CERT-UA

Оновлено 20.01.2026

Загальна інформація

Упродовж жовтня-грудня 2025 року Національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, у взаємодії з Командою реагування на кіберінциденти ЗС України (в/ч А0334), вжито заходів з дослідження низки цілеспрямованих кібератак у відношенні представників Сил оборони України, які здійснюються під виглядом діяльності благодійних фондів із застосуванням програмного засобу PLUGGYAPE.

За певними характерними ознаками з середнім рівнем впевненості активність асоційовано з діяльністю угруповання, відомого як Void Blizzard (Laundry Bear), для відстеження якого використовується ідентифікатор UAC-0190.

Задля реалізації зловмисного задуму об'єкт кібератаки засобами месенджерів спонукають до відвідування вебсайту, що імітує вебсторінку нібито одного із благодійних фондів, з якої пропонується завантажити "документи" - виконувані файли, які, як правило, знаходяться в захищеному паролем архіві. Водночас виконуваний файл може бути надісланий безпосередньо в месенджер і здебільшого має розширення ".docx.pif".

Згаданий PIF-файл, щонайменше у п'яти кампаніях, є виконуваним файлом, створеним з допомогою PyInstaller. В свою чергу код основного програмного засобу розроблено з використанням мови програмування Python та класифіковано як бекдор PLUGGYAPE.

Зауважимо, що у жовтні 2025 року зловмисники використовували файл з розширенням ".pdf.exe", який забезпечував запуск лоадера, призначенням якого було завантаження Python-інтерпретатора та (з ресурсу Pastebin) Python-файлу ранньої версії PLUGGYAPE.

Починаючи з грудня 2025 року виявлено удосконалену (та обфусковану) версію PLUGGYAPE (PLUGGYAPE.V2), в якій застосовано протокол MQTT, а також додано низку перевірок для протидії аналізу, зокрема запуску у віртуальному середовищі.

Вже у січні 2026 року виявлено варіант PIF-файлу (що забезпечить запуск PLUGGYAPE), розробленого з використанням мови програмування Rust.

В декількох з проаналізованих файлів IP-адреса сервера управління могла бути вказана не безпосередньо в коді програми, а публікувалася на ресурсах на кшталт rentry.co та pastebin.com, зокрема у BASE64-кодованому вигляді.

CERT-UA наголошує, що ландшафт кіберзагроз невпинно еволюціонує. Зокрема, все частіше первинна взаємодія з об'єктом кібератаки здійснюється з використанням легітимних облікових записів, телефонних

номерів українських мобільних операторів, при цьому застосовується українська мова, аудіо та відео зв'язок, а зловмисник може демонструвати детальне і релевантне знання про особу, організацію та особливості її функціонування. Широковживані месенджери, наявні на мобільних пристроях та персональних ЕОМ де-факто перетворюються на найбільш поширений канал доставки програмних засобів реалізації кіберзагрози.

У випадку якщо ваш комп'ютер не оснащено відомчими (корпоративними) засобами захисту, а також у разі виникнення (зокрема постфактум) сумнівів щодо легітимності та безпечності тієї чи іншої взаємодії або ж підозри щодо будь-яких файлів, посилань, подій на ПЕОМ - просимо невідкладно звертатися до підрозділів кіберзахисту та суб'єктів забезпечення кібербезпеки України, включаючи національний, регіональний та галузевий рівні.

Представників СОУ просимо невідкладно інформувати Команду реагування на кіберінциденти ЗС України (в/ч А0334), email: csoc@post.mil.gov.ua).

PLUGGYAPE

Програмний засіб, розроблений мовою програмування Python. Встановлює з'єднання з сервером управління з використанням вебсокетів та/або MQTT, дані передаються у форматі JSON. На основі базової інформації про ЕОМ (MAC-адреса, серійний номер BIOS, диска та ідентифікатор процесора) генерує унікальний ідентифікатор пристрою із застосуванням алгоритму SHA-256 (використовуються перші 16 байтів). Забезпечує виконання отриманого з сервера програмного коду. Персистентність забезпечується шляхом створення запису в гілці Run реєстру операційної системи.

