cert.gov.ua /article/6285549

Unknown Title

Загальна інформація

Національною командою реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA у вересні 2025 року виявлено низку програмних засобів, представлених у вигляді XLL-файлів зі специфічними

іменами, зокрема "Звернення УБД.xll", "recept_ruslana_nekitenko.xll". Такі файли є виконуваними (PE, Portable excutable) та, серед іншого, можуть завантажуватися Add-in менеджером Excel з використанням процедури (експортованої функції) "xlAutoOpen".

Згодом, від учасників інформаційного обміну отримано повідомлення щодо фіксації спроби розповсюдження засобами Signal файлу "500.zip" під виглядом документу щодо затримання осіб, які намагалися перетнути державний кордон України.

Згаданий архів містить XLL-файл "dodatok.xll", запуск якого забезпечить створення на комп'ютері декількох файлів, а саме: EXE-файлу з довільною назвою з 15-20 символів (внутрішня назва "runner.exe"), в т.ч. в каталозі автозапуску (Startup), XLL-файлу "BasicExcelMath.xll" (внутрішня назва "loader.xll") в каталозі "%APPDATA%\Microsoft\Excel\XLSTART\", та PNG-зображення "Office.png". При цьому, з метою забезпечення персистентності запуску EXE-файлу, буде створено ключ (з довільною назвою) в гілці "Run" реєстру Windows, а також заплановане завдання з довільною назвою. Додатково перевіряється значення в гілці реєстру "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\EXCEL.EXE" та видаляються значення з гілок "HKCU\Software\Microsoft\Office\ {14,15,16}.0\Excel\Resiliency\DisabledItems".

Основне призначення EXE-файлу - запуск EXCEL.EXE з параметром "/e" ("/embed") у прихованому режимі (без відкриття порожньої Excel таблиці). Ураховуючи створений на попередньому етапі файл "BasicExcelMath.xll", останній буде автоматично завантажено (виконано) програмою Excel.

Основне призначення XLL-файлу - зчитування "Office.png", пошук шелкоду та передача управління на нього (VirtualProtect + CreateThread). Шелкод класифіковано як програмний засіб CABINETRAT, що є повноцінним бекдором.

Слід зауважити, що у файлах "dodatok.xll", "loader.xll" та самому шелкоді імплементовано низку анти-VM та анти-аналіз процедур, зокрема:

- перевірка відсутності функції "wine_get_unix_file_name" в kernel32.dll;
- перевірка інформації BIOS (GetSystemFirmwareTable) на наявність характерних рядків: "VMware", "VirtualBox", "Xen", "QEMU", "Parallels", "Hyper-V";
- перевірка списку дисплеїв (EnumDisplayDevicesA) на наявність характерних рядків: "VMware", "VBox", "VirtualBox", "Virtual", "Microsoft Basic Display", "Parallels";
- перевірка наявності не менше двох ядер процесора і не менше 3ГБ оперативної пам’яті;
- кількаразове вимірювання та порівняння часу виконання CPUID за допомогою RDTSC;
- перевірка чи не закінчується SID облікового запису користувача на "500";
- перевірка флагу відладки в PEB.

Крім того, згадані файли використовують ідентичний спосіб обфускації - кожен рядок це масив 32-бітових індексів, за якими отримуються значення з відповідної таблиці.

Ураховуючи новизну в тактиках, техніках та процедурах, не беручи до уваги відомі випадки застосування XLL-файлів в цільових кібератаках, здійснених угрупуванням UAC-0002, зокрема, у відношення об'єктів критичної інфраструктури України, для відстежування описаної активності створено окремий ідентифікатор UAC-0245.

CABINETRAT

Програмний засіб, розроблений з використанням мови програмування C та представлений у вигляді шелкоду. Основний функціонал: отримання інформації про ОС та встановлені програми на ЕОМ, виконання команд, робота з файлами, виготовлення знімків екрану. Для взаємодії з сервером управління використовується протокол TCP; перед встановленням TCP-з'єднання здійснюються послідовні підключення на мережеві порти 18700, 42831, 20046, 33976 (може нагадувати "port knocking"). Дані передаються у вигляді пакетів, які (окрім типу 0) стискаються алгоритмом COMPRESS_ALGORITHM_MSZIP за допомогою Windows Compression API; у випадку, якщо розмір даних перевищує 65535 байтів, останні розбиваються на декілька фрагментів.

Основна логічна конструкція програмного засобу (типи пакетів):

0 - Ініціація підключення: відправка пакету типу 0 з рядком "Ninja", сервер відповідає пакетом типу 0 зі значенням "Bonjour";

1 - Виконання програми з відправкою результату на сервер;

2 - Відправка на сервер результатів успішно виконаних команд;

4 - Ексфільтрація файлу: вхідний пакет містить шлях до необхідного файлу;

5 - Отримання файлу з сервера: перший фрагмент містить шлях до необхідного файлу, в наступних фрагментах передаються дані;

6 - Відправка значень BIOS GUID після отримання "Bonjour" від сервера;

7 - Отримання інформації про ЕОМ (значення з гілки "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion");

8 - Отримання інформації про підключені диски;

9 - Отримання інформації про встановленні програми (значення гілок "HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall" та "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall");

10 - Отримання вмісту директорії: вхідний пакет містить шлях та маску пошуку;

11 - Отримання знімку екрану;

12 - Відправка на сервер коду помилки;

13 - Видалення файлу або директорії: вхідний пакет містить шлях до необхідного об'єкта.

