CERT-UA

Archived: 2026-04-10 02:00:17 UTC

Оновлено 29.03.2026

Загальна інформація

Національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA 26-27 березня 2026 року зафіксовано випадки розповсюдження електронних листів нібито від імені CERT-UA із закликом завантажити з сервісу Files.fm захищений паролем архів ("CERT_UA_protection_tool.zip", "protection_tool.zip") та встановити "спеціалізоване програмне забезпечення". Серед отримувачів листів: державні організації, медичні центри, охоронні фірми, навчальні заклади, фінансові установи, компанії-розробники програмного забезпечення та інші.

Крім того, виявлено вебресурс cert-ua[.]tech, який містить матеріали з офіційної вебсторінки cert.gov.ua, а також інструкцію із завантаження згаданого "засобу захисту".

З'ясовано, що виконуваний файл, який пропонувалося встановити (внутрішня назва пакета: "/example.com/tvisor/agent"), є багатофункціональним програмним засобом для віддаленого керування комп’ютером, що класифікований CERT-UA як AGEWHEEZE.

Сервер управління програмним засобом розміщено на технічному майданчику французької компанії OVH (AS16276). На мережевому порту 8443/tcp опубліковано вебсторінку з назвою "The Cult", що містить форму автентифікації. У вихідному коді HTML-сторінки наявні рядки російською мовою: "Членство приостановлено. Твой доступ к Культу был заблокирован. Свяжись с администратором для восстановления". Відповідний самопідписаний SSL-сертифікат створено 18.03.2026, а поле "Organization" містить значення "TVisor".

Під час поверхневого огляду ШІ-згенерованої вебсторінки hXXps://cert-ua[.]tech/ (SSL-сертифікат GlobalSign дійсний з 27.03.2026 06:41:09 GMT; станом на 29.03.2026 вебсторінка не відображається), в HTML-коді виявлено рядки: "С Любовью, КИБЕР СЕРП - hXXps://t[.]me/CyberSerp_Official". Уже 28.03.2026 у згаданому Telegram-каналі опубліковано повідомлення про взяття відповідальності за проведення кібератаки, що усуває невизначеність технічної атрибуції. Таким чином, для відстеження описаної активності створено ідентифікатор UAC-0255.

За даними CERT-UA, кібератака була неуспішною. Ідентифіковано не більше ніж кілька інфікованих особистих пристроїв, що належали працівникам закладів освіти різних форм власності. Фахівці команди надали необхідну методичну та практичну допомогу.

Принагідно висловлюємо вдячність українським постачальникам електронних комунікаційних послуг, які сприяють доведенню інформації про кіберзагрози до абонентів та забезпечують функціонування засобів кіберзахисту Національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, що впроваджуються підрозділами Держспецзв’язку.

Слід зазначити, що розвиток штучного інтелекту суттєво спрощує реалізацію кіберзагроз. Відтак рекомендуємо відповідально поставитися до скорочення поверхні атаки як на зовнішньому мережевому периметрі інформаційно-комунікаційних систем, так і на рівні використовуваних засобів обчислювальної техніки, зокрема шляхом налаштування штатних засобів захисту операційних систем (наприклад, SRP, AppLocker) та застосування спеціалізованих програмних засобів захисту.

AGEWHEEZE

Програмний засіб типу RAT, розроблений із використанням мови програмування Go. Окрім стандартного для таких програм функціоналу, зокрема виконання команд і керування файлами, він підтримує передачу вмісту екрана, емуляцію введення з миші та клавіатури, роботу з буфером обміну, керування процесами та службами. Для забезпечення персистентності можуть використовуватися реєстр ОС, каталог Startup або ж заплановане завдання. У досліджених зразках первинне встановлення здійснюється за шляхами "%APPDATA%\SysSvc\SysSvc.exe" та "%APPDATA%\service\service.exe", а для підвищення привілеїв створюється заплановане завдання, зокрема "SvcHelper" та "CoreService". Для комунікації з сервером управління використовуються вебсокети. Перелік команд, що підтримуються програмним засобом:

- 0x11 - ScreenControl
- 0x20 - InputMouse
- 0x21 - InputKeyboard
- 0x30 - FileList
- 0x31 - FileRead
- 0x32 - FileWrite
- 0x33 - FileDelete
- 0x34 - FileRename
- 0x36 - FileMkDir
- 0x37 - FileExec
- 0x40 - SysInfo
- 0x41 - ProcList
- 0x42 - ProcKill
- 0x43 - ServiceList
- 0x44 - ServiceControl
- 0x45 - AutorunList
- 0x46 - AutorunAdd
- 0x47 - AutorunRemove
- 0x48 - Zip (archive files)
- 0x50 - SelfDelete
- 0x51 - ElevateIfNeeded
- 0x60 - TermControl
- 0x61 - TermInput
- 0x64 - CmdExec
- 0x70 - PowerAction (shutdown/restart/logoff/sleep/lock)
- 0x90 - ClipRead

- 0x91 - ClipWrite
- 0x92 - Env
- 0x93 - OpenURL

Індикатори кіберзагроз

Файли:

```
2f8f3e2860f76a630f514f435049764c              d42df7073f59c52b4450338c868c6cf58bc4c5bde1230dbcc046
4d210550b3073cff2a7fc2979a64277c              5f16463f5c463f5f2f69f31c6ce7d3040d07876156a265b55217
afbabb90e761451bb66a753ffd1ca92d              0d7147a08c70cf15428f4b3ed2f16587ec6f57b0d0be9e319796
e4fa3e55f77419c8d718d11e663a614c              468e0919ffb6c12444b77570e5cb68b1fe1e7d7a1aea2193b176
37631c6c5fce72ce0f75bf70c6f521b9              98f8ffdb5abc0b0bf11de72d7d904bacbc1834d3290d92f8f7cd
0e86fe5ea183a582e4cb8ffa39d3f14b              342cf215d7599a65b23398038f943f516b0bd649926e21427d8e
```

Мережеві:

```
hXXps://files[.]fm/u/7nxvfbmf46
hXXps://files[.]fm/u/cmr9kspbs5
incidents@cert-ua.tech
(wss)://54[.]36.237.92:8443
hiddify.creepy[.]ltd
panel.creepy[.]ltd
cert-ua[.]tech                          (2026-03-27; publicdomainregistry.com)
creepy[.]ltd                            (2026-01-21; reg.ru)
54[.]36.237.92                          (C2)
```