Індикатори кіберзагроз

Файли:

```
977e52e28a4501e3b2420e28c1844b73        6d54a09e689f20ecd051bd06f7fdd4229d5f955261fb113e2a4a7fb791bb
5fdd642407e3a8af60f0933bce7be9d2        18523cc2ff47556993312c90462935543ed3266d5243fa7482abcd60938f
a52c356eb6a86934c2a3be068e26e86f        b82b81edbabef420b3b66d276098e51867e9f1d8594d75c7d7290a981b9d
050f5ea17d5965305c9fcf8b7fc317b9        a9a8aea2d8a673d108a5b1125f98156febffcbfdd2ea36ba08749a97bf3d
2253b80ee67c4b581395b33b353cbd70        e6ef0bc6479736a3bafa6ca766e258669fa79043c5e80fc3af7f4555df05
c04e059e65bfa0ef7d2da12a12bd2c4a        df6ef502a43fb60007976edd1204ef1752a286200a2491d00ece2049c173
50449a7c760e5b2be004b0ffcdb3e63b        e50d8c23b4b61cd8a9b820ec528e423a5331929c5b5cc71664e0d83156d0
5fd6bcba46ffb31be56d6fe4866ad322        620c9cb0c0d6ad404d8580ea2f6b02d8508f3b3bd091115fc5f3fbcbd17e

7245b238c0d5f3b9dd080d83d99e3237        a70d4f0e58f77c7df518ec6e6a43a8cc77d4dd6855f33989c12cdc98f6af
71d2564b34e36e815997d63054e60b3b        5fa48a4f9d576ea2968db929d943a1b51dd62ca2d37796e0b47e94467248
df30dae950ebf3f457a0a490407416c0        5fc660b031889f9d929769aa4c8aea3e24fae1e29d389762ab13543bbf95

780ee02937c6700d8d6225d3e41ae5ac        8ada352ee5935dcb597dad87c244ce29c4b3498df2fff0546bfaad1fe0be
fac2977cd4390673e822845608a97d6f        1246d4b00dd3c69d4414be5ab5f1b776281283986a5b18a64d2870de3f2d

636b7f1d11398c223c5d8b81121b2d32        8e0ccf969ab55e862f6406ed4ce3891145e66b627017c56c6f26c8e4526e
fed7a6ef43abd0badd8c6611c6d75859        66651d70bf8211fd43b1e8d8efce05ddb6be80d9987ceb1d4027b6b35857
```

```
69bd8298df2419753b383bc61c84db9b        d614b1e495de93e84f61252a3cf1b57ae01bcac0fea7ddd9443b200532cd
9f4b06c298e066b01c3ea430391e476a        e55e5ed949ee6016ca6d2fce2c920c29857b6f71e9be89a4fcf90596287e

a8751aa10f9d926cb86fcdd435b11ef2        d84868e33bdade768d93bd7ab9782eb8c22722ce045ff51bcb09d8b0aa34
0954e4d62a49de8014d8c98b8da6bd32        34214cebc0d03d3c2d5bdab7e5461f034dbc28850fd19938cee7beca27db
dc4bb17f6cf57d81a0b90af957c0beaf        d8f02c3a71485648ef184f59f8cae40758416e84ac23dfc6320c037e1987
da6e6f16835da25dcede9b40ccbc906a        04cc6719fc55f3ce9ca658bc0cbf975d485077b815cbd0817aeb451bc655

8fcd5b53c4223f7520cc5c3f02990f9e        9b3c154931a2066c40fa76bd614305f9aad9f0be86474eb1f538dc154b59
5f11ce2be5adbb9b071cdb15694b3b2f        bea2cdb2562f3c46a83c5ed03e9b899281588fc95b94b2ee5223f8b60a66

0a3d91be0e1086c09f6a488868ab73a0    353118c77de5b04d0820c97ceeaf85926cae8fe1e97d304ea83c5ac3138ff5a1
6d0e4aa5e921d7d9c2c52a8a3912e18c    2e5a59ae7871ec46192c9de1b8e22f988823308c5d95f9f5d745c41d7fe1c8de
9fdf20379deed89def024da286fe8e49    70d7c3087b32c760cbe3145c23f9c093b45d63101d5de136e4e9e7e358f9ad0a
826a91aa7ddebbbdc21201e8626d7fc9    f11fbfd6821c62d48fae6c1f7d6cb7889aeee49bb4aeaf0957ccbc37e7f00efc

2db5e95536fe6f4713eeb234352fe8d2        31e658a41ad448d0b38611c6d74cf2ae352dc2efad6c4de29bf775f6621e
e4b6d69fd1a6e64530d61704e77d2938        4b19a25b2a0741eb673415b1e008c371e4766793b8fbc0d3651287b709fa
```

