CERT-UA

Archived: 2026-04-05 21:11:53 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA отримано інформацію щодо розповсюдження 05.07.2022 електронних листів з темою "Спеціалізованої прокуратури увійськовій та оборонній сфері. Інформація щодо наявності вакансій та їх укомплектування" та вкладенням у вигляді XLS-документу "Інформація щодо наявності вакансій та їх укомплектування.xls".

Документ містить макрос, активація якого призведе до створення на комп'ютері та запуску файлу "write.exe".

Згаданий файл виконує роль дропера, забезпечуючи створення на диску файлу "%PROGRAMDATA%\TRYxaEbX", його дешифрування (RC4) та подальший запуск PowerShell-скрипта. Крім того, EXE-файл також забезпечує власну персистентність, створюючи ключ "Check License" в гілці "Run" реєстру Windows.

Отриманий PowerShell-скрипт, окрім обходу AMSI та відключення логування подій для PowerShell, забезпечить декодування та декомпресію даних в наступний PowerShell-скрипт, який, у свою чергу, забезпечить виконання шкідливої програми Cobalt Strike Beacon.

З середнім рівнем впевненості виявлену активність асоціюємо з діяльністю групи UAC-0056.

Індикатори компрометації

Файли:

```
c6e7af8d31a951b8c05565ab18c4f258    024054ff04e0fd75a4765dd705067a6b336caa751f0a804fefce787382ac45c1
28f18fc7d9a0ab530742c2314cbd5c32    14736be09a7652d206cd6ab35375116ec4fad499bb1b47567e4fd56dcfcd22ea
8409920ef2d78549fc214718c4719d3a    e68c83ce6359691ce63c957ebfdbf959c5b199c83fd2480aebe4220fec9f3304
1dc98fb372925fcba321b0bc8347fdcc    d1e6d365a3ede77bd7f6c77523b114dd9628f7b9bafb2e458f9b19bd6ce24c71
f4217387333f65faeb7b13637c1e7c72    e1cbfef74b4084023a1f02ab68b3ad3bc60561f7e988860b80ac94a91922fa86
26e326ba69f5258c4979902b5bd4f24e    9dec13e1b0ed9337fcbe233d5f83eff09c64a14c7f2400b9b915a685b29612ea
a4b4047022bce6f65faffc4c6033c5d2    c1e14c4d8d83281de413ccaa577621a057195df3773960274aabf855e2c7bea2
```

Мережеві:

```
skreatortemp[.]site
hXXps://skreatortemp[.]site/s/08u1XdxChhMrLYdTasfnOMQpbsLkpq3o/field-keywords/
hXXps://skreatortemp[.]site/nBz07hg5l3C9wuWVCGV-5xHHu1amjf76F2A8i/avp/amznussraps/
Mozilla/5.0_Frsg_stredf_o21_rutyyyrui_type (Windows NT 10.0; Win64; x64; Trident/7.0; D-M1-200309AC;
```

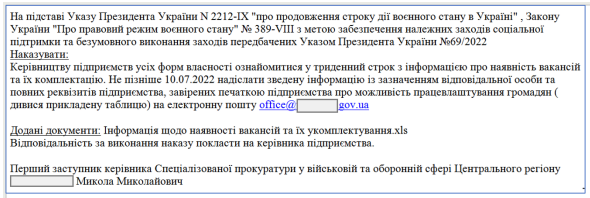
Хостові:

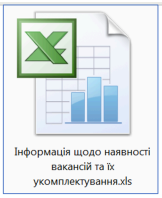
```
%PROGRAMDATA%\TRYxaEbX
%TMP%\write.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Check License
%PROGRAMFILES(x86)%\Microsoft Office\Office14\EXCEL.EXE %TMP%\write.exe (створення процесу)
```

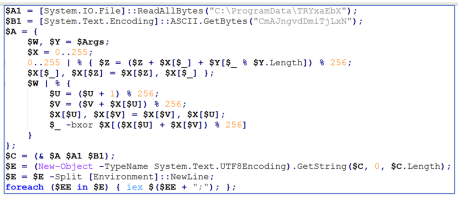
Рекомендації

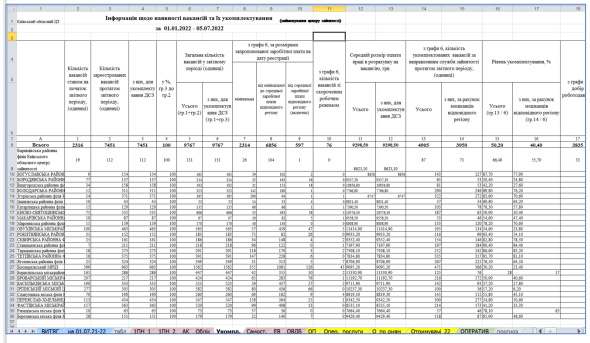
1. Заборонити можливість створення небезпечних дочірніх процесів з офісних програм (наприклад, https://support.eset.com/en/kb6119-configure-hips-rules-for-eset-business-products-to-protect-against-ransomware)

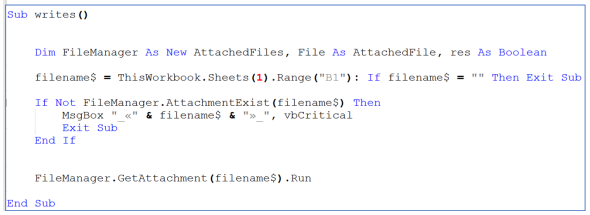
Графічні зображення


На підставі Указу Президента України N 2212-IX "про продовження строку дії воєнного стану в Україні" , Закону України "Про правовий режим воєнного стану" № 389-VIII з метою забезпечення належних заходів соціальної підтримки та безумовного виконання заходів передбачених Указом Президента України №69/2022
Наказувати:
Керівництву підприємств усіх форм власності ознайомитися у триденний строк з інформацією про наявність вакансій та їх комплектацію. Не пізніше 10.07.2022 надіслати зведену інформацію із зазначенням відповідальної особи та повних реквізитів підприємства, завірених печаткою підприємства про можливість працевлаштування громадян (дивися прикладену таблицю) на електронну пошту office@ gov.ua
Додані документи: Інформація щодо наявності вакансій та їх укомплектування.xls
Відповідальність за виконання наказу покласти на керівника підприємства.
Перший заступник керівника Спеціалізованої прокуратури у військовій та оборонній сфері Центрального регіону
Микола Миколайович






Інформація щодо наявності вакансій та їх укомплектування на 01.01.2022 - 05.07.2022



Source: https://cert.gov.ua/article/619229