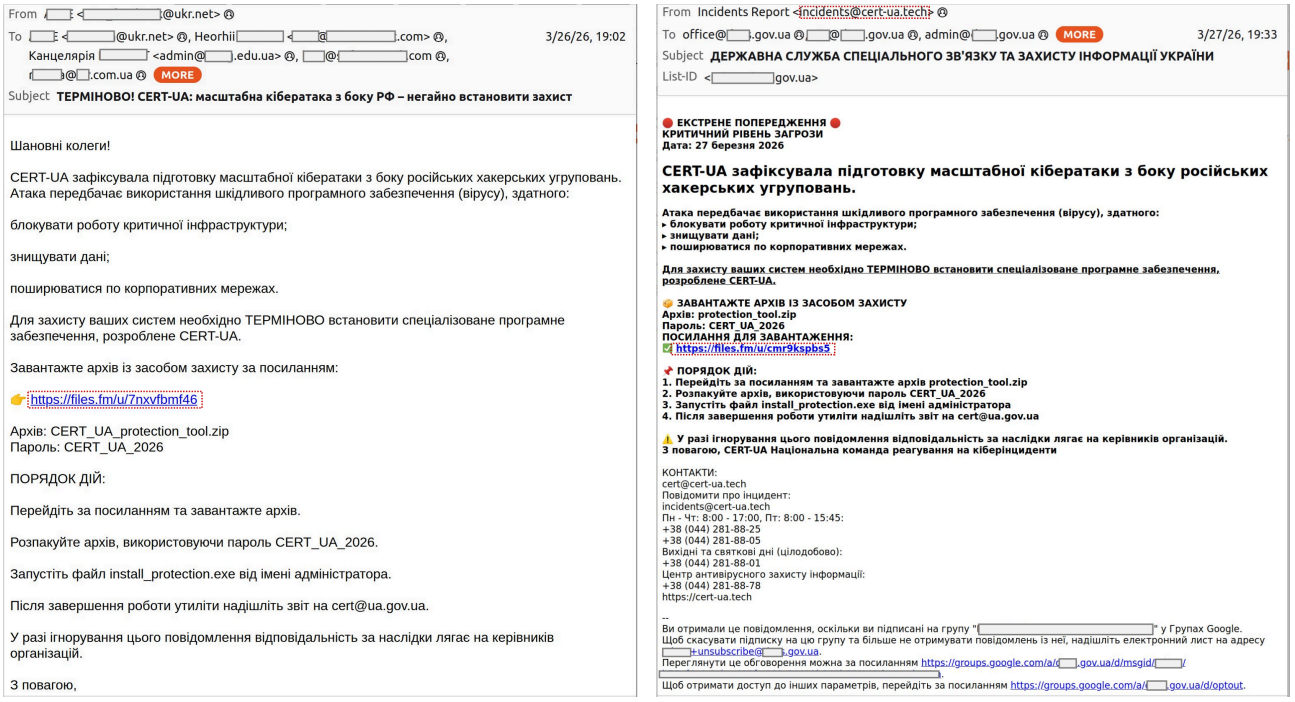
```
https://files.fm/u/7nxvfbmf46
https://files.fm/u/cmr9kspbs5
incidents@cert-ua.tech
wss://54.36.237.92:8443
hiddify.creepy.ltd
panel.creepy.ltd
cert-ua.tech
creepy.ltd
54.36.237.92
```

Хостові:

```
%APPDATA%\SysSvc\SysSvc.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\'SvcHelper'
SvcHelper (Scheduled Task)
%APPDATA%\service\service.exe
```

