# APT Cobalt Strike Campaign targeting Slovakia (DEF CON talk)

istrosec.com/blog/apt-sk-cobalt/

Ladislav Baco  Monday, Aug 9, 2021

DEF CON 29

HOW VIGILANT RESEARCHERS CAN UNCOVER APT ATTACKS FOR FUN AND NON PROFIT

IstroSec

Ladislav Baco
@ladislav_b

In March 2021 our researchers discovered APT campaign targeting Slovakia. We found that this campaign has been active at least since February 2021 and some C&C servers were still active in June 2021. Threat actor used mostly Cobalt Strike and phishing emails and documents on behalf of Slovak National Security Authority. Our threat intelligence and malware research revealed several command and controls servers around the globe. Some of them had direct relations to targets in Slovak republic.

## Cobalt Strike

As described on the Cobalt Strike's website, Cobalt Strike is "software for Adversary Simulations and Red Team Operations". It is a commercial tool with price $3,500 per user for one year and it is used by many pentesters and red teamers as well as by some of the advanced threat actors such as APT19, APT29, APT32, Leviathan, Cobalt Group and FIN6. Again, official website says:

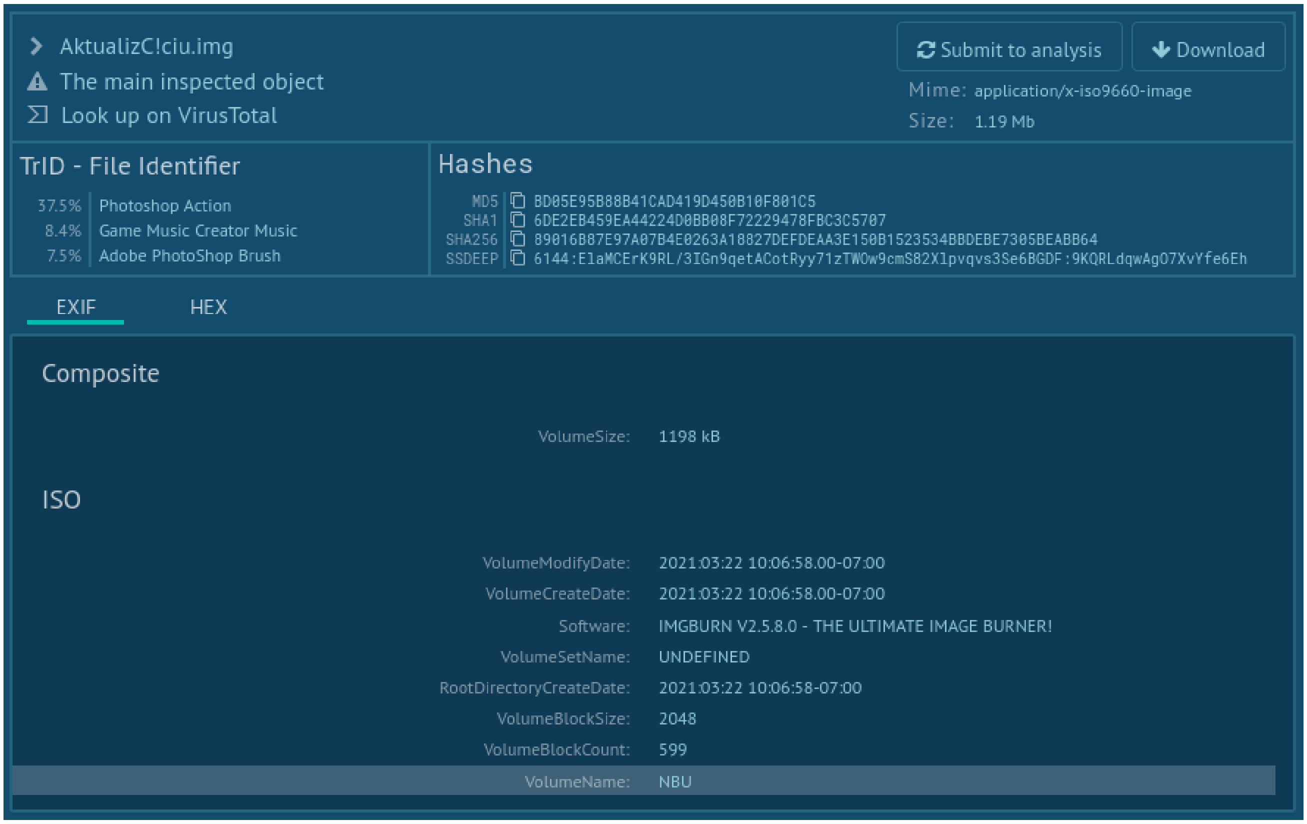
> "Cobalt Strike gives you a post-exploitation agent and covert channels to emulate a quiet long-term embedded actor in your customer's network".

Therefore it is kind of more interesting malware than relatively common backdoors, rats and Metasploit and other publicly accessible free samples.

## "NSA" ISO Sample

Somebody submitted the sample called AktualizC!ciu.img to the sandbox Any.Run on 23rd March 2021. This sample was been submitted for analysis from Slovakia. And then, it has been submitted again on 9th April. Probabably someone was already/again investigating the attack. The original ISO filesystem contains timestamps with information about the timezone: UTC-07:00 (Pacific Daylight Time). Also, this sample has been submitted to VirusTotal shortly after the reported timestamps of creation the ISO filesystems. This indicates that no tampering of creation timestamps of ISO filesystem has been applied.

