CERT-UA

Archived: 2026-04-05 16:13:46 UTC

CERT-UA при дослідженні інформації про кіберінциденти спостерігає збільшення кількості кібератак з використанням шкідливого програмного забезпечення (далі - ШПЗ) Pterodo хакерського угрупування Armageddon/Gamaredon, яке пов’язують з урядом РФ.

В зазначеній статті наведено результати дослідження декількох семплів ШПЗ Pterodo, які використовувались у недавніх кібератаках на державні органи України.

Сценарій 1

Особливістю кібератак було використання для розповсюдження інфікованих файлів «Microsoft Word» системи електронного документообігу на базі програмного забезпечення «АСКОД», яку використовує велика кількість організацій України.

Сценарій атаки наступний.

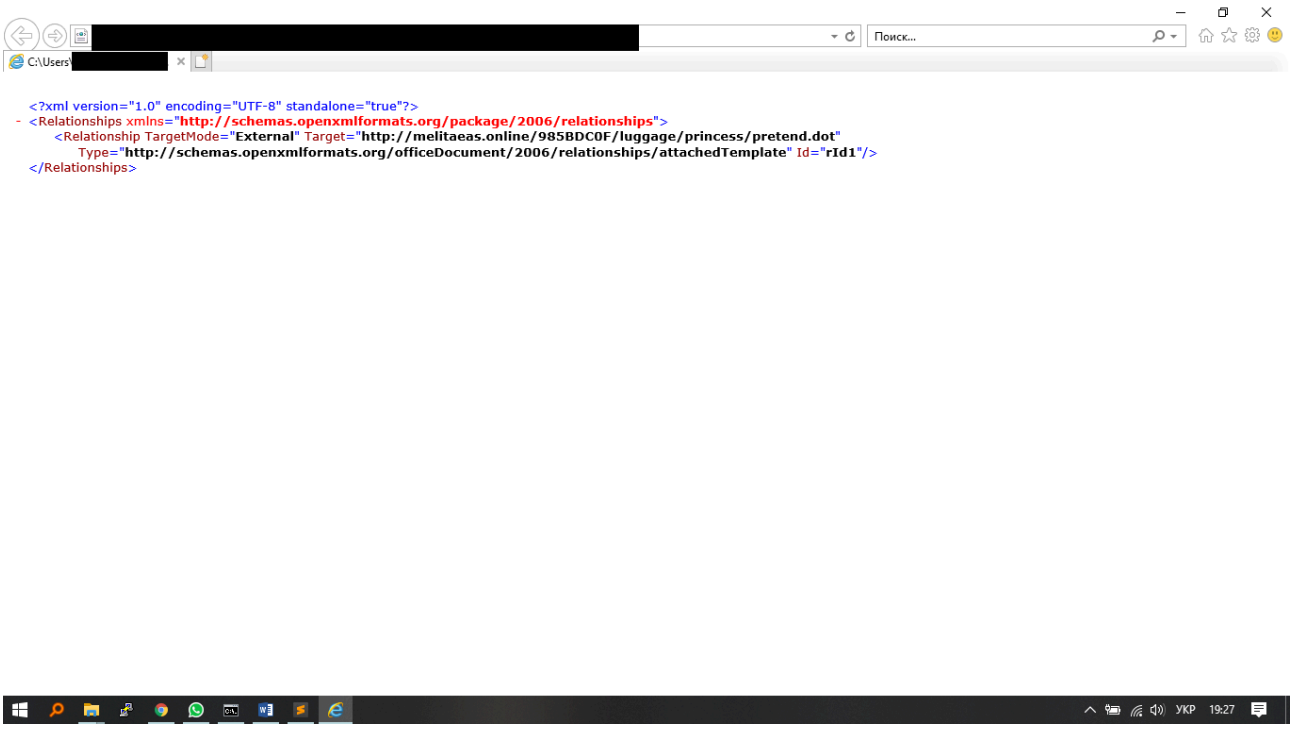
Зловмисники надсилають інфіковані документи до організації, які використовують «АСКОД». Для цього можуть використовуватись або скомпрометовані облікові записи користувачів «АСКОД», або користувачі із заражених Pterodo комп’ютерів самі відсилають інфіковані документи не знаючи цього.