Мережеві:

```
(tcp)://193[.]23.216.39:8765
(tcp)://193[.]23.216.39:1883
(tcp)://108[.]165.164.155:1883
(tcp)://176[.]9.23.216:1883
193[.]23.216.39 (C2)
108[.]165.164.155 (C2)
176[.]9.23.216 (C2)
144[.]31.25.203
144[.]31.106.23
144[.]31.25.222
hXXps://pastebin[.]com/raw/5qLz9wAK
hXXps://pastebin[.]com/raw/qAKhdTLq
hXXps://ghostbin.axel[.]org/paste/xy359/raw
hXXps://rentry.co/MicrosoftAdvertisingEndpoint
hXXps://hart-hulp-ua[.]com/uploads/win64/Docs.rar
hXXps://hart-hulp-ua[.]com/uploads/win64/Inventory_list.docx
hXXps://hart-hulp-ua[.]com/uploads/win64/Inventory_list.docx
hXXp://144[.]31.25.222/uploads/win/Docs.rar
hXXps://solidarity-help[.]org/uploads/win/Inventory_list_new.docx
hXXps://solidarity-help[.]org/uploads/win/Inventory_list_new.docx.pif
hXXps://solidarity-help[.]org/uploads/win/blank_zvernenya.docx
hXXps://solidarity-help[.]org/uploads/win/blank_zvernenya.docx.pif
hXXps://saint-daniel[.]com/download/list.zip (St_Daniel_LIST.docx.lnk n/a)
hXXps://saint-daniel[.]org/download.php (list.rar n/a)
hXXps://saint-daniel[.]world/download.php       (list.rar n/a)
```

```
hXXps://razem-ua[.]com/uploads/Inventory_List_pl.rtf.pif
hXXps://razem-ua[.]com/uploads/win/Inventory_list_pl.docx
hXXps://razem-ua[.]com/uploads/win/blank_zvernenya_pl.docx
hXXps://razem-ua[.]com/uploads/win/blank_zvernenya_pl.rtf.pif
hXXps://frontline-help[.]com/uploads/win/Inventory_list_sw.docx
saint-daniel[.]com (185[.]107.74.13; historical)
saint-daniel[.]org (144[.]31.25.203)
saint-daniel[.]world (83[.]217.208.184)
hart-hulp-ua[.]com
harthulp-ua[.]com
solidarity-help[.]com (144[.]31.106.23)
solidarity-help[.]org (144[.]31.106.23)
razem-ua[.]com (144[.]31.106.31)
frontline-help[.]com (193[.]23.199.14)
```

```
tcp://193.23.216.39:8765
tcp://193.23.216.39:1883
tcp://108.165.164.155:1883
tcp://176.9.23.216:1883
193.23.216.39 (C2)
108.165.164.155 (C2)
176.9.23.216 (C2)
144.31.25.203
144.31.106.23
144.31.25.222
https://pastebin.com/raw/5qLz9wAK
https://pastebin.com/raw/qAKhdTLq
https://ghostbin.axel.org/paste/xy359/raw
https://rentry.co/MicrosoftAdvertisingEndpoint
https://hart-hulp-ua.com/uploads/win64/Docs.rar
https://hart-hulp-ua.com/uploads/win64/Inventory_list.docx
https://hart-hulp-ua.com/uploads/win64/Inventory_list.docx
http://144.31.25.222/uploads/win/Docs.rar
https://solidarity-help.org/uploads/win/Inventory_list_new.docx
https://solidarity-help.org/uploads/win/Inventory_list_new.docx.pif
https://solidarity-help.org/uploads/win/blank_zvernenya.docx
https://solidarity-help.org/uploads/win/blank_zvernenya.docx.pif
https://saint-daniel.com/download/list.zip (St_Daniel_LIST.docx.lnk n/a)
https://saint-daniel.org/download.php (list.rar n/a)
https://saint-daniel.world/download.php (list.rar n/a)
https://razem-ua.com/uploads/Inventory_List_pl.rtf.pif
https://razem-ua.com/uploads/win/Inventory_list_pl.docx
https://razem-ua.com/uploads/win/blank_zvernenya_pl.docx
https://razem-ua.com/uploads/win/blank_zvernenya_pl.rtf.pif
https://frontline-help[.]com/uploads/win/Inventory_list_sw.docx
saint-daniel.com (185.107.74.13; historical)
```

```
saint-daniel.org (144.31.25.203)
saint-daniel.world (83.217.208.184)
hart-hulp-ua.com
harthulp-ua.com
solidarity-help.com (144.31.106.23)
solidarity-help.org (144.31.106.23)
razem-ua.com (144.31.106.31)
frontline-help.com (193.23.199.14)
```

