Troj/Cryakl-B

sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Cryakl-B/detailed-analysis.aspx

Troj/Cryakl-B exhibits the following characteristics:

File Information

Size
453K

SHA-1
dd4dec6887ffdf95128332ce85124cf45c63f08a

MD5
755410ad3c026a673153c382d5d0651a

CRC-32
5bee71a8

File type
Windows executable

First seen
2015-11-02

Runtime Analysis

Copies Itself To

- C:\Program Files\test_item.exe
- C:\test_item.exe
- c:\Documents and Settings\test user\Local Settings\Temp\test_item.exe

Dropped Files

- c:\Documents and Settings\test user\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-LUZFLQWCINTZEJPVAFLQWBGMSXDIOT.ZFK.cbf
- C:\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-VDJPVBHMSXDIOUZEKPVBFLRXBHNTXD.KPU.cbf
- C:\INSTALLERS\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-XFLRXEJOUAFLRXBHNTYDJOUZFLQWBI.NTZ.cbf

- C:\gnu\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-IRXCJPVAGMRXDIOTZEKQWAHMSXDJOU.AGL.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-ZGMSZEKQWBHMSXDJOUZFKQWBGMRXDI.PUZ.cbf
- c:\Documents and Settings\test user\Cookies\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-SBHNUAFKQWBHNTYDKPUAGLRWCHNTZE.KQV.cbf
- C:\bin\misc\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-BKQWDIOUZFLRWBHMSXDJOUZFKQWBGM.SYD.cbf
- c:\Documents and Settings\test user\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-CKQWCIOTZFLQWCHMSYEJPVAGLRWCHN.TYE.cbf
- C:\bin\OLD\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-VEKQXDJOUAFLRXCIOTZFLPVBHMSYDJ.PVZ.cbf
- c:\Documents and Settings\test user\Cookies\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-XEKQWCINTZFKQWBGMSXCIOTYEKQUAG.MRW.cbf
- c:\Documents and Settings\test user\Cookies\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-VDJOVBFMSXCIOTYEKPVAGLRXCHNTZE.KQV.cbf
- c:\Documents and Settings\test user\Application Data\Microsoft\Internet Explorer\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-HQWCIOUAFLRWCINSYEKPUAGLRWCHNT.YEK.cbf
- c:\Documents and Settings\test user\Cookies\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-CKQVDIOTAFLRWBHNSYEKPUAGLRWCHN.UYE.cbf

- C:\bin\OLD\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-MUAHNTZEKQWBHMSXDJOUZFKQWCHNTY.FLQ.cbf
- C:\bin\OLD\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-LVBGNTYEKPUAGLQWCHMSYDIOUZEKPV.BGN.cbf
- C:\bin\misc\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-DNTYGLRWCINTZEKQVBHMRXDJOUAFLQ.XCI.cbf
- C:\bin\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-TCINUAGLRWCHNTYDJPVAFLRWCHNSYE.JPU.cbf
- C:\bin\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-QYEKRWCINTZFJPVBGMSXCIOTZEKPVB.HMS.cbf
- C:\bin\loggers1.vbs
- C:\bin\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-XGMSYDJPUAGMRWCINSYEJPVAFLRWBH.OSY.cbf
- C:\bin\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-WFLRXDJOUAFLRXCHNTYEKQVBHMRXDI.PVA.cbf
- C:\bin\tile.vbs
- C:\bin\vireng.log
- C:\bin\loggers2.vbs
- C:\Documents and Settings\Default User\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-HRXDJPUAGMRWCINSYEJPUAFLQWBGMS.YEJ.cbf
- C:\Documents and Settings\Default User\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-HRXDKQWBHNSXDJPUAGLRWCINTYEJPU.AFM.cbf