Принцип роботи «АСКОД» такий, що при конвертації документу на сервері організації, в залежності від конфігурації може використовуватись програмне забезпечення «Microsoft Office». При такому використанні «Microsoft Office», «АСКОД» отримує доступ до командної строки з правами адміністратора та відкриває документ за допомогою WINWORD.EXE. Якщо на сервері використовується неоновлена версія «Microsoft Office», яка містить вразливості або в ньому дозволено використання макросів, документ з ШПЗ запуститься на сервері, використає вразливість або виконає макроси та інфікує робочі станції або сервери.

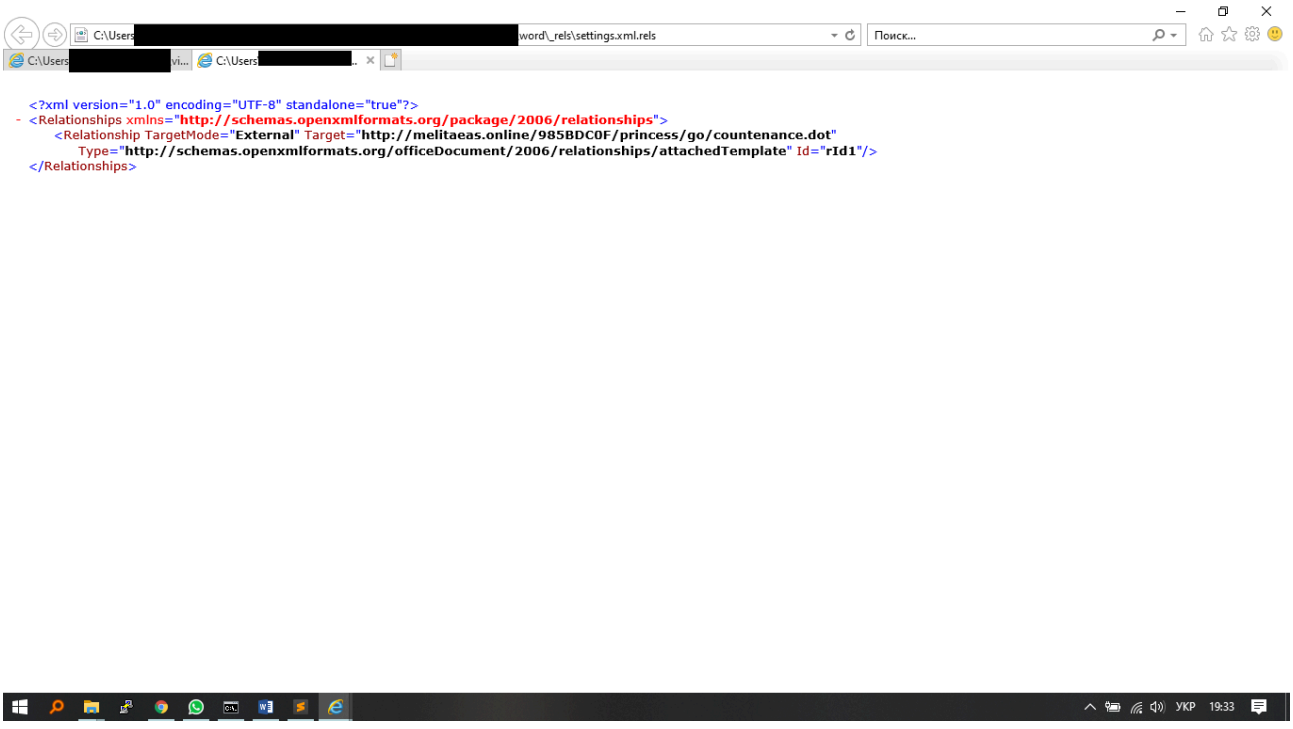
Використання в системах електронного документообігу на робочих станціях або серверах неоновлених/ неліцензійних версій «Microsoft Office», та відсутність встановленого антивірусного програмного забезпечення є потенційною критичною загрозою, яка використовувалась зловмисниками для зараження серверів, на яких встановлено «АСКОД».