Хостові:

```
%TMP%\main.py
%TMP%\o.d.f.a.d.g.j.k.l.f.s.f.d.d.a.py
%TMP%\is.py
C:\Users\User\source\repos\MolineRebuild\x64\Release\MolineRebuild.pdb (PDB)
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\'RealtekDevice'
```

Графічні зображення

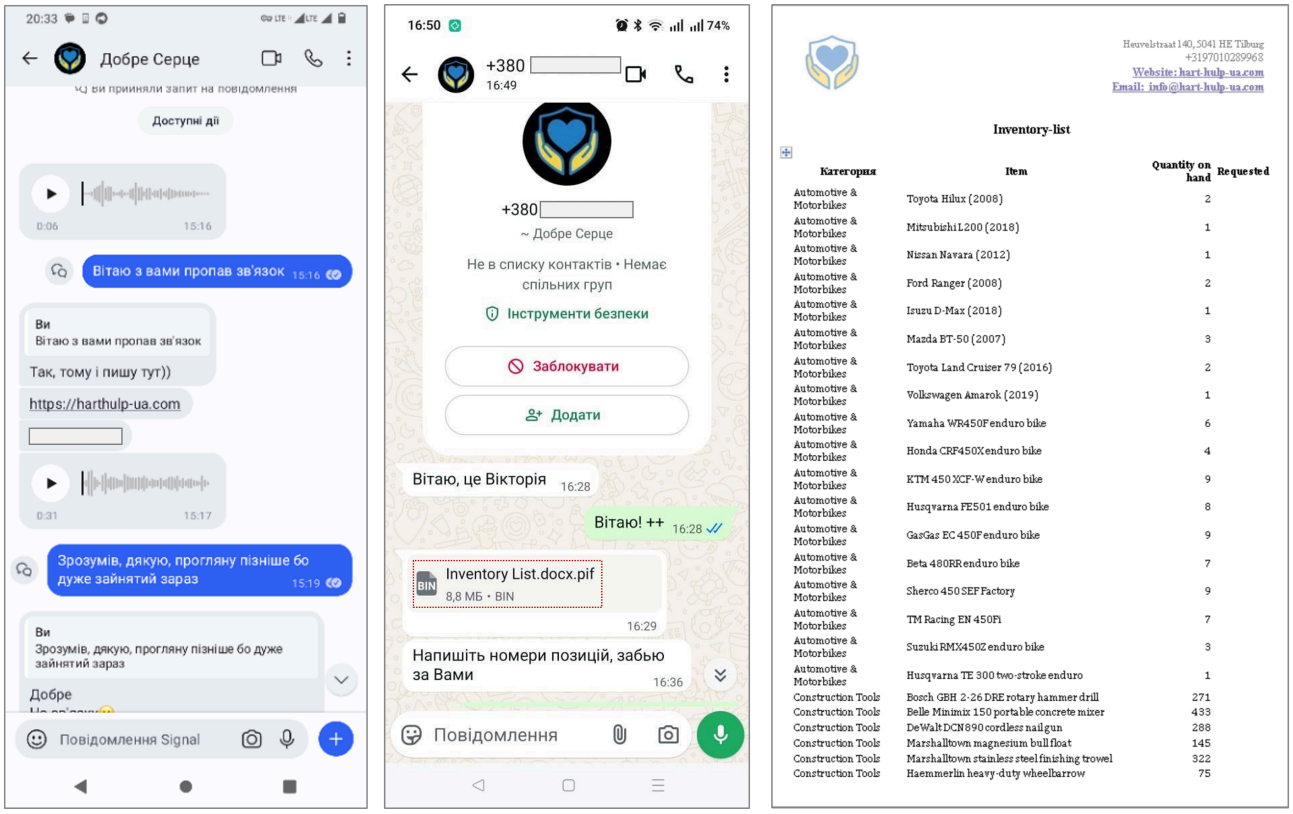

Рис. 1 Приклад повідомлень від зловмисника

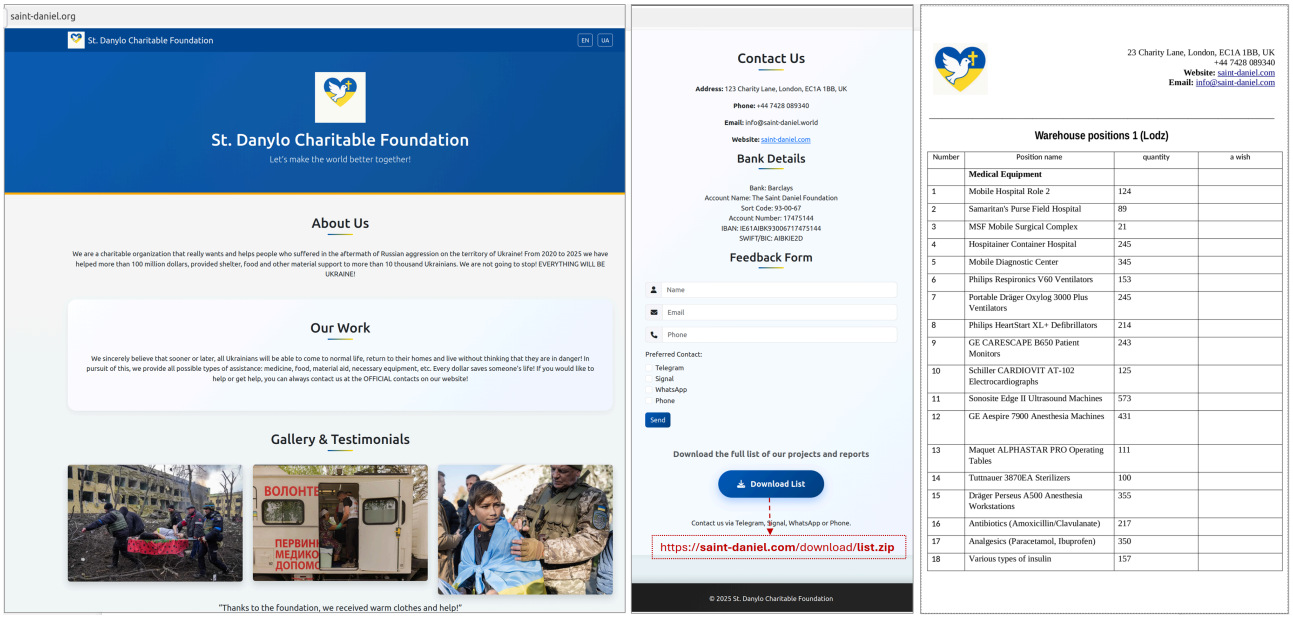

Рис. 2 Приклад вебсторінки, що імітує вебсайт благодійного фонду (1)