- C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-TBHNTZEJPVBGMSXCIOTZFKQVBGMRXC.INU.cbf
- C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-TCIOUAGMRXDIOTZEKQWAHNSXDJOUZF.LRW.cbf
- C:\Documents and Settings\Default User\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-QAFLSYEJPVAGLRXCINTYEKQUAGMRWC.IOU.cbf
- C:\Documents and Settings\Default User\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-VJPVCHNSYDJPUZFLQVBHNSXDJNTZFK.QWB.cbf
- C:\Documents and Settings\Default User\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-SCINUAFLRXCHNTYEKPVBGLRXDIOTZE.LQV.cbf
- C:\Documents and Settings\LocalService\Local Settings\Temp\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-MUBGNSYEKPVAGMRXDIOTZEJPVAGMRX.EJO.cbf
- c:\Documents and Settings\test user\Application Data\Microsoft\Address Book\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-VDKQWCINTZEJPVBFLRWCHNTYDJPUZF.LQW.cbf
- c:\Documents and Settings\test user\Application Data\Microsoft\Internet Explorer\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-GPVAHNRXDJOUAFLRWBHNTYEJPUZFLQ.WCH.cbf

- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-CKQVCHNTYEKQVBHMSYDIOUAFKQVBGM.SXC.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-AIOTAGLRXCHNTYEJPUZFLQVBHMRXDI.OTZ.cbf
- c:\Documents and Settings\test user\Cookies\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-OVBHNTYDKQUAGMRXDINTZFJPVBGMRX.DIO.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-EMTYEKQVBHMSXDJOTZFKPVAGLQWCHM.SYD.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-EMSXFKPVBGMSXDIOTZFLQWBHMSYDJP.VAG.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-FNTZFLQWBHNTYEKPUBGLRXDHOTZEKP.VAG.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-LTYEKQWCHNSYDJOUZEKQVAGMRWCINS.YEJ.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-MUAGNTYEKPVAGLRWCHNSYDIOUZFKQW.BHN.cbf

- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-KSYDKQVBHMSYEJOUAFLRWBHNTYDJPU.AGL.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-UBINTZFKQWBGMSXDIOTZFKPVBHLRXD.IOT.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-EMSYFLQVCIMSYDJOUZFKQVBGMRXBHN.TYE.cbf
- c:\Documents and Settings\test user\My Documents\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-RZFKRXCIOTZEKPVAGLQWCHNTZDJOVA.GLR.cbf
- C:\gnu\bin\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-KSYDKQVBHMRXDIOUZFKQWBGMSXCIOT.ZEK.cbf
- C:\gnu\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-DLRXEJPVSYEKPVAGLSXCIOUZFLQVBH.NTZ.cbf
- C:\mmjobid
- C:\INSTALLERS\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-KTZELRXCIOUZFLQVCHNTYEJPVAGMSX.DJO.cbf
- C:\gnu\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-UCINUZFLRWBHNSYEKOUAGLRXCHNSYD.KQV.cbf
- c:\Documents and Settings\test user\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-FNTZFLRXCIOTZFKPVBHMSXDIOUZELQ.WCI.cbf

- C:\gnu\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-FNTZGMRXDJNTZFKQVBGLRXCINTYEKP.VAG.cbf
- c:\Documents and Settings\test user\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-HSYEKQWCHNSYDJPUZFLQVBHNSYDJOT.AFL.cbf
- c:\Documents and Settings\test user\Templates\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-DLRWDJPUAGLQWCHMSYDIOUZFKQVBGL.SXC.cbf
- C:\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-SAGLTXEJPUAGLRXDHOTZEKQVAGMRWC.IOT.cbf
- C:\run.bat
- C:\screencap.png
- C:\gnu\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-YHNSZFKQWBHNSYEKPUAGLRXCIOTZEK.QVB.cbf
- C:\gnu\email-Seven_Legion2@aol.com.ver-CL 1.0.0.0.id-WFLQYDJOUAFLQWCINTZEJPVAFLRWCIOSYEJP-02@11@2015 10@47@599344641.randomname-MUBGNTYDKPVBHMRXDIOUZFLRWCINTZ.EKQ.cbf
- C:\Program Files\NPSJXGBTFY.ELK

Modified Files

- %PROFILE%\NTUSER.DAT.LOG
  Changed the file contents
- %PROFILE%\Cookies\index.dat
- %SYSTEM%\wbem\Repository\FS\MAPPING.VER
- %HISTORY%
  Set the hidden and system flags
- C:\Documents and Settings\LocalService\ntuser.dat.LOG
- %SYSTEM%\wbem\Logs\wbemess.log
  Changed the file contents
- C:\bin\usermemscan.pl
- %INTERNET_CACHE%
  Set the hidden and system flags
- %SYSTEM%\wbem\Logs\wbemcore.log
  Changed the file contents

