OPERATION HANGOVER

Unveiling an Indian Cyberattack Infrastructure

APPENDIXES

A: Telenor samples

B: Some examples of installers

C: Malware string indicators

D: Paths extracted from executables

E: Domain names

F: IP addresses

G: Sample MD5’s

Appendix A: Samples extracted from Telenor intrusion

```
00bd9447c13afbbb7140bef94e24b535, msupl.exe
02d6519b0330a34b72290845e7ed16ab, conhosts.exe
05c983831cad96da01a8a78882959d3e, svcohst.exe
10d8d691ec5c75be5dbab876d39501f1, cpyf.exe
1579467859b48085bdf99b0a1a8c1f86, splitter.exe
1676ded041404671bfb1fcfe9db34dcf, msspr.exe
21a52fedba7d5f4080a8070236f24a81, taskbase.exe
3eddb4a2c427ebba246ba2fa22dbdc50, vcmm.dll
61abb92f0fa605c62dab334c225ef770, winhost.exe
6367c72ef246798c2e8153dd9828e1fa, waulct.exe
82837a05f8e000245f06c35e9ddc3040, srsr.exe
85ce84970182be282436317ebc310c8e, msiep.exe
98ce593bfaeddbbbe056007525032e0d, msspr.exe
9d724c66844d52397816259abdf58cea, vmcc.dll
a25d1e14498dd60535c5645ed9f6f488, oprs.exe
bd52237db47ba7515b2b7220ca64704e, few important operational documents.doc.exe
bfd2529e09932ac6ca18c3aaff55bd79, windwn.exe
ca26ca59bafa3ae727560cd31a44b35d, winsvcr.exe
ecc8b373e61a01d56f429b2bd9907e09, chrm.exe
edc4bdfd659279da90fc7eab8a4c6de3, zfscu.dll
f21ca71866a6484a54cd9651282572fd, vtlp.dll
```

Appendix B: Some related cases based on behaviour and malware similarity parameters.

Name: "Pending_Electricity_Bill_(December-January).pdf.exe",
MD5: 681757936109f7c6e65197fdbb6a8655
Content: Pending_Electricity_Bill_(December-January).pdf
Content: wincert.exe
C&C : chkpoint.info

Name: "Horsemeat_scandal_another_Irish_company_suspends_burger_production.exe"
MD5: f52154ae1366ae889d0783730040ea85
Content: Horsemeat_scandal_another_Irish_company_suspends_burger_production.docx
Content: wincert.exe
C&C: chkpoint.info

Name: Unknown
MD5: f8b0e04506e57bfa2addade04e9a93d4
Content: "Indian_Involvement_in_Afghanistan.pdf"
Content: smsss.exe
Content: systems.exe
Content: csrsss.exe
Content: test.vbs
Content: start1.bat
C&C: sonification.com

Name: important.doc.exe
MD5: a7a223cebe5d89aa2d36864cb096b1b3
Content: important.doc
Content: smsss.exe
Content: exploer.exe
Content: ims.exe
Content: test.vbs
Content: start1.bat
C&C: sonificaton.com; researcherzone.net;

Name: Unknown, probably "ENRC__DEBT__INVESTORS__2012__for__your__Reference.exe"
MD5: e40205cba4e84a47b7c7419ab6d77322
Content: "ENRC__DEBT__INVESTORS__2012__for__your__Reference.docx"
Content: cftmont.exe
C&C: macsol.org; openhostingtalk.com;

Name: Unknown, probably "Deatils_for_the_ENRC_Board_Meeting_X1098977e79.exe"
MD5: a5a740ce2f47eada46b5cae5facfe848
Content: "Deatils_for_the_ENRC_Board_Meeting_X1098977e79.docx"
Content: acsrsss.exe
C&C: systoolsonline.org

Name: "Parminder bansil fraud with Nucleus software Full details.exe"
MD5: a7b5fce4390629f1756eb25901dbe105
Content: scan.docx
Content: winsvcr.exe
Content: wincert.exe
Content: wins.vbs
C&C: skylarzone.org; onlinestoreapp.net;