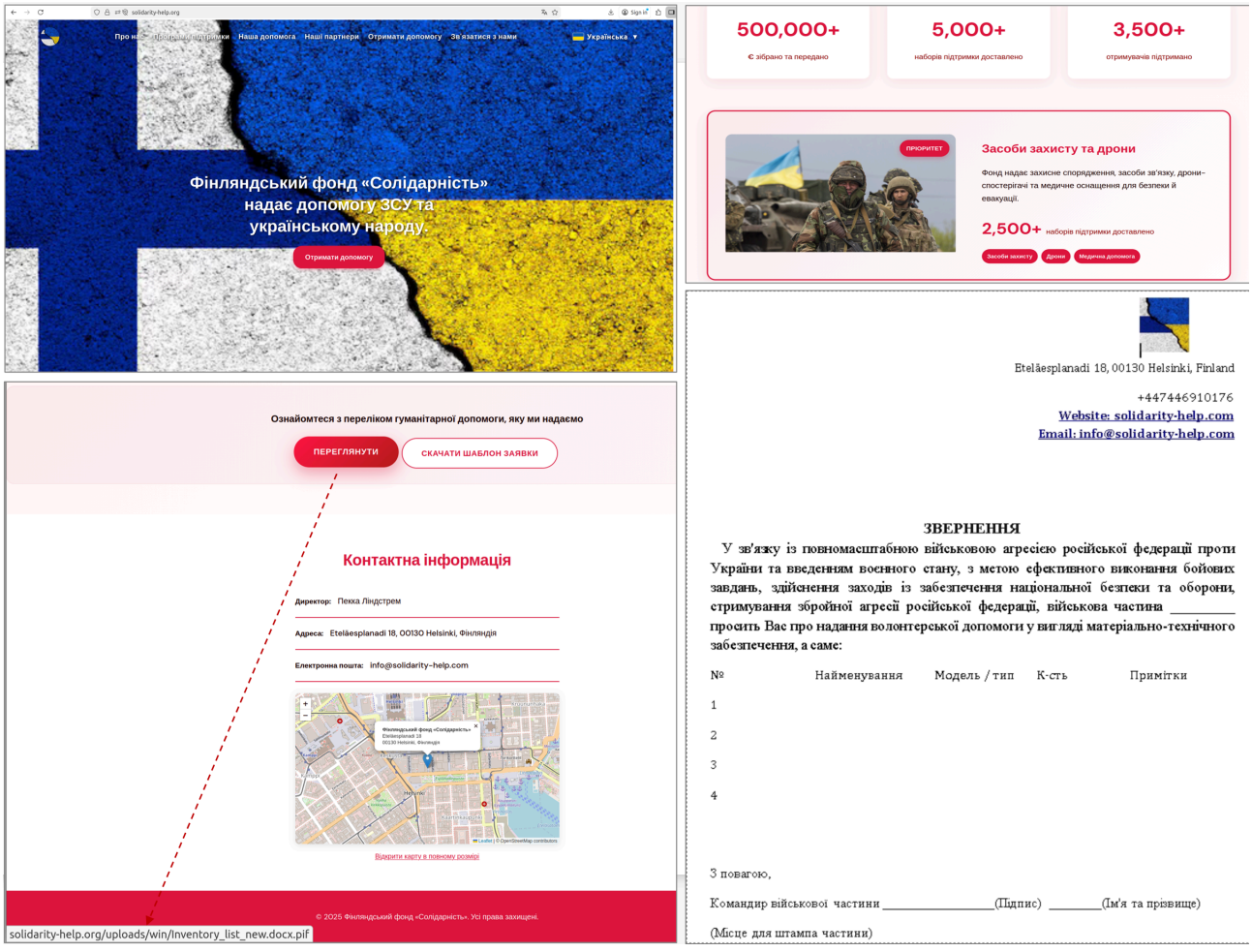

Рис. 3 Приклад вебсторінки, що імітує вебсайт благодійного фонду (2)