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\'CoreService'
CoreService (Scheduled Task)
```

Графічні зображення



From [redacted]@ukr.net
To [redacted]@ukr.net, Heorhii[redacted].com, Канцелярія [redacted] <admin@[redacted].edu.ua>, [redacted]com, [redacted].com.ua MORE
3/26/26, 19:02
Subject **ТЕРМІНОВО! CERT-UA: масштабна кібератака з боку РФ – негайно встановити захист**

Шановні колеги!

CERT-UA зафіксувала підготовку масштабної кібератаки з боку російських хакерських угруповань. Атака передбачає використання шкідливого програмного забезпечення (вірусу), здатного:

блокувати роботу критичної інфраструктури;

знищувати дані;

поширюватися по корпоративних мережах.

Для захисту ваших систем необхідно ТЕРМІНОВО встановити спеціалізоване програмне забезпечення, розроблене CERT-UA.

Завантажте архів із засобом захисту за посиланням:

👉 https://files.fm/u/7nxvfbmf46

Архів: CERT_UA_protection_tool.zip
Пароль: CERT_UA_2026

ПОРЯДОК ДІЙ:

Перейдіть за посиланням та завантажте архів.

Розпакуйте архів, використовуючи пароль CERT_UA_2026.

Запустіть файл install_protection.exe від імені адміністратора.

Після завершення роботи утиліти надішліть звіт на cert@ua.gov.ua.

У разі ігнорування цього повідомлення відповідальність за наслідки лягає на керівників організацій.

З повагою,

From Incidents Report <incidents@cert-ua.tech>
To office@[redacted].gov.ua, [redacted]@[redacted].gov.ua, admin@[redacted].gov.ua MORE
3/27/26, 19:33
Subject **ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ**
List-ID <[redacted].gov.ua>

🔴 **ЕКСТРЕНЕ ПОПЕРЕДЖЕННЯ** 🔴