Документи, які надсилались таким чином містили шкідливий код для експлуатації відомої вразливості «Microsoft Office» CVE-2017-0199 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199), що надає змогу зловмиснику виконати довільний код на пристрої користувача, при відкритті інфікованого файлу.

При відкритті документу, кінцевий пристрій встановлює з’єднання з командно-контрольним сервером http://melitaeas.online використовуючи модифікований \word_rels\settings.xml.rels файл. Вміст відповідного файлу наведено нижче:

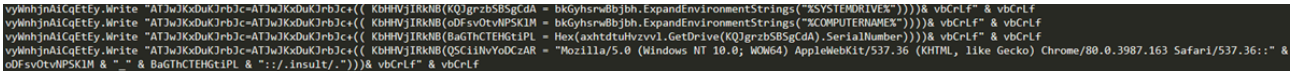


або



За допомогою відповідних налаштувань, в разі відсутності оновлень безпеки, що були опубліковані у квітні 2017 року на офіційному вебсайті Microsoft, на комп’ютер жертви автоматично завантажуються файли з розширенням .dot, що містять у собі шкідливий програмний код у вигляді макросу та ініціюється виконання коду.

Макрос містить у собі VBScript, що ініціює встановлення завантажувача (downloader) в систему, який надає командно-контрольному серверу (далі – C2) інформацію щодо назви пристрою, назви накопичувача та його серійного номеру, та отримує відповіді у вигляді програмного коду, що записується в оперативну пам'ять пристрою.



Після ініціалізації відповідного шкідливого програмного коду в системі створюються файли з розширенням .exe та .vbs, що мають конкретний шлях запису, наразі відомі таки директорії:

%PUBLIC% \Documents\

%APPDATA%\Microsoft\

Зокрема у системі створюються правила щодо регулярної ініціалізації сформованих файлів:

schtasks /Create /SC MINUTE /MO 15 /F /tn PublicFolderDownload /tr \Documents\inspection.exe //b \Documents\inspection.vbs, 0, False.

Після його ініціалізації, в системі строюються файли з такими фіксованими назвами: 6045.cmd.

6045.cmd – файл, що створює файли Say.vbs, Say.exe, yIaCaZTYKozaEDs.txt, BFXKwVzWGhXtYrG.vbs, saved.exe, завантажує scaffold.exe з **http://tridiuma.ru/scaffold.php**.

Після цього у планувальнику завдань відбувається встановлення з’єднання з командно-контрольним сервером, кожні 13 хвилин:

schtasks /Create /SC MINUTE /MO 13 /F /tn HelpOffice /tr "%APPDATA%\Microsoft\say\say.exe //b %APPDATA%\Microsoft\say\say.vbs"

Say.vbs перевіряє доступність до хосту "tridiuma.ru" за допомогою команди ping: C:\Windows\SysWOW64\PING.EXE ping **tridiuma.ru**

За допомогою адреси, що була використана для відповіді на команду ping, формується GET запит на отримання файлу "schedule.php", який зберігається до файлу "C:\Users\askod\AppData\Roaming\Microsoft\say\scaffold.exe". Запуск файлу scafold.exe

32154.vbs створює файли UserSupport.cs, UserSupport.bin. наступні файли отримують код з наступного ресурсу: **http://barbatus.online/get.php**. Після цього відбувається пошук усіх файлів в директорії C:\Windows\Microsoft.NET\Framework\v4.* та запис результату до 1.txt.

Відбувається компіляція UserSupport.cs завдяки csc.exe(компілятор C#) та відтворення результатів до UserSupport.exe.

Також створений UserSupport.exe додається до планувальника завдань на вконання кожних 5 хвилин:

SCHTASKS /CREATE /sc minute /mo 5 /tn "" /tr "%USERPROFILE%\UserSupport\UserSupport.exe" /F

VBS скрипт 7104.vbs є копією 32154.vbs та виконує аналогічні функції.