Name: "Reliance limited sustantibility issues full report 576676y8778.exe"
MD5: 0d5956dac2ac56f292ee8fa121450973
Content: Details.docx
Content: wauclt.exe
Content: wincerrt.exe
Content: wins.vbs
C&C: competitveedge.org; crystalrepo.org;

Name: update112.exe
MD5: 66203f184e4fdb004c0d24ede011ce6e
Content: msnger.exe
Content: igfxtrye.exe
C&C: wearwellgarments.eu; mysharpens.com;

Name: hp.exe
MD5: 74e571f9accf9fe1b4ea6ee0e02a5180
Content: Mendhar.doc
Content: isass.exe
C&C: forest-fire.com

Name: Unknown
MD5: 0f65c1202881f5c0e3d512aa64162716
Content: 20120316.pdf
Content: update.exe
Content: alg.exe
C&C: forest-fire.com; mailtranet.com;

Name: Unknown, probably "Details_for_the_ENRC_Board_Meeting_X10FR333_2012.exe"
MD5: 2895a9b0cf22cd45421d634dc0f68db1
Content: Details_for_the_ENRC_Board_Meeting_X10FR333_2012.docx
Content: avcsrss.exe
C&C: ezservicesenter.org; casinoaffiliatepartners.net;

Name: Unknown, probably "McKinsey_Quaterly_Newsletter_2012_____.exe"
MD5: 602f66b23b55dd2a22cd84e34c5b8476
Content: McKinsey_Quaterly_Newsletter_2012_____.docx
Content: cfmon.exe
C&C: casinoaffiliatepartners.net; openhostingtalk.com;

Name: important.exe
MD5: a1cad6b71ab30577ea8e204fab01ed47
Content: imprtant.jpg
Content: snmse.exe
C&C: cryptoanalysis.net

Name: Unknown, probably "Detail_description_of_ferro_chrome_silicon_and_ferro_chrome.exe"
MD5: 2102a18dc20dc6654c03e0e74f36033f
Content: Detail_description_of_ferro_chrome_silicon_and_ferro_chrome.docx
Content: ctmon.exe
C&C: macsol.org

Name: webmailapp.exe
MD5: 22a3a1d5a89866a81152cd2fc98cd6e2
Content: lnk.bat
Content: jre.exe
Content: dwm.exe
C&C: mobnetserver.com

Name: exploer.exe, winl.exe, lasss.exe
MD5: 634e4c640c4d7845a88faa5e0838ec0e
Content: winword.exe
Content: ssmss.exe
C&C: matrixfanclub.net

Name: Unknown
MD5: FFC2C9969B6A3B27FF96B926E9A6C18A
Content: ssmss.exe
Content: spoolsv.exe
C&C: follow-ship.com

Name: Unknown, probably "Taliban target creator, blow up ISI jihad lab.doc.exe"
MD5: E14B7985764E737333D531DAABF55970
Content: Taliban target creator, blow up ISI jihad lab.doc
Content: winword.exe
Content: csres.exe
Content: svchost.exe
C&C: redgolfclub.info

Name: Unknown, probably "MIRZAGHALIB.....IN2011.doc.exe"
MD5: 0680B9E247B2779799D4B32582F566C8
Content: MIRZAGHALIB.....IN2011.doc
Content: CSRSSS.exe
Content: SMSSS.exe
Content: start1.bat
Content: SYSTEMSS.exe
Content: test.vbs
C&C: sonificaton.com

Name: "agni5_inda's_deadliest_ballistic_nuclear_missile.exe"
MD5: 06E80767048F3EDEFC2DEA301924346C
Content: 1.pdf
Content: csrsss.exe
Content: dectop.ini
Content: lsasss.exe
Content: start.bat
Content: start1.bat
Content: test.vbs

Appendix C: Malware string indicators.

Text strings found inside malware.

