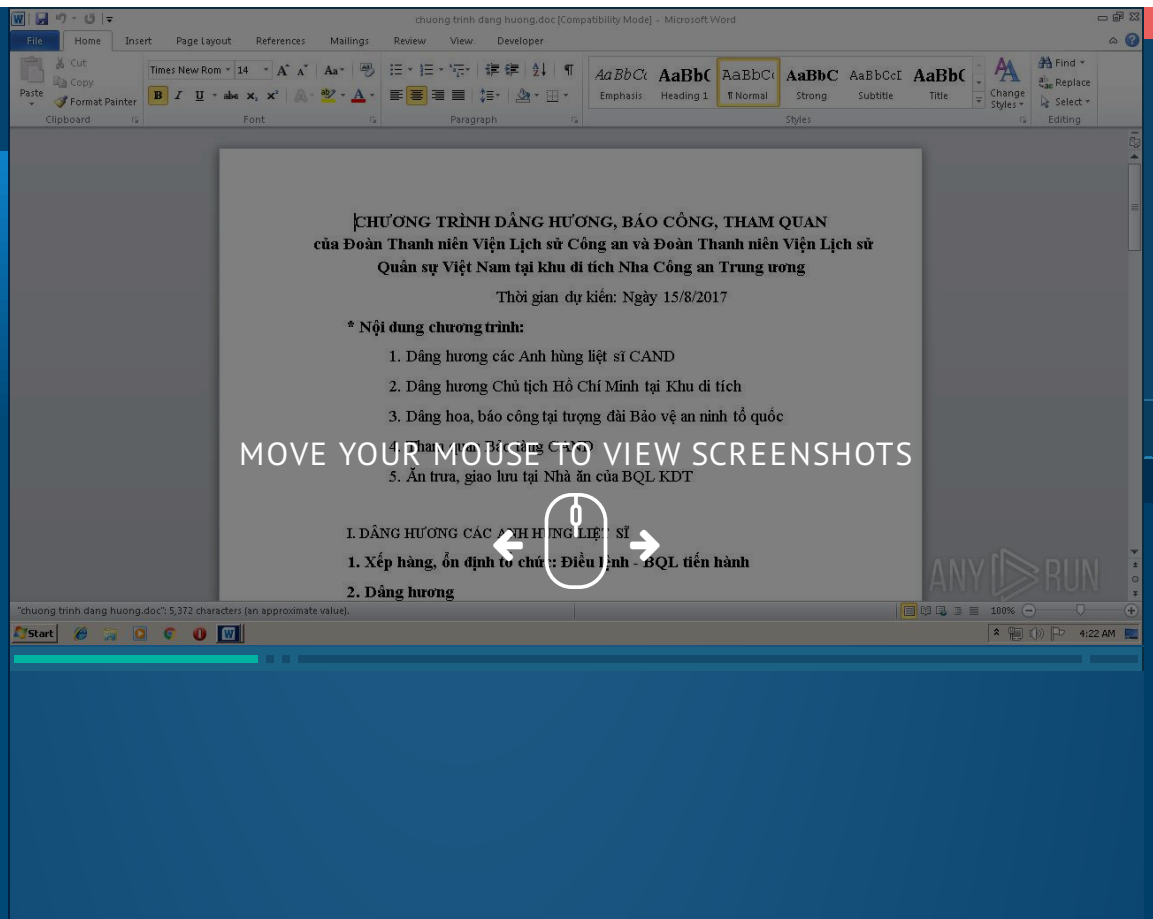

Malicious activity

chuong trinh dang huong.doc.lnk

MD5: 165F8683681A4B136BE1F9D6EA7F00CE

Start: 13.06.2019, 05:21 Total time: 60 s

Win7 32 bit
Complete

Indicators:

Get sample | IOC | MalConf | Restart

Text report | Graph | ATT&CK | AI Summary beta | Export

CPU RAM

Processes Filter by PID or name Only important

3572 cmd.exe /c for %x in (C:\Users\admin\AppData\Local\Temp=%cd... 233 6 32

3176 cmd.exe /c dir "C:\Users\admin\AppData\Local\Temp\chuo... 83 6 24

1364 mshta.exe "C:\Users\admin\AppData\Local\Temp\chuong tr... 608 54 122

2036 cmd.exe /c dir "C:\Users\admin\AppData\Local\Temp\chuo... 83 6 24

2104 mshta.exe "C:\Users\admin\AppData\Local\Temp\chuong tr... 582 55 118

3256 WMI cmd.exe /c powershell.exe -exec bypass -file C:\Users\adm... 125 6 26

3504 powershell.exe -exec bypass -file C:\Users\admin\AppData\L... 2k 478 210

1584 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Tem... 2k 1k 90

2864 cmd.exe /c copy /y C:\Windows\Microsoft.NET\Framew... 76 6 24

3960 cmd.exe /c copy /y C:\Windows\system32\wscript.exe ... 78 6 24

124 cmd.exe /c copy /y C:\Windows\system32\schtasks.exe ... 77 6 24

2452 cmd.exe /c C:\Users\admin\AppData\Local\Temp\wtas... 126 6 28

1464 wtask.exe PE /create /sc minute /mo 3 /tn "Se... 154 0 48

1332 cmd.exe /c C:\Users\admin\AppData\Local\Temp\wtas... 98 6 28

2696 wtask.exe PE /run /tn "Security Script kb005990... 106 0 46

3212 WMI cmd.exe /c powershell.exe -exec bypass -file C:\Users\adm... 125 6 26

2796 powershell.exe -exec bypass -file C:\Users\admin\AppData\L... 2k 482 210

2100 WINWORD.EXE /n "C:\Users\admin\AppData\Local\Tem... 808 251 76

2872 cmd.exe /c copy /y C:\Windows\Microsoft.NET\Framew... 79 6 24

\Windows\system32\wscript.exe ... 83 6 24

\Windows\system32\schtasks.exe... 81 6 24

admin\AppData\Local\Temp\wtas... 97 6 28

/create /sc minute /mo 3 /tn "Se... 153 0 48

HTTP Requests 1 | Connections 4 | DNS Requests 2 | Threats 6 | Filter by PID, name or url | PCAP

NETWORK FILES DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
8497 ms	GET | 200: OK	?	2236	InstallUtil.exe		http://www.download.windowsupdate.c...	56

Danger [2236] InstallUtil.exe Loads dropped or rewritten executable

Try community version for free! Register now