The Volume name of the ISO filesystem is interesting - it contains "NBU", which is abbreviation of the National Security Authority in Slovakia.



Mime: application/x-iso9660-image
Size: 1.19 Mb

TrID - File Identifier

| | |
|---|---|
| 37.5% | Photoshop Action |
| 8.4% | Game Music Creator Music |
| 7.5% | Adobe PhotoShop Brush |

Hashes

```
   MD5  BD05E95B88B41CAD419D450B10F801C5
  SHA1  6DE2EB459EA44224D0BB08F72229478FBC3C5707
SHA256  89016B87E97A07B4E0263A18827DEFDEAA3E150B1523534BBDEBE7305BEABB64
SSDEEP  6144:ElaMCErK9RL/3IGn9qetACotRyy71zTWOw9cmS82Xlpvqvs3Se6BGDF:9KQRLdqwAgO7XvYfe6Eh
```

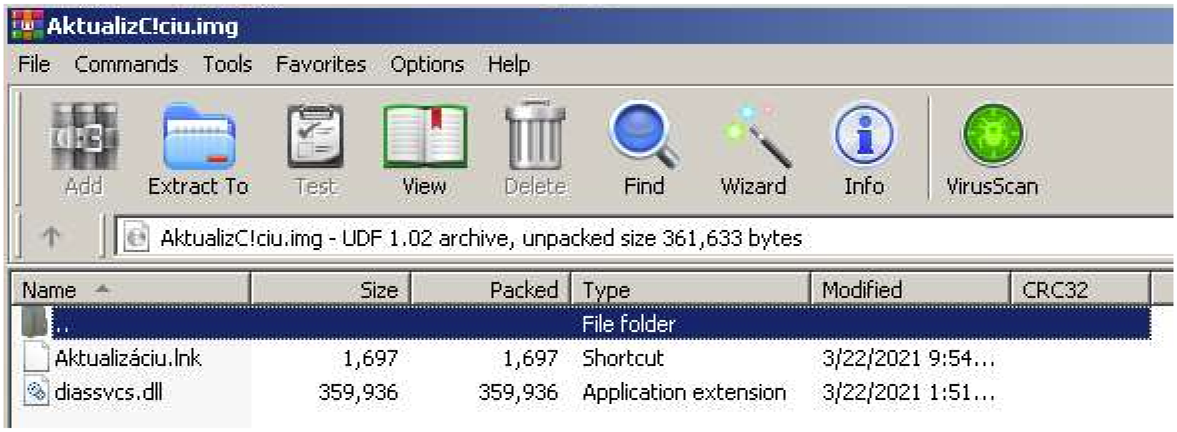
Composite

| | |
|---|---|
| VolumeSize: | 1198 kB |

ISO

| | |
|---|---|
| VolumeModifyDate: | 2021:03:22 10:06:58.00-07:00 |
| VolumeCreateDate: | 2021:03:22 10:06:58.00-07:00 |
| Software: | IMGBURN V2.5.8.0 - THE ULTIMATE IMAGE BURNER! |
| VolumeSetName: | UNDEFINED |
| RootDirectoryCreateDate: | 2021:03:22 10:06:58-07:00 |
| VolumeBlockSize: | 2048 |
| VolumeBlockCount: | 599 |
| VolumeName: | NBU |

Fig. 1: NSA ISO Sample



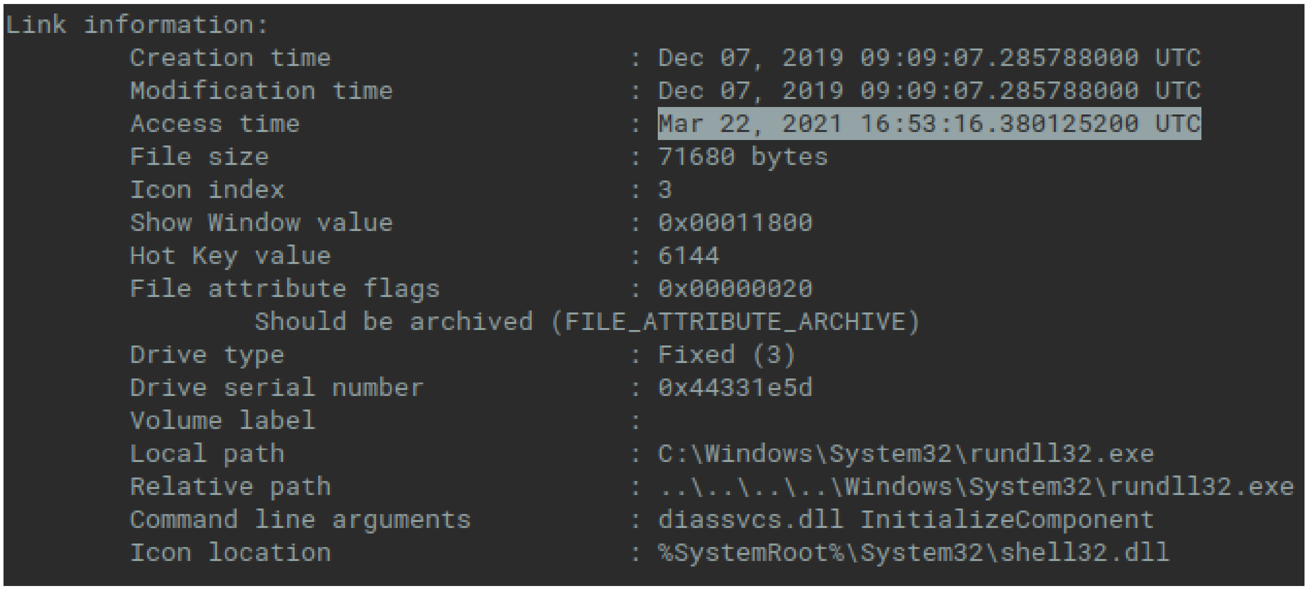
AktualizC!ciu.img - UDF 1.02 archive, unpacked size 361,633 bytes

| Name | Size | Packed | Type | Modified | CRC32 |
|---|---|---|---|---|---|
| .. | | | File folder | | |
| Aktualizáciu.lnk | 1,697 | 1,697 | Shortcut | 3/22/2021 9:54... | |
| diassvcs.dll | 359,936 | 359,936 | Application extension | 3/22/2021 1:51... | |