Файл UserSupport.exe націлений на дослідження хосту. Таким чином, завдяки йому відбувається дослідження файлової системи(перебір та визначення наявності папок та файлів) та визначення її стану. Дані файли взаємодіють з **http://188.225.37.128/index.php** (РФ).

Сценарій 2

У цьому випадку метод розповсюдження був більш звичайний – для зараження використовувались фішингові розсилки електронних листів зі шкідливими вкладеннями. Користувачі заражених пристроїв самі того не підозрюючи створювали документи, які містили шкідливий код та відправляли їх за допомогою легітимної робочої пошти, ща збільшувало вірогідність відкриття шкідливих листів.

У цьому випадку також експлуатувалась вразливість CVE-2017-0199 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199).

При відкритті інфікованого документу «Microsoft Word» кінцевий пристрій встановлює з’єднання з командно-контрольним сервером та завантажує файл з розширенням .dot, що містить у собі шкідливе програмне навантаження. Після його ініціалізації, в системі створюється виконуваний файл, з псевдовипадковою назвою, проте незалежно від назви містить у собі VBScript, з назвою 27270.

Після його ініціалізації, в системі строюються файли з такими фіксованими назвами: satisfy.exe, satisfy.vbs, savagely.exe, 3070.cmd, scenes.exe, TjAaneBEaKsklpl.vbs, 7ZSfx000.cmd, D6BDA66A.tmp та TdJIPGeKMNeyqOh.txt.

TjAaneBEaKsklpl.vbs звертається до командно-контрольних серверів **http://optica-rd.myftp.biz/satisfy.php** та **188.225.58.175/savagely.php** за запитом POST (домен та IP адреса знаходяться в РФ).

Файл satisfy.vbs звертається до командно-контрольних серверів **http://graphiuma.online/hat.php** та **185.119.59.227/phone.php** за запитом GET.

Файл savagely.exe створюється в системі відповідно до отриманих даних з контрольно-командного сервера, **http://graphiuma.online/hat.php**.

Файл scenes.exe, являє собою копію файлу System32\WScript.exe, а satisfy.exe, в свою чергу є копією scenes.exe.

Файл 7ZSfx000.cmd містить у собі наступні команди, де vcqkmwhafaky.exe – відповідний виконуваний файл з псевдовипадковою назвою, що містить у собі VBScript.

```
:Repeat
del "C:\Users\Administrator\AppData\Local\Temp\IT4N2ATA\vcqkmwhafaky.exe"
if exist "C:\Users\Administrator\AppData\Local\Temp\IT4N2ATA\vcqkmwhafaky.exe" goto Repeat
del "C:\Users\ADMINI~1\AppData\Local\Temp\7ZSfx000.cmd"
```

Файл 3070.cmd, є копією відповідного виконуваного файлу з псевдовипадковою назвою, що містить у собі VBScript.

Також запускається процес перевірки доступності з’єднання кінцевого пристрою з мережею інтернет:

C:\Windows\SysWOW64\PING.EXE ping 127.0.0.1

та у планувальнику завдань прописується встановлення з’єднання з командно-контрольним сервером, кожні 13 хвилин

@schtasks /Create /SC MINUTE /MO 13 /F /tn HelpOffice /tr satisfy.exe //b satisfy.vbs

Зокрема, під час аналізу файлової системи було виявлено такі файли на інфікованому кінцевому пристрої, що працюють аналогічно до зазначених вище:

C:\Users\user\AppData\Roaming\Microsoft\casks.exe – файл є копією системного файлу System32\WScript.exe.

C:\Users\user\AppData\Roaming\Microsoft\casks.vbs

Відповідний VBScript звертається до командно-контрольних серверів http://dipteran.online/napoleon.php та http://dipteran.online/saucer.php за запитом GET та формує відповідно до їх відповіді в системі файл hasten.exe та ініціює його запуск.

C:\Users\user\AppData\Local\Temp\24180-9520.vbs

C:\Users\user\AppData\Local\Temp\24214-30768.vbs

Відповідні два файли звертаються за методом POST до **hxxp://apoxipodes.ru/straightforward.php**.