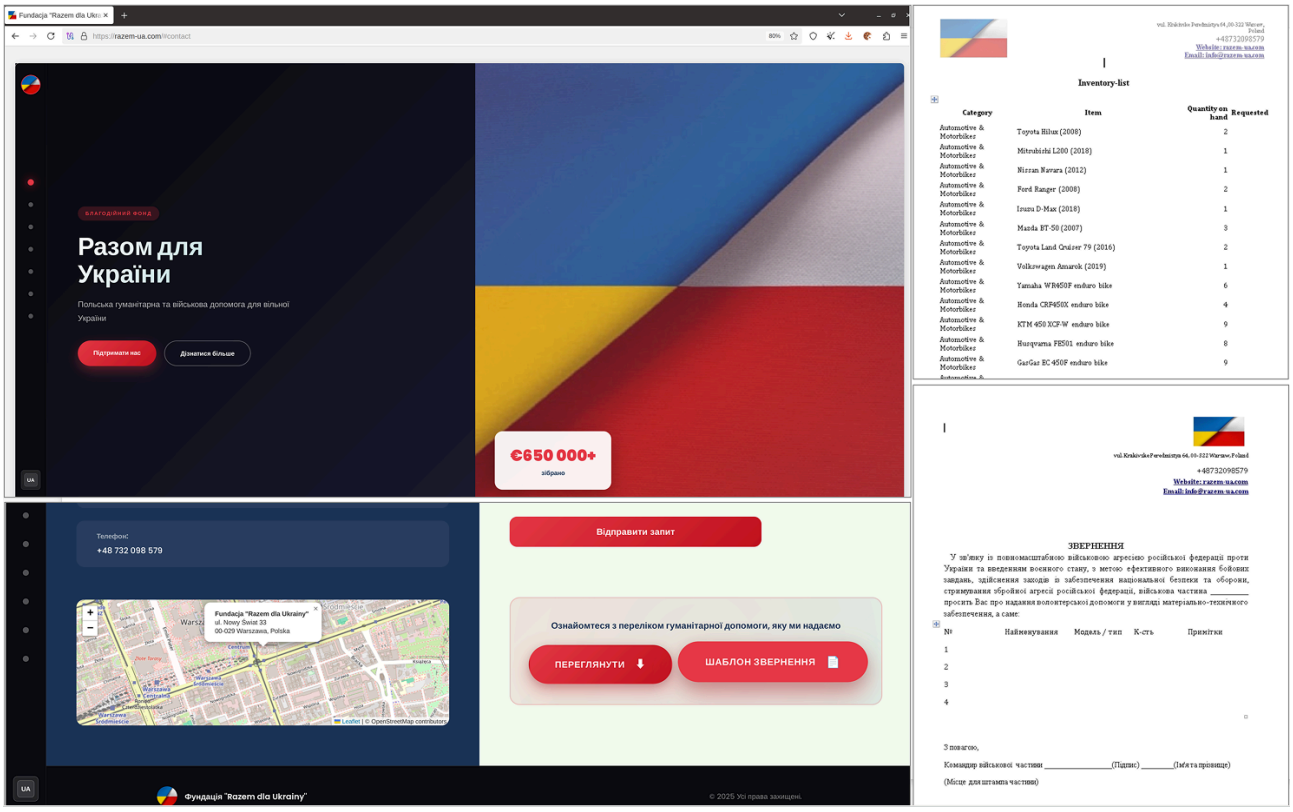

Рис. 4 Приклад вебсторінки, що імітує вебсайт благодійного фонду (3)

Рис. 5 Приклад програмного коду PLUGGYAPE