Fig. 2: Content of NSA ISO Sample

The “NSA” ISO Sample contains two files: one LNK file and one DLL file. The LNK file actually executes the following command: `C:\Windows\System32\rundll32.exe diassvcs.dll InitializeComponent`

Refering the access time of LNK file, this file has been accessed 13 minutes before the ISO filesystem has been created. Thus there is probably no automation in the packaging process of the malware sample and the payload for delivery (see below) has been created manually by human.

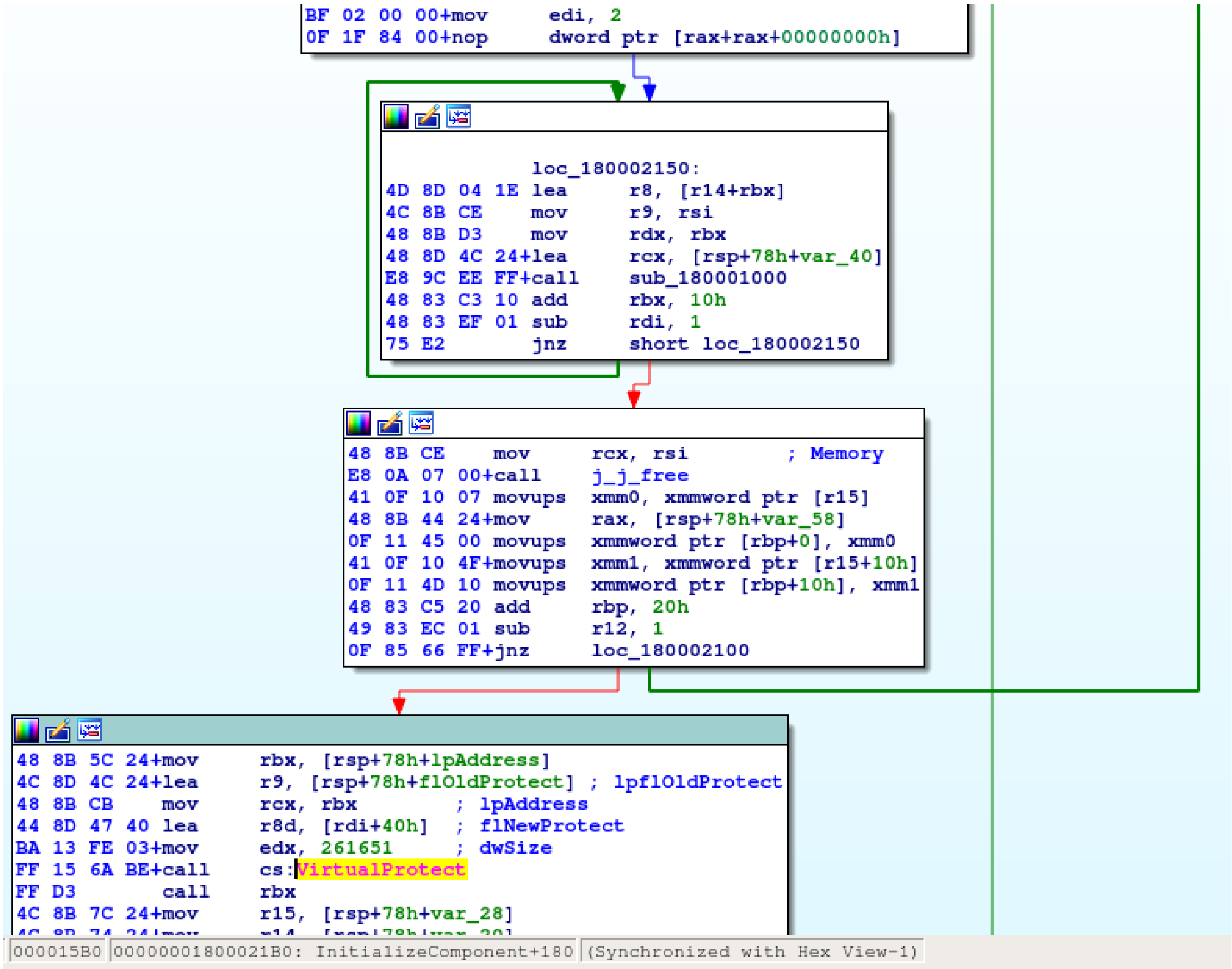


```
Link information:
        Creation time                       : Dec 07, 2019 09:09:07.285788000 UTC
        Modification time                   : Dec 07, 2019 09:09:07.285788000 UTC
        Access time                         : Mar 22, 2021 16:53:16.380125200 UTC
        File size                           : 71680 bytes
        Icon index                          : 3
        Show Window value                   : 0x00011800
        Hot Key value                       : 6144
        File attribute flags                : 0x00000020
                Should be archived (FILE_ATTRIBUTE_ARCHIVE)
        Drive type                          : Fixed (3)
        Drive serial number                 : 0x44331e5d
        Volume label                        :
        Local path                          : C:\Windows\System32\rundll32.exe
        Relative path                       : ..\..\..\..\Windows\System32\rundll32.exe
        Command line arguments              : diassvcs.dll InitializeComponent
        Icon location                       : %SystemRoot%\System32\shell32.dll
```