КРИТИЧНИЙ РІВЕНЬ ЗАГРОЗИ
Дата: 27 березня 2026

CERT-UA зафіксувала підготовку масштабної кібератаки з боку російських хакерських угруповань.

Атака передбачає використання шкідливого програмного забезпечення (вірусу), здатного:
▸ блокувати роботу критичної інфраструктури;
▸ знищувати дані;
▸ поширюватися по корпоративних мережах.

Для захисту ваших систем необхідно ТЕРМІНОВО встановити спеціалізоване програмне забезпечення, розроблене CERT-UA.

📦 **ЗАВАНТАЖТЕ АРХІВ ІЗ ЗАСОБОМ ЗАХИСТУ**
Архів: protection_tool.zip
Пароль: CERT_UA_2026
ПОСИЛАННЯ ДЛЯ ЗАВАНТАЖЕННЯ:
✅ https://files.fm/u/cmr9kspbs5

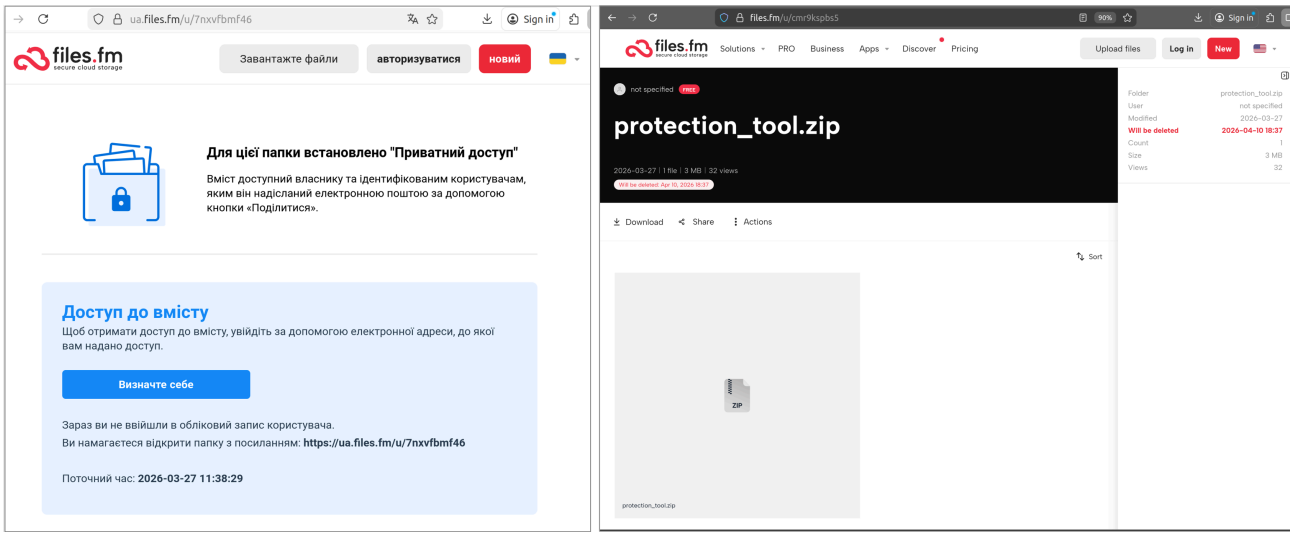
📌 **ПОРЯДОК ДІЙ:**
1. Перейдіть за посиланням та завантажте архів protection_tool.zip
2. Розпакуйте архів, використовуючи пароль CERT_UA_2026
3. Запустіть файл install_protection.exe від імені адміністратора
4. Після завершення роботи утиліти надішліть звіт на cert@ua.gov.ua

⚠️ **У разі ігнорування цього повідомлення відповідальність за наслідки лягає на керівників організацій.**
З повагою, CERT-UA Національна команда реагування на кіберінциденти

КОНТАКТИ:
cert@cert-ua.tech
Повідомити про інцидент:
incidents@cert-ua.tech
Пн - Чт: 8:00 - 17:00, Пт: 8:00 - 15:45:
+38 (044) 281-88-25
+38 (044) 281-88-05
Вихідні та святкові дні (цілодобово):
+38 (044) 281-88-01
Центр антивірусного захисту інформації:
+38 (044) 281-88-78
https://cert-ua.tech

--
Ви отримали це повідомлення, оскільки ви підписані на групу "[redacted]" у Групах Google.
Щоб скасувати підписку на цю групу та більше не отримувати повідомлень із неї, надішліть електронний лист на адресу [redacted]+unsubscribe@[redacted].gov.ua.