Висновок

Активність хакерського угрупування Armageddon/Gamaredon в Україні збільшується з кожним роком. Для реалізації своїх кібератак вони шукають нові методи та техніки і використовують фішингові листи та документи створенні спеціально під конкретні організації.

Негативними наслідками реалізації подібних кібератак, за умов відсутності антивірусного програмного забезпечення та/або несвоєчасного встановлення оновлень програмного забезпечення, що використовується на робочих станціях та серверах організацій, можуть бути:

- отримання зловмисниками адміністративного доступу до інфікованого серверу та/або робочих станцій (розміщення бекдорів);

- інфіковані сервери та робочі станції стають джерелом подальшого розповсюдження ШПЗ в інші інформаційні та інформаційно-телекомунікаційні системи державних органів;

- наявність доступу зловмисника до інфікованих ресурсів може призвести до витоку інформації (файлів, електронних документів, паролів до облікових записів тощо);

- на завершальній стадії кібератаки може відбутися шифрування даних чи файлової системи з метою приховування дій зловмисника або вимагання викупу за розшифрування.

Рекомендації

1. Забезпечити невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки.

Контактні дані:

email: cert@cert.gov.ua

тел: (044) 281-88-05 (044) 281-88-05 (044) 281-88-01(цілодобово)

форам для повідомлення про кіберінцидент: https://cert.gov.ua/contact-us

2. Використовувати лише ліцензійне програмне забезпечення та своєчасно оновлювати його.

3. Використовувати антивірусне програмне забезпечення з актуальною антивірусною базою. Забезпечити регулярну повну перевірку системи на предмет наявності шкідливих програм.

4. Забезпечити негайне відключення інфікованих серверів та робочі станції від локальної обчислювальної мережі.

5. Забезпечити розмежування інформаційних систем на відокремлених обчислювальних ресурсах.

6. При отримані повідомлення електронною поштою, якщо ім'я чи адреса відправника, або зміст повідомлення викликають підозри, не відкривати прикріплені файли та не переходити за посиланнями.

7. Налаштувати фільтрування вхідних/вихідних інформаційних потоків, наприклад заборонити отримання працівниками повідомлень електронної пошти, що містить в додатках виконувані файли.

8. Налаштувати SPF, DKIM та DMARC для зменшення випадків отримання спаму, реалізації спуфінгу та інших кібератак.

9. Обмежити права доступу користувачам, заборонити ініціалізацію файлів з правами адміністратора.

10. Використовувати поштові клієнти для роботи з сервісами електронної пошти.

11. Політики інформаційної безпеки повинні містити вимогу щодо обмеження використання флеш-носіїв, у тому числі їх перевірку антивірусним програмним забезпеченням.

12. Заборонити стандартні сервіси шифрування операційної системи, що не використовуються, для унеможливлення використання їх шифрувальниками.

13. Обмежити можливість запуску виконуваних файлів (*.exe, *js, *.com, *.bs, *jar, *.vbs і т.д.) на пристроях з директорій Temp, AppData.

14. Заборонити чи обмежити використання макросів в програмному забезпеченні Microsoft Office.

15. Обмежити чи заборонити використання powershell.

16. На регулярній основі забезпечити процес резервного копіювання програмного забезпечення та критичних даних на відокремлених ресурсах.

Індикатори компрометації

Сценарій 1

Файлова система

C:\Users\user\AppData\Roaming\Microsoft\

C:\Users\user\AppData\Local\TEMP\servicehubs

C:\Users\user\AppData\Local\

%PUBLIC% \Documents\

%APPDATA%\Microsoft\

%windir%\SysWOW64\

%APPDATA%\Microsoft\Office\

%TEMP%

SHA-1: 7641A24A6F84ADC89BB29855F979F7AEC474B90D (Index.html)

SHA-1: 54ddcbc4b743255c5b1a742a3a16af6e65a4c078 (abominable.exe)

SHA-1: 04893332e1fac997d2dc6062ed10460d79402bef (insist.vbs)

SHA-1: b4e21d2ef8cfdde74550b184ec40b74143df0515 (scarf.exe)

SHA-1: f4be7384c04d2bae7a37fd475028a8e668f09f49 (UserSupport.exe)