Fig. 3: Details of LNK file from NSA ISO Sample

## Cobalt Strike Beacon

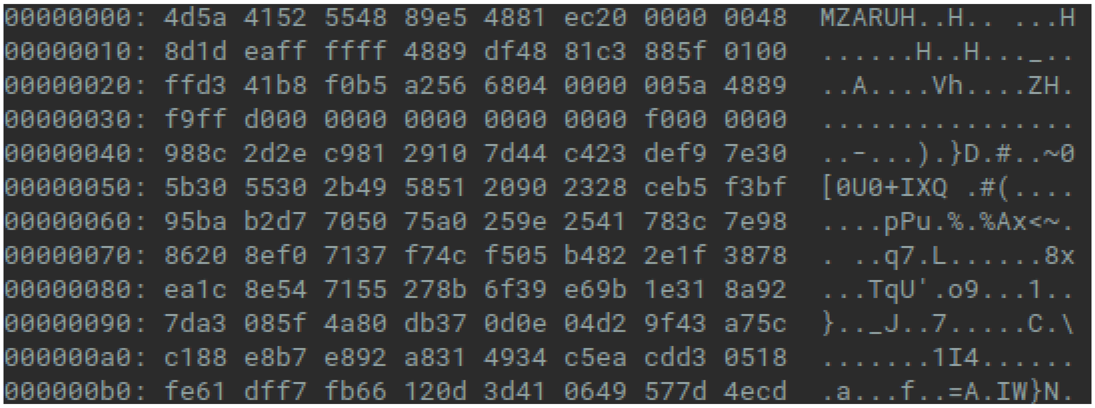
DLL file `diassvcs.dll` is a loader/packer with some anti-analysis protections enabled. In the picture below there is the unpacking routine consisting of decryption loops followed by the calls to `VirtualProtect` Windows API and to the unpacked payload itself.



```
BF 02 00 00+mov     edi, 2
0F 1F 84 00+nop     dword ptr [rax+rax+00000000h]

                loc_180002150:
4D 8D 04 1E lea     r8, [r14+rbx]
4C 8B CE    mov     r9, rsi
48 8B D3    mov     rdx, rbx
48 8D 4C 24+lea     rcx, [rsp+78h+var_40]
E8 9C EE FF+call    sub_180001000
48 83 C3 10 add     rbx, 10h
48 83 EF 01 sub     rdi, 1
75 E2       jnz     short loc_180002150

48 8B CE    mov     rcx, rsi         ; Memory
E8 0A 07 00+call    j_j_free
41 0F 10 07 movups  xmm0, xmmword ptr [r15]
48 8B 44 24+mov     rax, [rsp+78h+var_58]
0F 11 45 00 movups  xmmword ptr [rbp+0], xmm0
41 0F 10 4F+movups  xmm1, xmmword ptr [r15+10h]
0F 11 4D 10 movups  xmmword ptr [rbp+10h], xmm1
48 83 C5 20 add     rbp, 20h
49 83 EC 01 sub     r12, 1
0F 85 66 FF+jnz     loc_180002100

48 8B 5C 24+mov     rbx, [rsp+78h+lpAddress]
4C 8D 4C 24+lea     r9, [rsp+78h+flOldProtect] ; lpflOldProtect
48 8B CB    mov     rcx, rbx         ; lpAddress
44 8D 47 40 lea     r8d, [rdi+40h]   ; flNewProtect
BA 13 FE 03+mov     edx, 261651      ; dwSize
FF 15 6A BE+call    cs:VirtualProtect
FF D3       call    rbx
4C 8B 7C 24+mov     r15, [rsp+78h+var_28]

000015B0 00000001800021B0: InitializeComponent+180 (Synchronized with Hex View-1)
```

Fig. 4: Unpacking routine of DLL Loader from NSA ISO Sample

The unpacked payload is DLL file, but without standard MS-DOS header. This malformed header can be often seen for example in Metasploit’s Meterpreter payloads and it is used as a part of shellcode.



```
00000000: 4d5a 4152 5548 89e5 4881 ec20 0000 0048  MZARUH..H.. ...H
00000010: 8d1d eaff ffff 4889 df48 81c3 885f 0100  ......H..H..._..
00000020: ffd3 41b8 f0b5 a256 6804 0000 005a 4889  ..A....Vh....ZH.
00000030: f9ff d000 0000 0000 0000 0000 f000 0000  ................
00000040: 988c 2d2e c981 2910 7d44 c423 def9 7e30  ..-...).}D.#..~0
00000050: 5b30 5530 2b49 5851 2090 2328 ceb5 f3bf  [0U0+IXQ .#(....
00000060: 95ba b2d7 7050 75a0 259e 2541 783c 7e98  ....pPu.%.%Ax<~.
00000070: 8620 8ef0 7137 f74c f505 b482 2e1f 3878  . ..q7.L......8x
00000080: ea1c 8e54 7155 278b 6f39 e69b 1e31 8a92  ...TqU'.o9...1..
00000090: 7da3 085f 4a80 db37 0d0e 04d2 9f43 a75c  }.._J..7.....C.\
000000a0: c188 e8b7 e892 a831 4934 c5ea cdd3 0518  .......1I4......
000000b0: fe61 dff7 fb66 120d 3d41 0649 577d 4ecd  .a...f..=A.IW}N.
```

