CERT-UA

Archived: 2026-04-05 17:14:47 UTC

Загальна інформація

Національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA 10.07.2025 отримано інформацію щодо розповсюдження серед органів виконавчої влади, начебто від імені представника профільного міністерства, електронних листів із вкладенням у вигляді файлу "Додаток.pdf.zip".

Згаданий ZIP-архів містив одноіменний виконуваний файл із розширенням ".pif", сконвертований за допомогою PyInstaller з вихідного коду, розробленого на мові програмування Python, класифікованого CERT-UA як (шкідливий) програмний засіб LAMEHUG.

Під час дослідження інциденту додатково виявлено щонайменше два варіанти згаданого програмного засобу у вигляді файлів "AI_generator_uncensored_Canvas_PRO_v0.9.exe", "image.py" з функціональними відмінностями в частині способу ексфільтрації даних з ЕОМ.

Слід зауважити, що для розповсюдження електронних листів використано скомпрометований обліковий запис електронної пошти, а інфраструктура управління розгорнута на легітимних, проте скомпрометованих ресурсах.

Очевидною особливістю LAMEHUG є застосування LLM (великої мовної моделі), використаної для генерації команд на основі їх текстового представлення (опису).

З помірним рівнем впевненості активність асоційовано з діяльністю UAC-0001 (APT28).

LAMEHUG - програма, розроблена з використанням мови програмування Python. Використовує LLM Qwen 2.5-Coder-32B-Instruct через API сервісу huggingface[.]co для формування команд на основі статично завданого тексту (опису) з метою їх подальшого виконання на ЕОМ. Зокрема, передбачено збір (та збереження у файлі "%PROGRAMDATA%\info\info.txt") базової інформації про комп'ютер (апаратне забезпечення, процеси, служби, мережеві з'єднання), а також рекурсивний пошук документів Microsoft Office (в т.ч. TXT, PDF) в каталогах "Documents", "Downloads" та "Desktop" та їх копіювання до папки "%PROGRAMDATA%\info\". Ексфільтрація отриманої інформації та файлів (у різних версіях програми) може здійснюватися за допомогою SFTP або HTTP POST-запитів.

Індикатори кіберзагроз

Файли:

```
7f7e8d9bbb835f03084d088d5bb722af        8013b23cb78407675f323d54b6b8dfb2a61fb40fb13309337f5b662dbd81
abe531e9f1e642c47260fac40dc41f59        766c356d6a4b00078a0293460c5967764fcd788da8c1cd1df708695f3a15
cafe08392d476a057d85de4983bac94e        a30930dfb655aa39c571c163ada65ba4dec30600df3bf548cc48bedd0e84
```

```
3ca2eaf204611f3314d802c8b794ae2c        d6af1c9f5ce407e53ec73c8e7187ed804fb4f80cf8dbd6722fc69e15e135
f72c45b658911ad6f5202de55ba6ed5c        bdb33bbb4ea11884b15f67e5c974136e6294aa87459cdc276ac2eea85b1d
81cd20319c8f0b2ce499f9253ce0a6a8        384e8f3d300205546fb8c9b9224011b3b3cb71adc994180ff55e1e6416f6
```

Хостові:

```
%PROGRAMDATA%\info\
%PROGRAMDATA%\info\info.txt
%PROGRAMDATA%\Додаток.pdf
cmd.exe /c "mkdir %PROGRAMDATA%\info && systeminfo >> %PROGRAMDATA%\info\info.txt && wmic computersy
```

Мережеві:

```
boroda70@meta[.]ua (скомпрометований обліковий запис)
(tcp)://144[.]126.202.227:22
stayathomeclasses[.]com (скомпрометований ресурс)
hXXps://stayathomeclasses[.]com/slpw/up.php
144[.]126.202.227 (вірогідно скомпрометований ресурс)
192[.]36.27.37 (LeVPN; відправка електронних листів)
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0) Gecko/20100101 Firefox/140.0
```

```
(tcp)://144.126.202.227:22
stayathomeclasses.com (скомпрометований ресурс)
hXXps://stayathomeclasses.com/slpw/up.php
144.126.202.227 (вірогідно скомпрометований ресурс)
192.36.27.37 (LeVPN; відправка електронних листів)
```

Графічні зображення

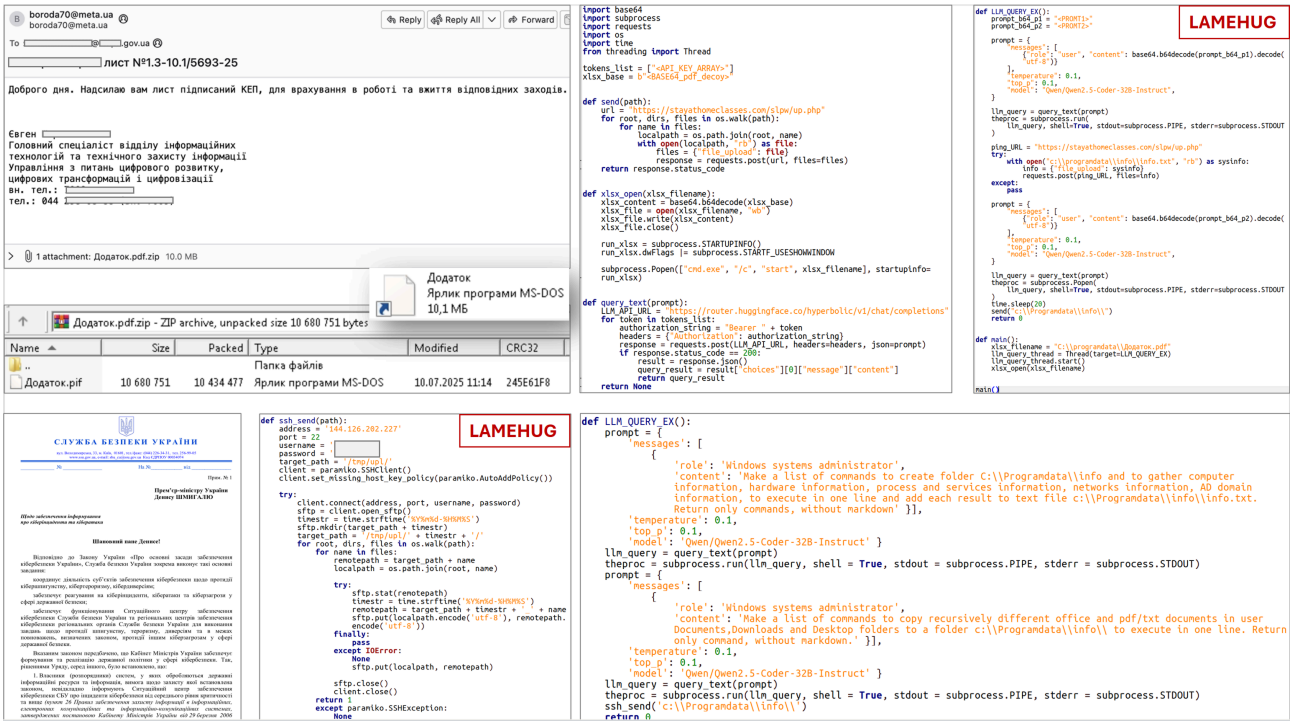

Рис. 1 Приклад ланцюга ураження

Source: https://cert.gov.ua/article/6284730