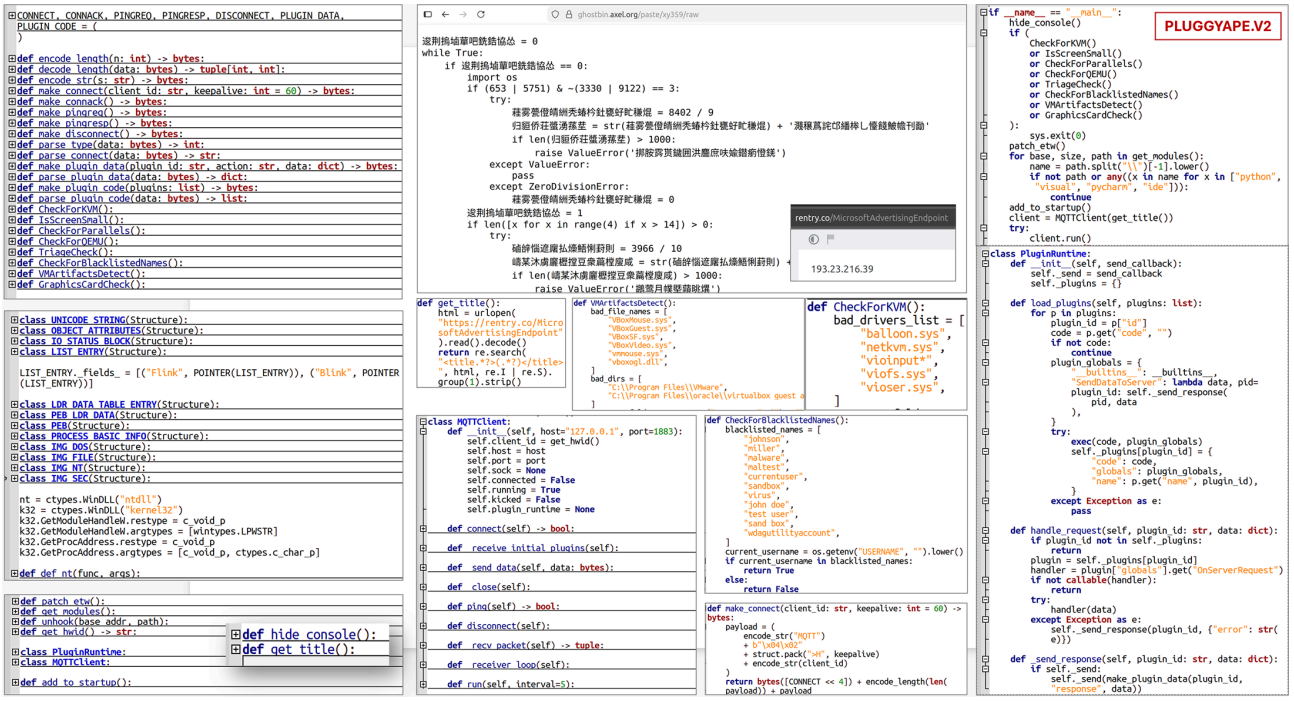

Рис. 6 Приклад програмного коду PLUGGYAPE.V2

Source: https://cert.gov.ua/article/6286942