Fig. 5: Malformed MZ header of unpacked Cobalt Strike Beacon

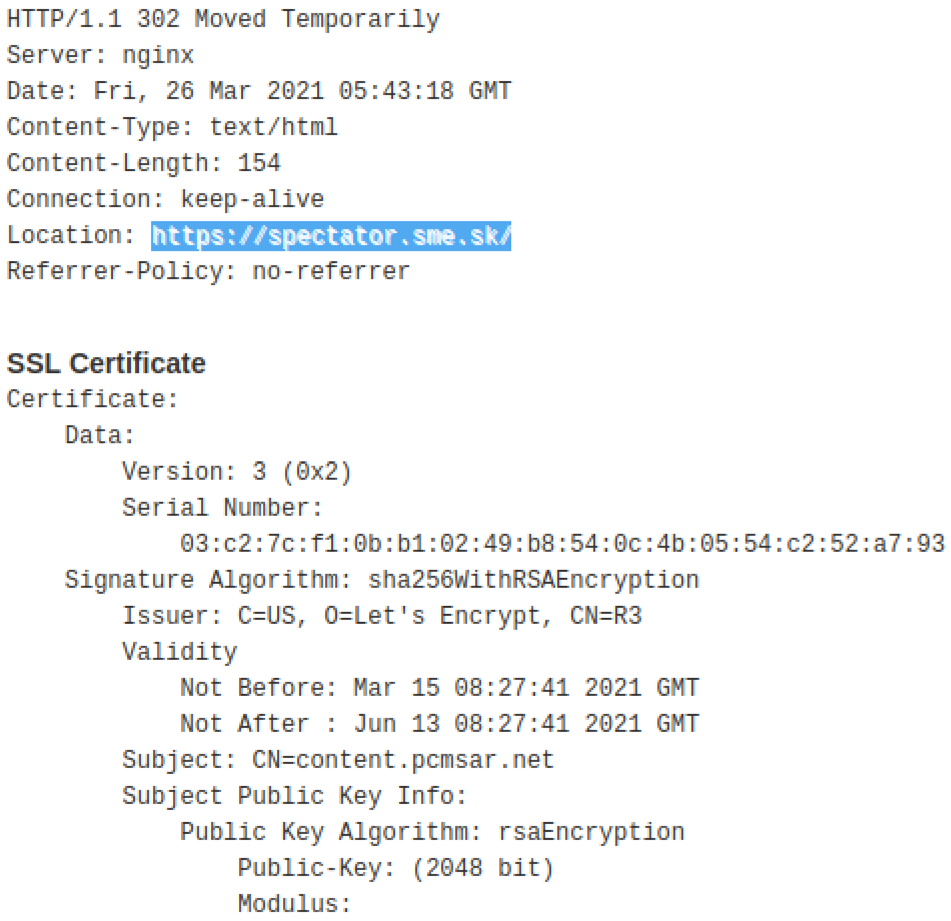
This DLL file is actually a Cobalt Strike Beacon. The extracted configuration is attached below.

```
BeaconType                       - HTTPS
Port                             - 443
SleepTime                        - 45000
MaxGetSize                       - 1403644
Jitter                           - 37
MaxDNS                           - Not Found
PublicKey                        -
b'0\x81\x9f0\r\x06\t*\x86H\x86\xf7\r\x01\x01\x01\x05\x00\x03\x81\x8d\x000\x81\x89\x02
\xa0\x13/.@\xda\xf4\xf7q\xf3y\x84\xf3b!\x9fw\xf4\xf6D\xb5\xe7w\x19\x17\xe60&\x10\xb4]

C2Server                         - content.pcmsar.net,/jquery-3.3.1.min.js
UserAgent                        - Not Found
HttpPostUri                      - /jquery-3.3.2.min.js
HttpGet_Metadata                 - Not Found
HttpPost_Metadata                - Not Found
SpawnTo                          -
b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
PipeName                         - Not Found
DNS_Idle                         - Not Found
DNS_Sleep                        - Not Found
SSH_Host                         - Not Found
SSH_Port                         - Not Found
SSH_Username                     - Not Found
SSH_Password_Plaintext           - Not Found
SSH_Password_Pubkey              - Not Found
HttpGet_Verb                     - GET
HttpPost_Verb                    - POST
HttpPostChunk                    - 0
Spawnto_x86                      - %windir%\syswow64\dllhost.exe
Spawnto_x64                      - %windir%\sysnative\dllhost.exe
CryptoScheme                     - 0
Proxy_Config                     - Not Found
Proxy_User                       - Not Found
Proxy_Password                   - Not Found
Proxy_Behavior                   - Use IE settings
Watermark                        - 1359593325
bStageCleanup                    - True
bCFGCaution                      - False
KillDate                         - 0
bProcInject_StartRWX             - False
bProcInject_UseRWX               - False
bProcInject_MinAllocSize         - 17500
ProcInject_PrependAppend_x86     - b'\x90\x90'
                                   Empty
ProcInject_PrependAppend_x64     - b'\x90\x90'
                                   Empty
ProcInject_Execute               - ntdll:RtlUserThreadStart
                                   CreateThread
                                   NtQueueApcThread-s
                                   CreateRemoteThread
                                   RtlCreateUserThread
ProcInject_AllocationMethod      - NtMapViewOfSection
bUsesCookies                     - True
HostHeader                       -
```

