8630ee706de53e1
Viyskovi_zlochinci_RU.rar
73479ebeb7db408e1cabd3e5a9c3ab8d
baae0ac6b3873dfdec2587dcddfaf1a327aadf77f7fea6a1532960f31e3dd240 War
criminals destroying Ukraine (home addresses, photos, sociall pages).
```

Network:

vadim_melnik88 @ i [.] ua (envelope-from)
194 [.] 38.21.12 (X-Sender-IP)
hxxp: // jokotras [.] ru / su / faicon.ico
hxxp: // prefer [.] jokotras.ru/hear/nephew/su
hxxp: // tiloraso [.] ru / get.php
hxxp: // tiloraso [.] ru / index.php
jokotras [.] ru
tiloraso [.] ru
milotrad [.] ru
potrakit [.] ru
tortunas [.] ru
66 [.] 175,219,231 (@ linode.com)

Hosts:

C: \ Users \ Public \ test.vbs
% TMP% \ <rand_digits> .exe

Graphic images