SHA-1: 00635F771B861FAAFE1A7A70C6D452C460CED6A7 (BFXKwVzWGhXtYrG.vbs)

SHA-1: F4EACFBA8F23391EF14392444A75A28B451B7000 (1.txt)

SHA-1: F68CE31B69959C93EE9BEF230EE2F4A8B8EF4A16 (countenance.dot)

SHA-1: F68CE31B69959C93EE9BEF230EE2F4A8B8EF4A16 (pretend.dot)

SHA-1: 54DDCBC4B743255C5B1A742A3A16AF6E65A4C078 (abominable.exe)

SHA-1: 04893332E1FAC997D2DC6062ED10460D79402BEF (insist.exe)

SHA-1: D30313685658184449C34796798CE355128B3A21 (inspection.vbs)

SHA-1: 58D94FDEE57786858DE5F6B9268BFE326D360EC9 (MultiDrives.exe)

SHA-1: D26A907EEFE2D0299DF8DB81F6A46F2E1615BD04 (say.exe)

SHA-1: BCD274BEBB48FC25862698173C8150148263D618 (say.vbs)

SHA-1: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709 (scaffold.exe)

SHA-1: C0280CE9D05ECFAFC0ADC5E5EC92BE362094E7D8 (UserSupport.bin)

SHA-1: 515F86C9BF74A6E277238FD19E03451EDA0C6322 (UserSupport.cs)

SHA-1: 73CB6707F9C99211A0A71EBD70D665FB106123AE (Index.vbs)

SHA-1: 8C135B6A6282FD8E8CF584AA5C32CF4386B89790 (Index5A9A-8104.cmd)

SHA-1: 8C135B6A6282FD8E8CF584AA5C32CF4386B89790 (SID-5A9A8104.exe)

SHA-1: BC9D60AF6AF0EB632D9037967DB3AAD9956B718E (WebMedia.vbs)

SHA-1: B7161836FF12A44EC5ADC9537096A68CB4C32474 (abroad.vbs)

SHA-1: 48E50F75E31DAA7054086ABD58A3DD858BCE2195 (street.vbs)

SHA-1: 802233F29918A04EBA0E97970144996EFAA72A4E (jessie.vbs)

SHA-1: E66575467275CED94DAEE25DC6CC16ACC68A3522 (RemoteWinRar.vbs)

SHA-1: 479A69B5AB8815C0E79731833F5F70D8A5CE95D8 (4529)

SHA-1: 46E28173484036D2B3EDE44DF8DC0AF9313C5191 (6045.cmd)

SHA-1: 6333C64FB9D7B1DEAB16D514830BF89B69895E82 (7104.vbs)

SHA-1: F283A10A138CAF8F8D693B24FC9F613F00BBEC0D (32154.vbs)

SHA-1: D26A907EEFE2D0299DF8DB81F6A46F2E1615BD04 (saved.exe)

SHA-1: 5BE05DDECF4804A895CD6CDF2D183EC8D8E0AE9A (yIaCaZTYKozaEDs.txt)

SHA-1: 9AF13791AA1973786AA2D9A909DF66EB3D96BBC0 (DECLARATION.lnk)

Планувальник завдань

@schtasks /CREATE /sc minute /mo 5 /tn "" /tr "%USERPROFILE%\UserSupport\UserSupport.exe" /F

@schtasks /Create /SC MINUTE /MO 13 /F /tn HelpOffice /tr "%APPDATA%\Microsoft\say\say.exe //b %APPDATA%\Microsoft\say\say.vbs".