From this config we can see that this is a HTTP Beacon based on jQuery Malleable-C2 profile

## Cobalt Strike C2 Server

Analysis of Cobalt Strike C2 Server at content.pcmsar[.]net revealed couple of interesting things. The server is hosted at Canadian OVH SAS hosting. It is powered by nginx webserver, with Let's Encrypt certificate issued on Mar 15 08:27:41 2021 GMT (approximately one week before the Cobalt Strike Payload packed into ISO). Without any parameters, the HTTP requests are redirected to https://spectator.sme.sk/, a popular Slovakia's English-language online newspaper.



```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Fri, 26 Mar 2021 05:43:18 GMT
Content-Type: text/html
Content-Length: 154
Connection: keep-alive
Location: https://spectator.sme.sk/
Referrer-Policy: no-referrer
```

**SSL Certificate**

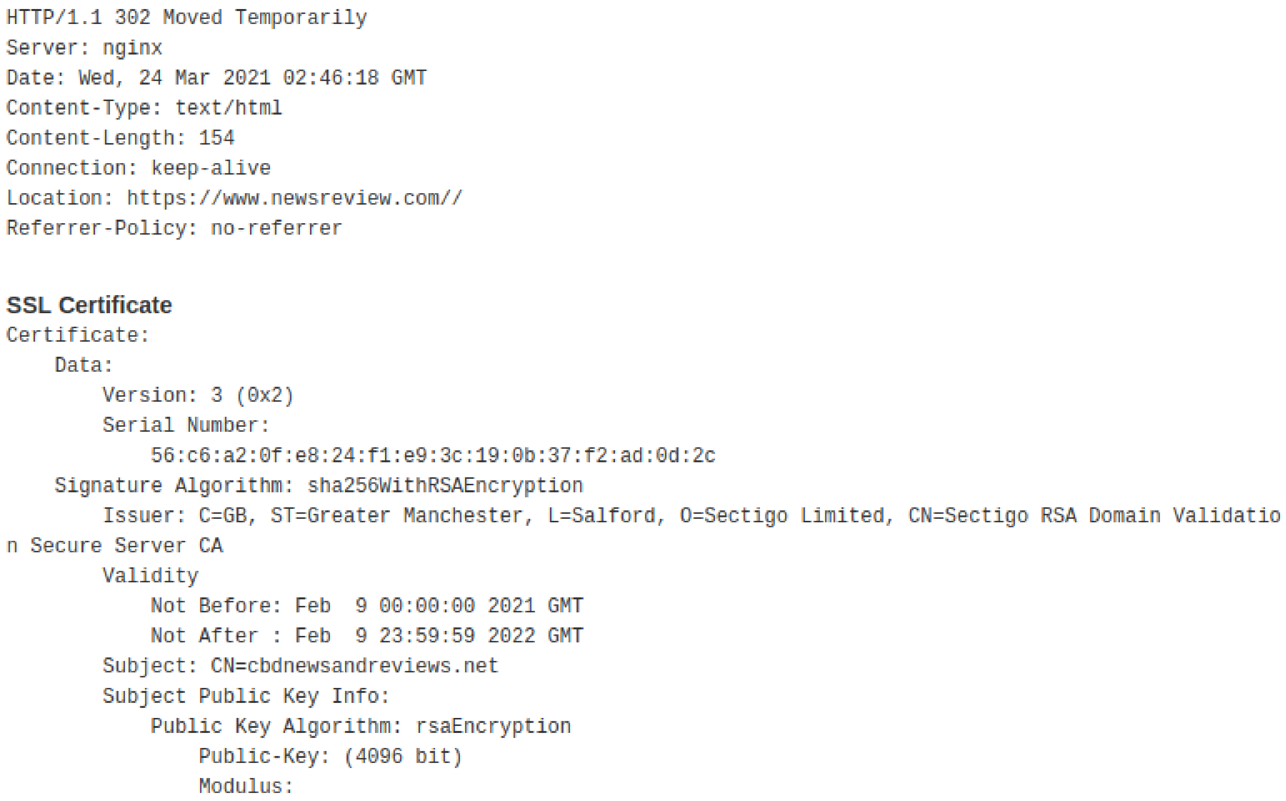
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:c2:7c:f1:0b:b1:02:49:b8:54:0c:4b:05:54:c2:52:a7:93
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=R3
        Validity
            Not Before: Mar 15 08:27:41 2021 GMT
            Not After : Jun 13 08:27:41 2021 GMT
        Subject: CN=content.pcmsar.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
```

Fig. 6: HTTPS details of Cobalt Strike C&C server

## Threat Actor C2 Infrastructure

Based on observations above (and couple of others) there is possible to discover more C2 servers. Some of them are hosted in OVH, and many of them have SSL/TLS certificates issued by Sectigo instead of Let's Encrypt. They are active since February 2021 (confirmed), but probably some of them was used also back in 2020. These C2 servers also incorporated the redirection to innocent websites and they uses similar domains by themselves. For example, C2 server hosted at cbdnewsandreviews[.]net redirects visitors to https://www.newsreview.com//.

The discovered C2 servers are located around the globe, for example, in Canada, France and Australia.