HANGOVER 1.2.2 (C++ uploader)

```
Unable to load conf
Drives are:
%c:/
Could  not upload file...
encrypted
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
]Tfufss/mph
Uploading files to web server...
Source Directory:
%d out of %d uploaded
IMAGE
Dec: Couldn't open file:
enc_
Dec: Couldn't create file:
7kmL||HHt98jdf4z#F1+25jf7+3MIG
Enc: Couldn't open file:
Enc: Couldn't create file:
Couldn't open source :
MBVDFRESCT
90B452BFFF3F395ABDC878D8BEDBD152
Excep while up %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
{CAF1C46F-D91d7-C912F7F4F609}
WINAPP
[CryptProvider::Enc] Unable to encrypt data:
[CryptProvider::Enc] Unable to decrypt data:
 [ProvHandle::ProvHandle] Unable to create provider:
Microsoft Enhanced Cryptographic Provider v1.0
[CrypHash::CryptHash] Unable to create hash:
[CryptKey::CryptKey] Unable to create key:
E:\My\lan scanner\Task\HangOver 1.2.2\Release\Http_t.pdb
```

HANGOVER 1.3.2 (C++ uploader)

```
Unable to load conf
Drives are:
%c:/
Could  not upload file...
encrypted
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
]Tfufss/mph
Uploading files to web server...
Source Directory:
%d out of %d uploaded
IMAGE
Dec: Couldn't open file:
enc_
Dec: Couldn't create file:
7kmL||HHt98jdf4z#F1+25jf7+3MIG
Enc: Couldn't open file:
Enc: Couldn't create file:
Couldn't open source :
MBVDFRESCT
90B452BFFF3F395ABDC878D8BEDBD152
Excep while up %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
/c xcopy    "
    "
"        /Y
cmd
open
yahoo
windows dirctory
{AHAn4T-TRAH-PI12F7110903}
WINAPP
[CryptProvider::Enc] Unable to encrypt data:
[CryptProvider::Enc] Unable to decrypt data:
[ProvHandle::ProvHandle] Unable to create provider:
Microsoft Enhanced Cryptographic Provider v1.0
[CrypHash::CryptHash] Unable to create hash:
[CryptKey::CryptKey] Unable to create key:
D:\Monthly Task\September 2011\HangOver 1.3.2 (Startup)\Release\Http_t.pdb
```

HANGOVER 1.5.3 (C++ uploader)

%c:/
%userprofile%
encrypted
\sample2.txt
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
]Tfufss/mph
%d out of %d uploaded
0mbohvbhf/qiq
hvbhf
/qiq
tpojgjdbupo/dpn
EMSCBVDFRT
F390395ABFBD452BFFC87BE8D8DBD152
Excep while up %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
cmd
open
/c xcopy "
"
" /Y
dekstop.ico
EXE
mozila
windows dirctory
{2FC02671-E810-48b3-96DE-C4284E94EFC9}
WINAPP
T:\final project backup\uploader version backup\HangOver 1.5.3 (Startup)\Release\Http_t.pdb

HANGOVER 1.5.4 (C++ uploader)

%c:/
%userprofile%
encrypted
\sample2.txt
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
]Tfufss/mph
%d out of %d uploaded
0nztibs/qiq
hvbhf
/qiq
nztibsqfot/dpn
EMSCBVDFRT
F390395ABFBD452BFFC87BE8D8DBD152
Excep while up %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
bad cast
/c xcopy "
"
" /Y
cmd
open
dektpMSI89.ico
EXE
mozilaII
windows dirctory
{67FC0221-E016-48B3-8D9H-E894C854YF92}
WINAPP
T:\final project backup\uploader version backup\fud all av hangover1.5.4\with icon +shortcut link\HangOver 1.5.3 (Startup)\Release\Http_t.pdb

HANGOVER 1.5.7 (C++ uploader)

%c:/
%userprofile%
encrypted
%s%04d%02d%02d%02d%02d%02d.%s
\nts.txt
Uploaded file %s to web server
Failed to upload file %s
]Tfufss/mph
%d out of %d uploaded
tqbsl/qiq
o11c5v/dpn
EMSFRTCBVD
F39D45E70395ABFB8D8D2BFFC8BBD152
Excep while up %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
windows dirctory
C:\Users\Yash\Desktop\New folder\HangOver 1.5.7 (Startup) uploader\Release\Http_t.pdblink\HangOver 1.5.3 (Startup)\Release\Http_t.pdb