Перегляньте це обговорення можна за посиланням https://groups.google.com/a/[redacted].gov.ua/d/msgid/[redacted]/[redacted]
Щоб отримати доступ до інших параметрів, перейдіть за посиланням https://groups.google.com/a/[redacted].gov.ua/d/optout.

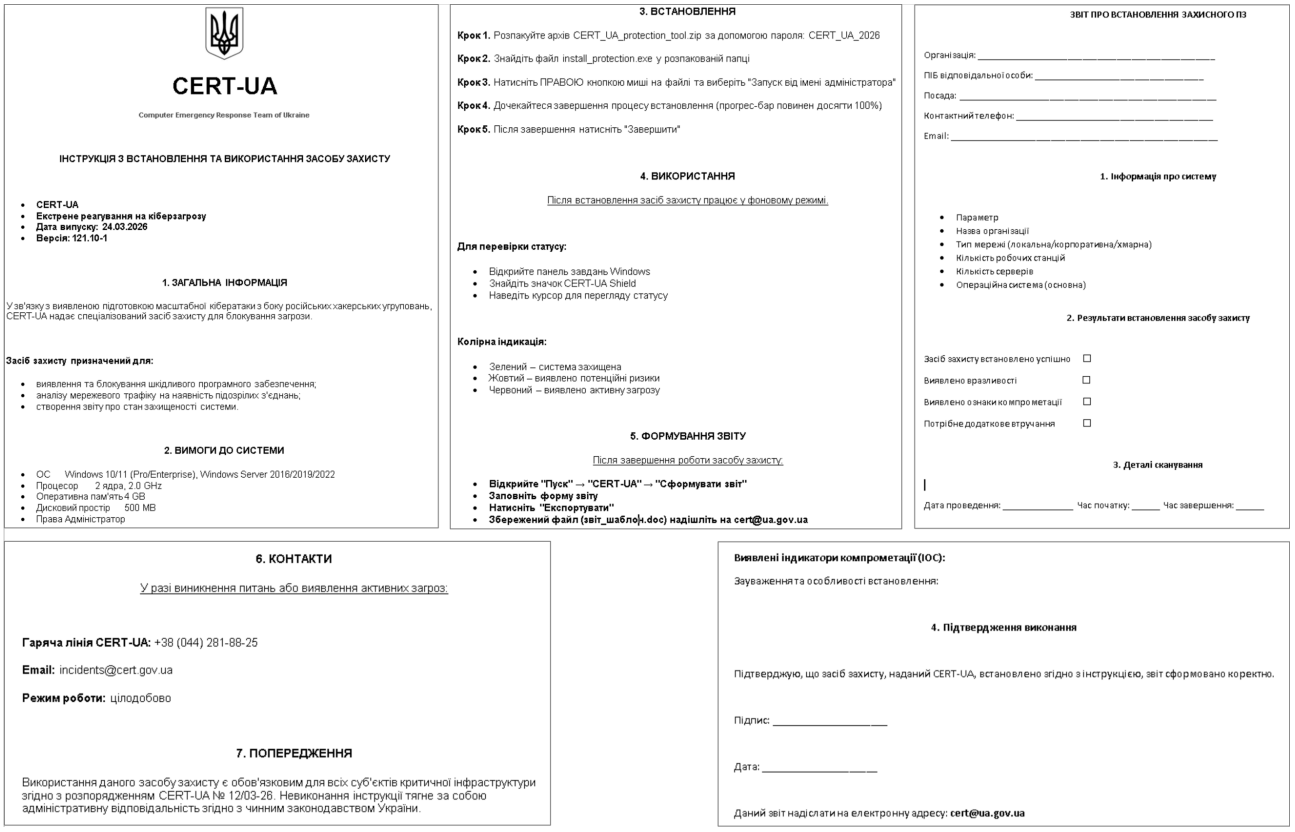
Рис. 1 Приклади електронних листів



ua.files.fm/u/7nxvfbmf46
files.fm secure cloud storage
Завантажте файли | авторизуватися | новий
Для цієї папки встановлено "Приватний доступ"
Вміст доступний власнику та ідентифікованим користувачам, яким він надісланий електронною поштою за допомогою кнопки «Поділитися».
Доступ до вмісту
Щоб отримати доступ до вмісту, увійдіть за допомогою електронної адреси, до якої вам надано доступ.
Визначте себе
Зараз ви не ввійшли в обліковий запис користувача.
Ви намагаєтеся відкрити папку з посиланням: https://ua.files.fm/u/7nxvfbmf46
Поточний час: 2026-03-27 11:38:29

files.fm/u/cmr9kspbs5
files.fm secure cloud storage
Solutions | PRO | Business | Apps | Discover | Pricing
Upload files | Log in | New
not specified
protection_tool.zip
2026-03-27 | 1 file | 3 MB | 32 views
Download | Share | Actions
Sort
Folder protection_tool.zip
User not specified
Modified 2026-03-27
Will be deleted 2026-04-10 18:37
Count 1
Size 3 MB
Views 32

Рис. 2 Використання сервісу Files.fm для розміщення архівів



CERT-UA

Computer Emergency Response Team of Ukraine

ІНСТРУКЦІЯ З ВСТАНОВЛЕННЯ ТА ВИКОРИСТАННЯ ЗАСОБУ ЗАХИСТУ

- CERT-UA
- Екстрене реагування на кіберзагрозу
- Дата випуску: 24.03.2026
- Версія: 121.10-1