```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Wed, 24 Mar 2021 02:46:18 GMT
Content-Type: text/html
Content-Length: 154
Connection: keep-alive
Location: https://www.newsreview.com//
Referrer-Policy: no-referrer
```

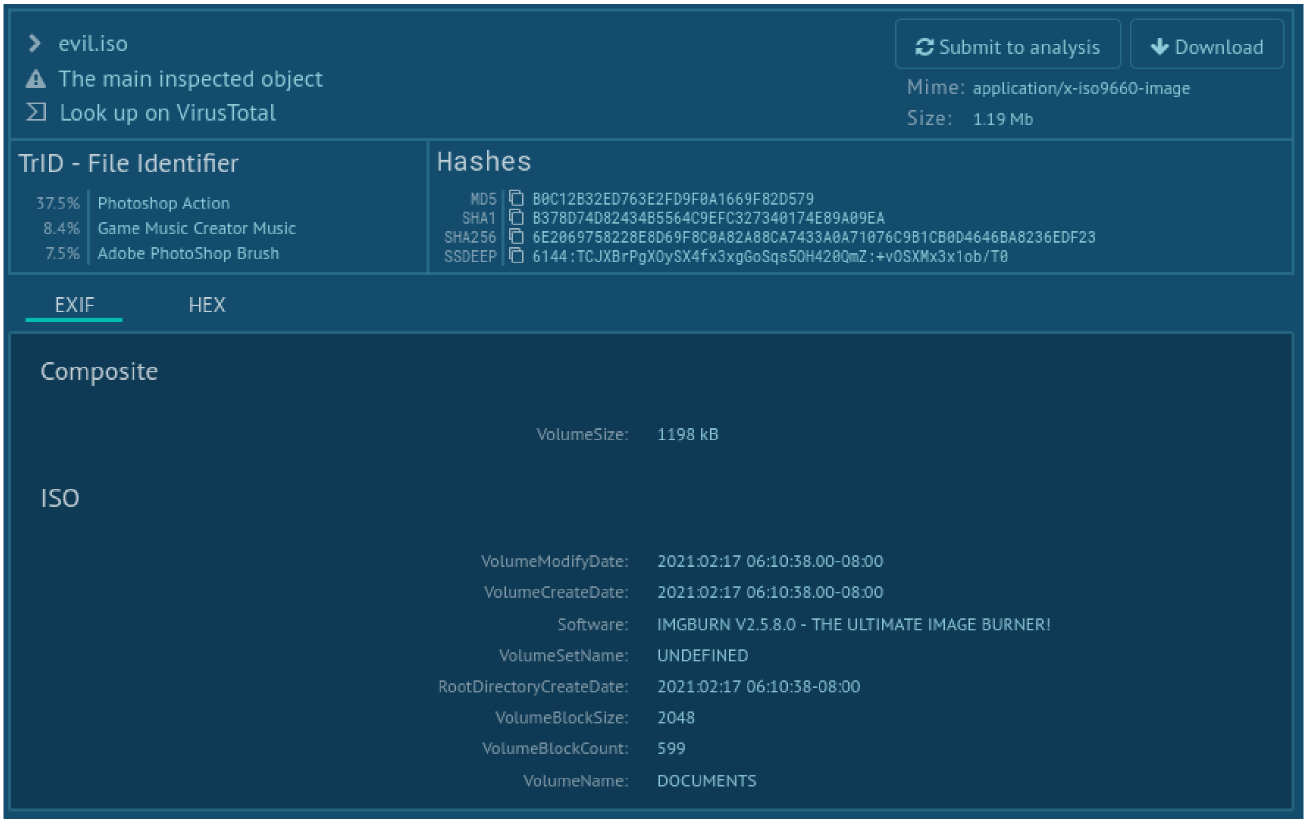
**SSL Certificate**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:c6:a2:0f:e8:24:f1:e9:3c:19:0b:37:f2:ad:0d:2c
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validatio
n Secure Server CA
        Validity
            Not Before: Feb  9 00:00:00 2021 GMT
            Not After : Feb  9 23:59:59 2022 GMT
        Subject: CN=cbdnewsandreviews.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
```

Fig. 7: HTTPS details of another Cobalt Strike C&C server

## More Malware Samples

With information about C2 infrastructure, our researchers have found another malware samples linked to the same threat actor. For example, another ISO called evil.iso. This file is very similar to the analyzed “NSA” ISO, it contains LNK and DLL file with Cobalt Strike Beacon payload. It was submitted to Any.Run on 26th February 2021 from Netherlands (hypothesis is that the malware analyst used the ProtonVPN which is often used by them for protecting their privacy). First submittion on VirusTotal is from 25th February, however, the ISO file (with original name invitation.iso) was created most likely on 17th February in Pacific Standard Timezone (UTC-08:00).



Mime: application/x-iso9660-image
Size: 1.19 Mb

TrID - File Identifier

| | |
|---|---|
| 37.5% | Photoshop Action |
| 8.4% | Game Music Creator Music |
| 7.5% | Adobe PhotoShop Brush |

Hashes

```
   MD5  B0C12B32ED763E2FD9F0A1669F82D579
  SHA1  B378D74D82434B5564C9EFC327340174E89A09EA
SHA256  6E2069758228E8D69F8C0A82A88CA7433A0A71076C9B1CB0D4646BA8236EDF23
SSDEEP  6144:TCJXBrPgXOySX4fx3xgGoSqs5OH420QmZ:+vOSXMx3x1ob/T0
```

