Кібератака групи UAC-0010 (Armageddon) на державні організації України (CERT-UA#4378)

Кібератака групи UAC-0010 (Armageddon) на державні організації України (CERT-UA#4378)

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA виявлено факт розповсюдження електронних листів з темою "Інформація щодо військових злочинців РФ" серед державних органів України. Електронний лист містить HTML-файл "Військові злочинці РФ.htm", відкриття якого призведе до створення на комп'ютері RAR-архіву "Viyskovi_zlochinci_RU.rar". Згаданий архів містить файл-ярлик "Військові-злочинці що знищують Україну (домашні адреси, фото, номера телефонів, сторінки у соціальних сетях).lnk", відкриття якого призведе до завантаження HTA-файлу, який містить VBScript-код, що, у свою чергу, забезпечить завантаження і запуск powershell-скрипта "get.php" (GammaLoad.PS1). Завданням останнього є визначення унікального ідентифікатору комп'ютера (на основі імені комп'ютера та серійного номеру системного диску), передача цієї інформації для використання як XOR-ключа на сервер управління за допомогою HTTP POST-запиту, а також завантаження, XOR-декодування та запуск пейлоаду.

Активність асоційовано з діяльністю групи UAC-0010 (Armageddon).

Звертаємо увагу на необхідність додаткової перевірки електронних листів із вкладеннями у вигляді HTM-файлів, адже, наразі, рівень їхнього детектування низький.

Індикатори компрометації

Файли:

```
c1c62da5a36fed274f7777d5b8d111ae
ad03c5f2add8c629f4294b2a7df440cbae213f466e18f98af66db0b82a4e4142
Інформація щодо військових злочинців РФ[REDACTED]2022-04-03 1459.eml
602e39a47a531b3f2b394a7176d6c87d
452a89dd1c760881e0066a5f6c0fc7b5f936a90a197859a4f3ee74b39f705da0    Військові
злочинці РФ.htm
35323ab59c094f3742a60998be6d0a27
ded51c96d161e9ac22782d7f9df37fe4816eae13be9369f9c8630ee706de53e1
Viyskovi_zlochinci_RU.rar
73479ebeb7db408e1cabd3e5a9c3ab8d
baae0ac6b3873dfdec2587dcddfaf1a327aadf77f7fea6a1532960f31e3dd240
Військові-злочинці що знищують Україну (домашні адреси, фото, номера
телефонів, сторінки у соціальних сетях).lnk
```

Мережеві:

```
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)
```

Хостові:

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

Графічні зображення