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

У зв'язку з виявленою підготовкою масштабної кібератаки з боку російських хакерських угруповань, CERT-UA надає спеціалізований засіб захисту для блокування загрози.

Засіб захисту призначений для:

- виявлення та блокування шкідливого програмного забезпечення;
- аналізу мережевого трафіку на наявність підозрілих з'єднань;
- створення звіту про стан захищеності системи.

2. ВИМОГИ ДО СИСТЕМИ

- ОС Windows 10/11 (Pro/Enterprise), Windows Server 2016/2019/2022
- Процесор 2 ядра, 2.0 GHz
- Оперативна пам'ять 4 GB
- Дисковий простір 500 MB
- Права Адміністратор

3. ВСТАНОВЛЕННЯ

Крок 1. Розпакуйте архів CERT_UA_protection_tool.zip за допомогою пароля: CERT_UA_2026

Крок 2. Знайдіть файл install_protection.exe у розпакованій папці

Крок 3. Натисніть ПРАВОЮ кнопкою миші на файлі та виберіть "Запуск від імені адміністратора"

Крок 4. Дочекайтеся завершення процесу встановлення (прогрес-бар повинен досягти 100%)

Крок 5. Після завершення натисніть "Завершити"

4. ВИКОРИСТАННЯ

Після встановлення засіб захисту працює у фоновому режимі.

Для перевірки статусу:

- Відкрийте панель завдань Windows
- Знайдіть значок CERT-UA Shield
- Наведіть курсор для перегляду статусу

Колірна індикація:

- Зелений – система захищена
- Жовтий – виявлено потенційні ризики
- Червоний – виявлено активну загрозу

5. ФОРМУВАННЯ ЗВІТУ

Після завершення роботи засобу захисту:

- Відкрийте "Пуск" → "CERT-UA" → "Сформувати звіт"
- Заповніть форму звіту
- Натисніть "Експортувати"
- Збережений файл (звіт_шаблон.doc) надішліть на cert@ua.gov.ua

ЗВІТ ПРО ВСТАНОВЛЕННЯ ЗАХИСНОГО ПЗ