Composite

| | |
|---|---|
| VolumeSize: | 1198 kB |

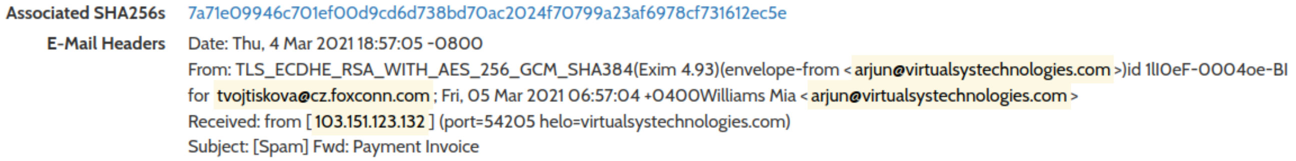
ISO

| | |
|---|---|
| VolumeModifyDate: | 2021:02:17 06:10:38.00-08:00 |
| VolumeCreateDate: | 2021:02:17 06:10:38.00-08:00 |
| Software: | IMGBURN V2.5.8.0 - THE ULTIMATE IMAGE BURNER! |
| VolumeSetName: | UNDEFINED |
| RootDirectoryCreateDate: | 2021:02:17 06:10:38-08:00 |
| VolumeBlockSize: | 2048 |
| VolumeBlockCount: | 599 |
| VolumeName: | DOCUMENTS |

Fig. 8: Evil ISO Sample

## Delivery Method

Based on similarities of analyzed ISO files we were able to find another similar files. It seems that at least some of them have been delivered via phishing emails with ISO/IMG attachments looking like Word documents. Moreover, it seems that the same threat actor delivers at least one phishing email to the targets in Czech republic in March 2021.



| | |
|---|---|
| Associated SHA256s | 7a71e09946c701ef00d9cd6d738bd70ac2024f70799a23af6978cf731612ec5e |
| E-Mail Headers | Date: Thu, 4 Mar 2021 18:57:05 -0800<br>From: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(Exim 4.93)(envelope-from < arjun@virtualsystechnologies.com >)id 1lI0eF-0004oe-BI for tvojtiskova@cz.foxconn.com ; Fri, 05 Mar 2021 06:57:04 +0400Williams Mia < arjun@virtualsystechnologies.com ><br>Received: from [ 103.151.123.132 ] (port=54205 helo=virtualsystechnologies.com)<br>Subject: [Spam] Fwd: Payment Invoice |

Fig. 9: Example of email with similar attachement delivered to the private company

## Findings and Summary

We were able to discover and track the campaign targeting Slovakia Government and Cobalt Strike infrastructure used by the threat actor. This analysis was based solely on publicly available information, community threat intelligence sources and our own malware research. The incident and results have been reported to the local authorities such as computer security incident response team. The report included the collected indicators of compromise such as hashes and IP addresses. These IOCs have been used during the investigation. Imagine, it is like the oraculum - you can predict which IP addresses will the attacker use in the next steps, or, you can use the reported IOCs as a pivots during the forensic analysis. All the results are only from the hunting in public sources.

## DEF CON Talk

RECON VILLAGE
(VIRTUAL )

DEF CON 29

www.reconvillage.org
@reconvillage

LADISLAV BACO

@ladislav_b

How vigilant researchers can uncover APT attacks for fun and non profit

Live Q&A on Discord

https://discord.gg/defcon
#rv-talks-voice

Fig. 10: Our talk at DEFCON 29 Recon Village

We presented this case at Recon Village at DEF CON 29 conference in August 2021 (Las Vegas & Virtual). We also introduced and explained couple of concepts, tips and tricks for malware hunting and advanced search. Presentation slides and video from our talk are available below.

DEF CON 29 Recon Village Presentation Slides [PDF]

How vigilant researchers can uncover APT attacks for fun and non-profit

A POOR MAN'S TOOLKIT
RESOURCES

- Malware Samples
  - Online repositories, e.g. Malware Bazaar and vx-underground
- Malware Feeds + Advanced search capabilities
  - Hybrid-Analysis, Any.Run, Tria.ge
  - VirusTotal relations and graphs

Watch Video At:

https://youtu.be/HMpePkNivjo

## Afterword

*(updated on Sep 13, 2021)*

This blog post was originally based on research and analysis during March and April 2021. Therefore, we published our results based only on data available at that time, without referring to the results and articles published a few weeks and months later.

Few days after DEF CON talk and after publishing this blog post, Slovak technology portal Zive.sk wrote an article about this incident based on our research. Then, ESET Research found that this attack targeted diplomats from more than 13 European countries and think-tanks and this attack was linked to **APT29/Dukes/Nobelium** also by Microsoft Threat Intelligence Center. In their article from the end of May they published IOCs which contain also some of the IOCs mentioned here, including “NSA” ISO Sample.

And finally, Catalin Cimpanu from The Record published post “Russian cyberspies targeted the Slovak government for months” based on above work.

## Sample IOCs

### Hashes

- bd05e95b88b41cad419d450b10f801c5: AktualizC!ciu.img

- ed24b708a0abb91d2d984c646527823f: Aktualizáciu.lnk
- e55d9f6300fa32458b909fded48ec2c9: diassvcs.dll
- 1adfe420043628286d0f3ff007113bfa: Cobalt Strike Beacon
- b0c12b32ed763e2fd9f0a1669f82d579: evil.iso
- 038579bdb1de9e0ab541df532afeb50d: Programme outline.lnk
- 72b494d0921296cdd5e4a07a0869b244: Plending forms.lnk
- 600aceaddb22b9a1d6ae374ba7fc28c5: GraphicalComponent.dll

### Domains

- content.pcmsar[.]net
- cbdnewsandreviews[.]net

### IP Addresses

- 51.79.69[.]211
- 139.99.167[.]177

## References