Індикатори кіберзагроз

Файли:

```
81f42481017489f0f92589c86797f897
19f54a95737182ba63b189f56ac9df046984efbaebb9ffc8bab63246f83b7641
Звернення УБД.xll
ab538c3f9e60a415ddb0b1a63d949505
fe07542413e38358eecae83b490d2dfa9c899bfb89c56b7cf6a350f916bb7cba
spreadsheet.xlsx
2b9b72f342c0c6d30e601d089c2317cd
cc9a50e2e6a6456c9f8b86f3ba4451cd7306c57ca9c4377ca0e29b357e1b1dd5
runner.exe
531f95c191783ae3e71cefd6242046c0
b81b3bc94f8849f951f1c5883c271aa639bb12ff6e09a9b5f63b2c9140469877
loader.xll
6bebcf3b0fb3f36bd0e4b20a10c6bd08
bac9e042b9e4433c5d3a50f23be990ae59b326c162ac7ad81cdc1fce11f98fe0
Office.png (містить шелкод CABINETRAT)

50648a1be6d80c9d193d2ad40c7f3cc6
16f6fb64cbb24f1d5853acc4918000c4bc93e15f1336c9427feff20b80294c2a        500.zip
33740666bf5489f5da80936f48f0dca4
ab3ff2a36a5c34e90b76421e5ee68fc29e5f2b541341fc008e2083d9130d5d6d
spreadsheet.xlsx
ead3b4e939fff983b99f9fcb275188f8
f616d6581acbe9f53317a6482e3efbf28643ce19554db2122f1d1285c0f854a6
runner.exe
836073b5aedb33a4e8e9f7cedb649b15
d69528e2b06801383668e3ede868bad6dbad83a89bce0f1818a91c754001a58d
dodatok.xll
e7ca716a01e5acf698a9bd07a0f50bef
af79b600ad113df92a76bc51c61a9d775b11a146bc8dac326ae22107331443d5
loader.xll
61098aa344ff34a1a9c5efab336f0ef7
e70dd343ea3897409deac26ca2b9dca09209d162e0dfe11e69f119527ffeb0bd
Office.png (містить шелкод CABINETRAT)
```

82d88529fc14719a736c5d76ef974e9e
033898b5adc8bd8bd8f5209b6af4043835c6c2b2e1939891a7eb21b7525fcc9c
82d88529fc14719a736c5d76ef974e9e.zip
23051468091526bb5a810f9a9e9e0cca
15e40d67b85110c2a421c44a0c88b62c1911ba8f6cc1a9d1c1f2bceefdcb656e
Рапорт.xll
9aaf31e8bf60f9872ec42ab523b97ead
11e8e7bdfa114d2e585dea73b9a3275878c48597a3b5be400dedf01a779b8455
spreadsheet.xlsx
962cf8d0041711c48d5d2ce5b9ac8446
8cd808e2601430fea91e36630304fc1483639c8845ef60c13afd86217bf7d446
runner.exe
1ac96dbb9914e2e03d392482a9b82b0d
489371f4a33164b60c99554c028e1b880ff17ec538cd44b383e4167bb6215b96
loader.xll
a2d195bf836b61974a8dfe7ca50e1161
a1c9ca9f83bffb0c00123667949be2fec74b94d2dc3306fa572593f65de05547
Office.png (містить шелкод CABINETRAT)
ce99e5a556f8a18b5ce0ace6a789975a
cbefa5a93ae0f6634b53a2c5bd9a6d864a1a35c4452cb2ebe5347c2e9311d0b9
Звернення УБД.xll
3f75eba2acfc24ea384dc39306596e81
fd8bd724c062c808bb9f872ad5351bbb0eb28fe7b5e2e05acf43aa66b47a1796
spreadsheet.xlsx
974ed91212685f59e4674bf32af683ea
b74dc23dd11a66e0a92ffb8616fb4f137be14964dca9bf70362ddafc81fa66cb
runner.exe
399b3bc8a1c3c000e5b6e7335c7e28a1
d749932f68ec6186480af5f3e4d284ff9d0e03d26de0fba0533db84c4f4b6bd5
loader.xll
172abe81452aa2069ee34648cbb09d52
3c3761cf92f0a36181d86d936cad32f9effd774705d602c5dffde1d1c6cfea25
Office.png (містить шелкод CABINETRAT)

Хостові:

%APPDATA%\Microsoft\Excel\XLSTART\BasicExcelMath.xll
%APPDATA%\Microsoft\Office\<RAND15-20CHARS>.exe
%APPDATA%\Microsoft\Office\Office.png
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\<RAND15-20CHARS>.exe
%EXCEL_PATH%\excel.exe /e

```
%LOCALAPPDATA%\Microsoft\Office\<RAND15-20CHARS>.exe
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'<RAND15-
20CHARS>'
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DisabledItems
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Resiliency\DisabledItems
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Resiliency\DisabledItems
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths\EXCEL.EXE
schtasks /create /sc hourly /mo 12 /tn "<RAND_NAME>" /tr
"%LOCALAPPDATA%\Microsoft\Office\<RAND15-20CHARS>.exe" /f /RL LIMITED /IT
```

Мережеві:

```
(tcp)://20[.]112.250.113:443
(tcp)://20[.]70.246.20:433
20[.]112.250.113
20[.]70.246.20
```

```
tcp://20.112.250.113:443
tcp://20.70.246.20:433
20.112.250.113
20.70.246.20
```

Графічні зображення

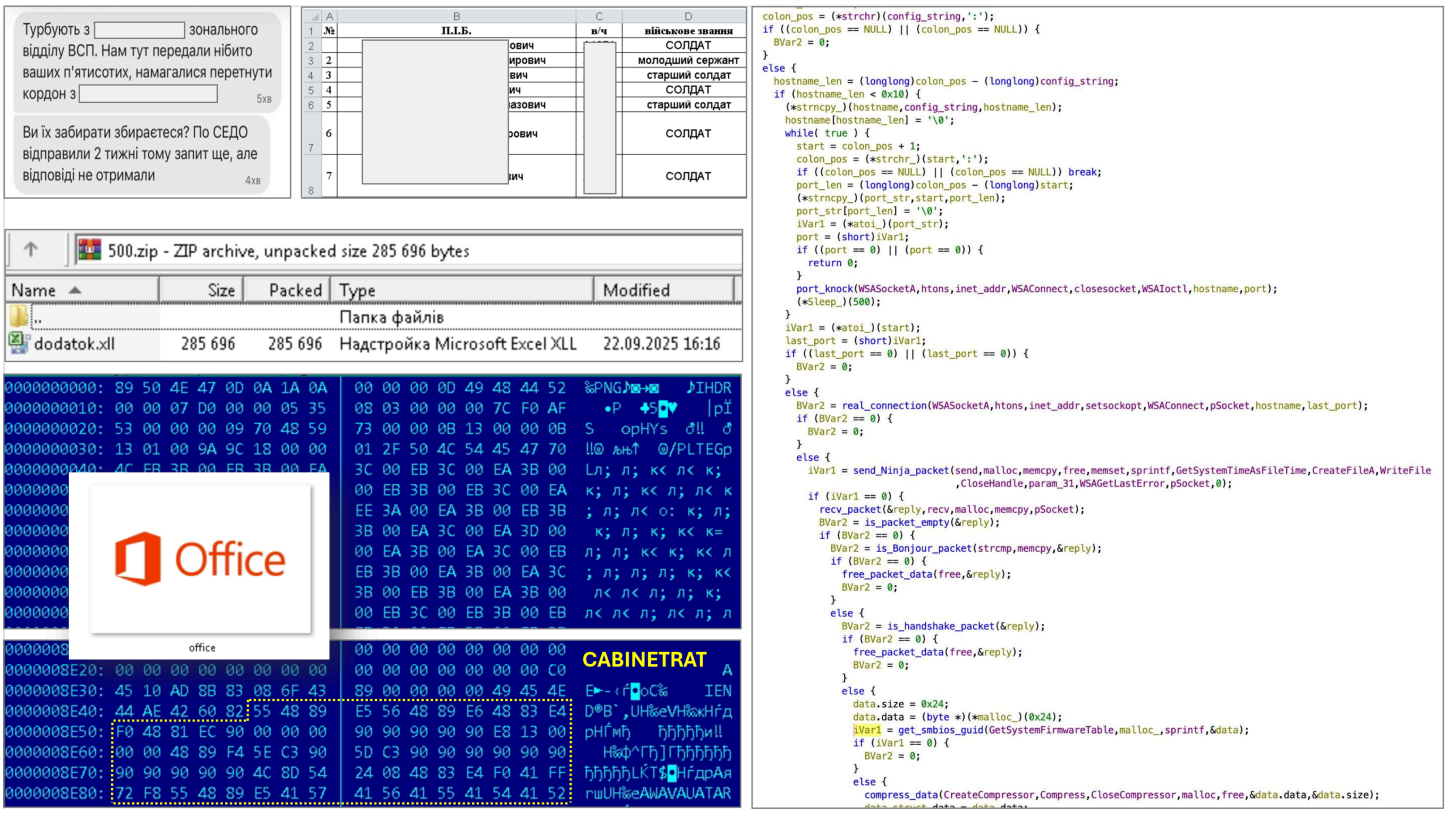

Рис. 1 Приклад електронного листа та файлу-приманки