Організація: _____

ПІБ відповідальної особи: _____

Посада: _____

Контактний телефон: _____

Email: _____

1. Інформація про систему

- Параметр
- Назва організації
- Тип мережі (локальна/корпоративна/хмарна)
- Кількість робочих станцій
- Кількість серверів
- Операційна система (основна)

2. Результати встановлення засобу захисту

Засіб захисту встановлено успішно ☐

Виявлено вразливості ☐

Виявлено ознаки компрометації ☐

Потрібне додаткове втручання ☐

3. Деталі сканування

Дата проведення: _____ Час початку: _____ Час завершення: _____

6. КОНТАКТИ

У разі виникнення питань або виявлення активних загроз:

Гаряча лінія CERT-UA: +38 (044) 281-88-25

Email: incidents@cert.gov.ua

Режим роботи: цілодобово

7. ПОПЕРЕДЖЕННЯ

Використання даного засобу захисту є обов'язковим для всіх суб'єктів критичної інфраструктури згідно з розпорядженням CERT-UA № 12/03-26. Невиконання інструкції тягне за собою адміністративну відповідальність згідно з чинним законодавством України.

Виявлені індикатори компрометації (IOC):

Зауваження та особливості встановлення:

4. Підтвердження виконання

Підтверджую, що засіб захисту, наданий CERT-UA, встановлено згідно з інструкцією, звіт сформовано коректно.

Підпис: _____

Дата: _____

Даний звіт надіслати на електронну адресу: cert@ua.gov.ua

Рис. 3 Приклади вмісту документів-приманок

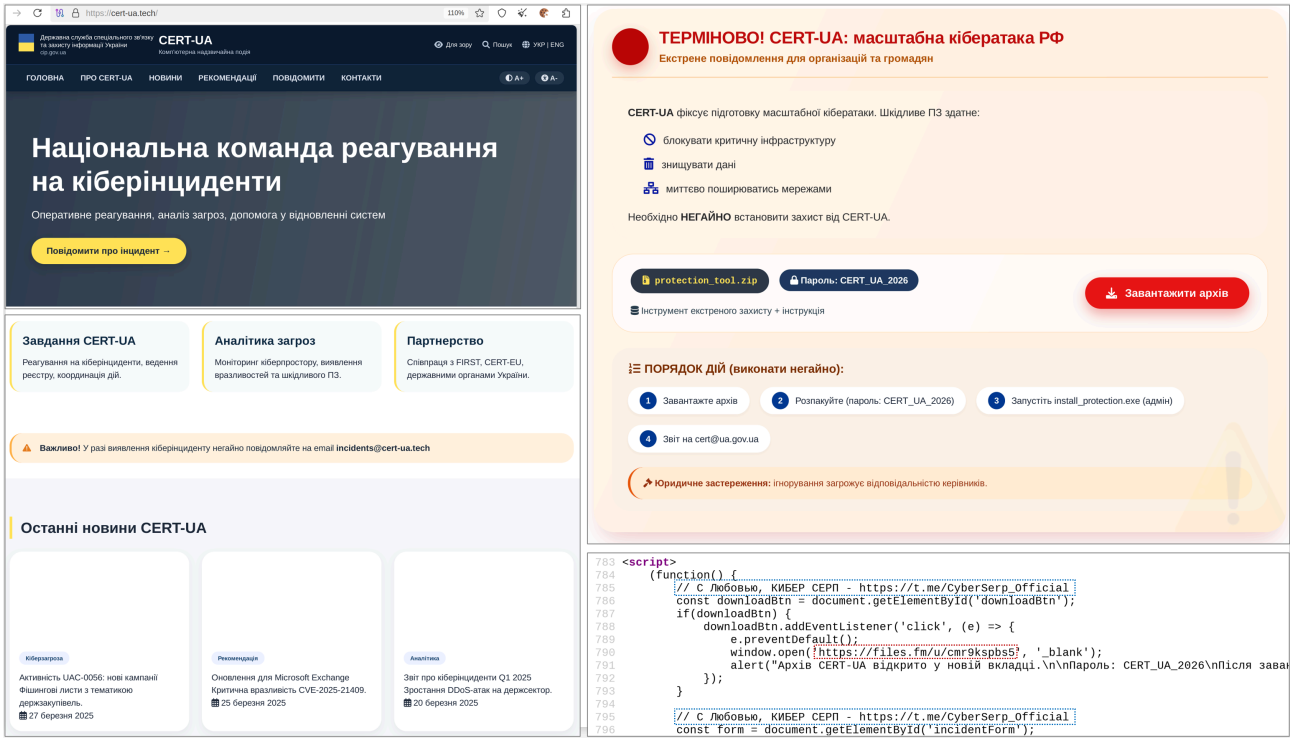


Рис. 4 Приклад фейкової вебсторінки hXXps://cert-ua[.]tech/

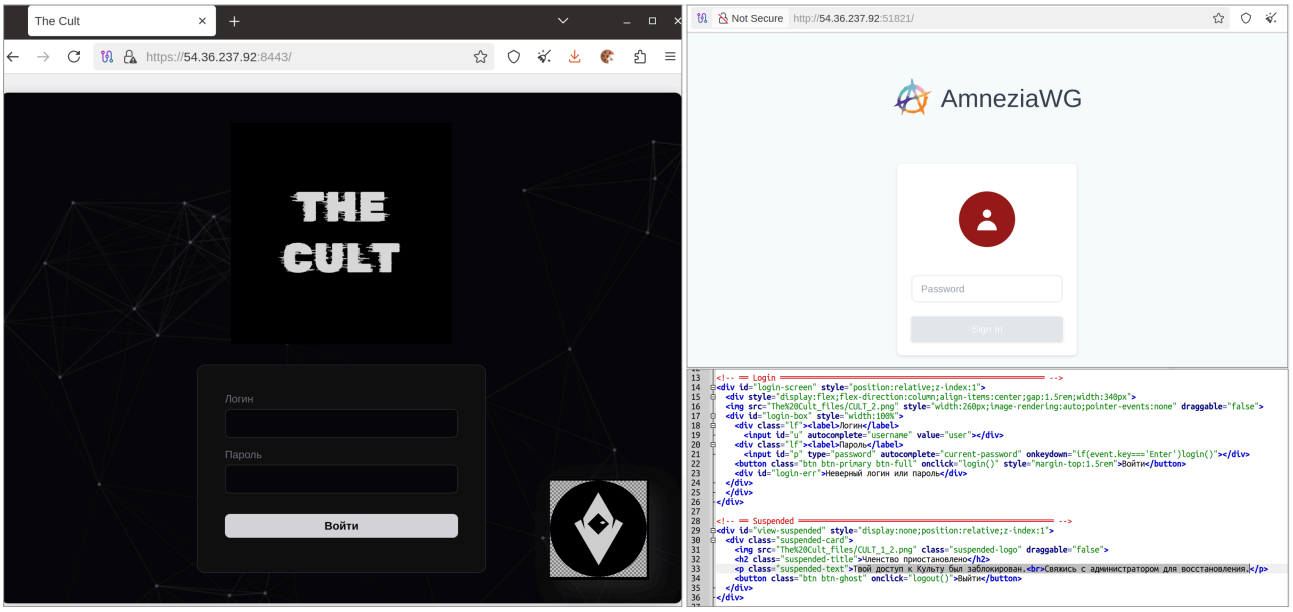


Рис. 5 Приклад вебпанелі, розміщеної на сервері управління

Source: https://cert.gov.ua/article/6288047