RON 2.00 (Appin) (C++ uploader)

```
VERSIONTYPE{he3l4m5k2n4m5kgs8c9f9}
Reg
Write
Option Explicit
on error resume next
Dim objShell, strRoot, strModify
strRoot = ''
Set objShell = CreateObject("WScript.Shell")
strModify = objShell.
(strRoot,"
","REG_SZ")
strModify = null
WScript.Quit
ScheduledTime
In OnTimer...
Available drives are:
%c:
Could  not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded to server
\Program Files
\WINDOWS
\Temp
\Local Settings
\Start Menu
\Application Data
\UserData
\Cookies
\Favorites
\SendTo
\NetHood
\PrintHood
\LocalService
\NetworkService
File Found %s
Fail to find Write time of file %s
Fail to Access file %s
File %s is inserted in list
File found with different Pattern :: %s
Uploading files to web server...
backup%Y%m%d%H%M%S
Source Directory:
\detail.txt
Search Process Failed
Started by timer
Couldn't open source file:
sendFile
FFF3F395A90B452BB8BEDC878DDBD152
access.php
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
SetTimer returned %d
%sBackup-%s.log
Backup*.log
C:\BNaga\kaam\Appin SOFWARES\RON 2.0.0\Release\Ron.pdb
```

RON 2.31 (Tourist) (C++ uploader)

```
CONTENT-LENGTH:
GET
 HTTP/1.1
Host:
Connection: keep-alive
]tztubn/fyf
xfcnjdsptpguvqebuf/ofu
0jnbhft0ubtliptu/fyf
[MONTHLYDESX]
 /c
In OnTimer...
Available drives:
%c:
Could  not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded to server
\*.*
\Program Files
\WINDOWS
\Temp
\Local Settings
\Start Menu
\Application Data
\UserData
\Cookies
\Favorites
\SendTo
\NetHood
\PrintHood
\LocalService
\NetworkService
\ProgramData
File Found %s
%s_%02d_%02d_%04d_%02d_%02d_%02d.%s
Fail to find Write time of file %s
Fail to Access file %s
File %s is inserted in list
File found with different Pattern :: %s
Uploading files to web server...
backup%Y%m%d%H%M%S
Source Directory:
\csb.log
Search Process Failed
Started by timer
Couldn't open source file:
BUGMAAL
2BB8FFF3F39878DDB5A90B45BEDCD152
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
SetTimer returned %d
%Y-%m-%d
%sInfo-%s.log
%c -
Info*.log
Y:\Uploader\HTTP\Tourist uplo\Tourist Uplo 2.3.1\Release\Ron.pdb
```

RON 2.33 (C++ uploader)

```
CONTENT-LENGTH:
GET
 HTTP/1.1
Host:
Connection: keep-alive
]mqtbtt/fyf
np{jmbvqebuf/dpn
0qmvhjo/uyu
Global\{FABF2E92-DA28-C7851754D733}
In OnTimer...
Available drives:
%c:
Could  not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded to server
Uploading files to web server...
backup%Y%m%d%H%M%S
Source Directory:
\csb.log
Search Process Failed
\*.*
\Program Files
\WINDOWS
\Temp
\Local Settings
\Start Menu
\Application Data
\UserData
\Cookies
\Favorites
\SendTo
\NetHood
\PrintHood
\LocalService
\NetworkService
File Found %s
Fail to find Write time of file %s
Fail to Access file %s
Started by timer
Couldn't open source file:
sMAAL
2BB8FFF3F39878DDB5A90B45BEDCD152
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
SetTimer returned %d
%sInfo-%s.log
%c -
Info*.log
E:\Datahelp\UPLO\HTTP\NEW Up For Trinity\RON 2.3.3\Release\Ron.pdb
```