- %SYSTEM%\wbem\Repository\FS\OBJECTS.DATA
- %SYSTEM%\wbem\Repository\FS\MAPPING2.MAP
- %SYSTEM%\wbem\Repository\FS\OBJECTS.MAP
- %SYSTEM%\wbem\Repository\FS\MAPPING1.MAP
- %SYSTEM%\wbem\Repository\$WinMgmt.CFG
- %SYSTEM%\wbem\Repository\FS\INDEX.BTR
- %SYSTEM%\wbem\Repository\FS\INDEX.MAP
- C:\KMDhips.txt
  Changed the file contents
- %SYSTEM%\config\SAM.LOG
- %SYSTEM%\config\system.LOG
  Changed the file contents
- %PROFILE%\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat.LOG
- %SYSTEM%\config\software.LOG
  Changed the file contents

Registry Keys Created

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  pr
  C:\Program Files\test_item.exe

- HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_APISPYDRV\0000\Control
  ActiveService
  ApiSpyDrv

- HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SAVSERVICE\0000\Control
  ActiveService
  SAVService

- HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
  c:\windows\system32\cmdminimentor.exe
  Windows Command Processor

- HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_APISPYDRV\0000
  DeviceDesc
  ApiSpyDrv

- HKLM\SYSTEM\CurrentControlSet\Services\ApiSpyDrv\Enum
  NextInstance
  0x00000001

Registry Keys Modified

- HKCU\SessionInformation
  ProgramCount
  0x00000009

- HKLM\SOFTWARE\Sophos\SAVService\Status\Infected
  SuspiciousBehaviorDetected
  0x00000001

- HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
  ActiveTimeBias
  0x00000000

- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
  SavedLegacySettings
  3c 00 00 00 cb 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 80 88 73 da f3 98 ca 01 01 00 00 00 ac 10 00 06 00 00 00 00 00 00 00 00

- HKCU\Software\Microsoft\Internet Explorer\Main
  Window_Placement
  2c 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 42 00 00 00 42 00 00 00 7c 03 00 00 52 02 00 00

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\5B3B929D6C65CC643B3A1A7A48BC8B4E\Usage
  SAVService
  0x476209c2

- HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E7E6F031-17CE-4C07-BC86-EABFE594F69C}\iexplore
  Time
  df 07 0b 00 01 00 02 00 0a 00 2e 00 06 00 86 01

- HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{FB5F1910-F110-11D2-BB9E-00C04F795683}\iexplore
  Time
  df 07 0b 00 01 00 02 00 0a 00 2e 00 07 00 90 02

- HKLM\SYSTEM\CurrentControlSet\Control\ServiceCurrent
  (Default)
  0x0000000e

- HKLM\SOFTWARE\Sophos\SAVService\Status\LastScan
  NormalScan
  0x56373f54

- HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU
  MRUListEx
  01 00 00 00 00 00 00 00 02 00 00 00 03 00 00 00 06 00 00 00 05 00 00 00 04 00 00 00 ff ff ff ff

- HKLM\SYSTEM\CurrentControlSet\Services\ApiSpyDrv
  ImagePath
  \??\c:\bin\ApiSpy.sys

- HKLM\SOFTWARE\Sophos\SAVService\Status
  UpToDateState
  0x00000002

- HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore
  Time
  df 07 0b 00 01 00 02 00 0a 00 2e 00 06 00 6d 00

- HKLM\SOFTWARE\Microsoft\Cryptography\RNG
  Seed
  be 1b 36 8c bf e7 fb 6a 73 8a c6 df e0 a1 a4 ec 65 b8 c2 3a c9 33 20 cf 01 cd 72 88 65 a6 97 e6 00 d4 26 6f 99 6f 7f 3e 84 a9 f0 ef 18 9d 51 f4 48 10 b6 47 40 38 1b 52 aa 71 5d 07 c8 5a 04 b9 05 f9 d1 6a 17 f4 0d a3 fc 85 74 f9 87 d2 15 39

- HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E2DD38-D088-4134-82B7-F2BA38496583}\iexplore
  Time
  df 07 0b 00 01 00 02 00 0a 00 2e 00 07 00 90 02

HTTP Requests

http://google-update.com/install/inst.php

DNS Requests

google-update.com