@schtasks /Create /SC MINUTE /MO 15 /F /tn PublicFolderDownload /tr \Documents\inspection.exe //b \Documents\inspection.vbs, 0, False

@schtasks /create /SC MINUTE /MO 20 /TN 'Firefox Compability check' /TR '\'C:\Users\Public\Temp\scarf.exe

Посилання

hxxp://melitaes.online/985BDC0F/luggage/princess/pretend.dot

hxxp://melitaes.online/985BDC0F/luggage/princess/countenance.dot

hxxp://emterox.ru/infant.php

hxxp://tridiuma.ru/schedule.php

hxxp://barbatus.online/get.php

hxxp://188.225.37.128/index.php

hxxp://acteran.ru/striped?

hxxp://omyce.ru/index.html

Домени та IP адреси

188.225.37.128

195.62.53.63 (circulas.ru)

109.68.212.97

melitaes.online

emterox.ru

ryomy.ru

erwini.ru

89.223.124.22 (tridiuma.ru)

109.68.214.176 (barbatus.online)

89.223.124.22 (candidar.ru)

89.223.124.22 (omyce.ru)

89.223.124.22 (acteran.ru)

109.68.214.176 (mulleti.ru)

109.68.214.176 (sardanal.online)

Сценарій 2

Файлова система

%WorkingDir%\IdmPyYVUudYaVF.dot

27270

SHA-1: 73B289EFE5109946DFDB6C1F369F8D82ACBD0909

C:\Users\user\AppData\Local\Temp\TdJIPGeKMNeyqOh.txt

SHA-1: 691295BF2C8FF344F0241A98512ABF01285182DC

C:\Users\user\AppData\Roaming\Microsoft\satisfy\satisfy.vbs

SHA-1: 1900B6BBA95E7E6A27BD86E6454C7808F6777120

C:\Users\user\AppData\Roaming\Microsoft\satisfy\satisfy.exe

SHA-1: 7FD5A5D1A8E673FAC52C74C475AA71BD73B4BED2

C:\Users\user\AppData\Local\Temp\3070.cmd

SHA-1: 73B289EFE5109946DFDB6C1F369F8D82ACBD0909

C:\Users\user\AppData\Local\Temp\scenes.exe

SHA-1: 860265276B29B42B8C4B077E5C651DEF9C81B6E9

C:\Users\user\AppData\Local\Temp\TjAaneBEaKsklpl.vbs

SHA-1: C97CDC25D1C194FF0E2D3A9E19247E091C9B677F

C:\Users\user\AppData\Local\Temp\7ZSfx000.cmd

SHA-1: BF871005126BD2FE61152408857781A2E5012A1D

C:\Users\user\AppData\Roaming\Microsoft\satisfy\savagely.exe

C:\Users\user\AppData\Local\Temp\24197-HeDSIhKlNiKRBpV.txt

SHA-1: 1C2E1B07EBDF940D0C67713D99369CF2026F8F7E

C:\Users\user\AppData\Local\Temp\24180-9520.vbs

SHA-1: DAAC7C18C74326AA4A82EA490295993E471C1C15

C:\Users\user\AppData\Local\Temp\24214-30768.vbs

SHA-1: ECBC76737EA44A05F2D042644ACA7098ACE9C57A

C:\Users\user\AppData\Roaming\Microsoft\casks.exe

SHA-1: A057D27FC8F3E3B7CF9061AEDED0601C56D746E1

C:\Users\user\AppData\Roaming\Microsoft\casks.vbs

SHA-1: 52C30594D8FCD238C889B537C93AE55EBA96431E

C:\Users\user\AppData\Roaming\Microsoft\casks\hasten.exe

Планувальник завдань

@schtasks /Create /SC MINUTE /MO 13 /F /tn HelpOffice /tr satisfy.exe //b satisfy.vbs

@schtasks /Create /SC MINUTE /MO 5 /F /tn ScheduledDefrag /tr wscript.exe //b sorting.vbs

@schtasks /Create /SC MINUTE /MO 5 /F /tn ScheduledDefrag /tr wscript.exe //b souvenir.vbs

Посилання, домени та IP адреси

hxxp://scorpiones.online/12639B73/IdmPyYVUudYaVF.dot

hxxp://graphiuma.online/hat.php

hxxp://optica-rd.myftp.biz/satisfy.php

hxxp://188.225.58.175/savagely.php

hxxp://194.58.112.174/phone.php

hxxp://apoxipodes.ru/straightforward.php

hxxp://dipteran.online/napoleon.php

hxxp://dipteran.online/saucer.php

185.119.59.227

188.225.58.175

194.58.112.174

188.225.24.78

109.68.212.97