RON 2.43 (Tourist) (C++ uploader)

```
In OnTimer...
/c xcopy    "
    "
"        /Y
cmd
open
appdata
windows dirctory
Global\{C78517FA-D28A-BF254D111010}
%02X
Available drives:
%c:
Could  not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded to server
Uploading files to web server...
backup%Y%m%d%H%M%S
Source Directory:
\ksb.log
Search Process Failed
\*.*
File Found %s
Fail to find Write time of file %s
Fail to Access file %s
Started by timer
Couldn't open source file:
SIMPLE
78DDB5A902BB8FFF3F398B45BEDCD152
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
SetTimer returned %d
%sReport-%s.txt
Report*.txt
S:\final project backup\task information\task of september\Tourist 2.4.3 (Down Link On Resource) -L\Release\Ron.pdb
```

RON 2.45 (Tourist) (C++ uploader)

```
%userprofile%
Appl
icati
on Data
Global\{C7121E67-D28A-BF25KD72EKK3}
TextX
windows dirctory
%02X
Available drives:
%c:
Could  not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded to server
Uploading files
 to web server...
backup
Source
Directory:
\ksb.log
Search Process Failed
\*.*
Fail to find Write time of file %s
Fail to Access file %s
Couldn't open source file:
SPLIME
5A902B8B45BEDCB8FFF3F39D152
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
%sReport-%s.txt
%c -
Report*.txt
N:\payloads\Trinity\Uploader\Tourist 2.4.5 (Down Link On Resource) -L(fud norton360internet security)\Release\Ron.pdb
```

Babylon 5.11 (C++ uploader)

In OnTimer...
happyfeet
StartServiceCtrlDispatcher: Error %ld,
OpenSCManager failed, error code = %d
Failed to create service %s, error code = %d
Service %s installed
OpenService failed, error code = %d
Failed to delete service %s
Service %s removed
Service %s stoped
ControlService failed, error code = %d
Service %s started
StartService failed, error code = %d
RegisterServiceCtrlHandler failed, error code = %d
SetServiceStatus failed, error code = %d
Information Loaded
Fail To Load Information
Unable to load configuration file.
Loaded Settings
Unable to send files to server. Check your connection and settings
Available drives:
%c:
Could not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded
\Program Files
\WINDOWS
\Temp
\Local Settings
\Start Menu
\Application Data
\UserData
\Cookies
\Favorites
\SendTo
\NetHood
\PrintHood
\LocalService
\NetworkService
File Found %s
Fail to find Write time of file %s
Fail to Access file %s
File %s is inserted in list
File found with different Pattern :: %s
Uploading files to web server...
Source Directory:
\csb.log
Search Process Failed
dectop.ini
SerName
ServerSettings
UpDir
CDir
UpFreq
Extensions
SourceDirectory
Couldn't open source file:
sMAAL
2BB8FFF3F39878DDB5A90B45BEDCD152
tata.php

Babylon 5.11 continued (C++ uploader)

```
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
SetTimer returned %d
%sInfo-%s.log
Info*.log
EFile Couldn't open
enc_
EFile Couldn't
7dasgfhgrtyethgfdhgfhgfgMIGG#F17
EncryptFile: Couldn't open source file:
EncryptFile: Couldn't create encrypted file:
vector<T> too long
[CryptProvider::Enc] Unable to encrypt data:
[CryptProvider::Enc] Unable to decrypt data:
[ProvHandle::ProvHandle] Unable to create provider:
Microsoft Enhanced Cryptographic Provider v1.0
[CrypHash::CryptHash] Unable to create hash:
[CryptKey::CryptKey] Unable to create key:
Y:\Uploader\HTTP\HTTP Babylon 5.1.1\HTTP Babylon 5.1.1\Httpbackup\Release\HttpUploader.pdb
```

Ron Dragonball 1.00 (C++ uploader)

```
Global\{2F3A8556-D28A-8F1BghS4POMD}
%02X
Available drives:
%c:
Could  not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded to server
Uploading files
 to web server...
backup
Source
Directory:
\ksb.log
Search Process Failed
\*.*
%s_%02d_%02d_%04d_%02d_%02d_%02d.%s
Fail to find Write time of file %s
Fail to Access file %s
Couldn't open source file:
SIMPLE
5A9DCB8FFF3F02B8B45BE39D152
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
%sReport-%s.txt
Report*.txt
D:\december task backup\TRINITY PAYLOAD\Dragonball 1.0.0(WITHOUT DOWNLOAD LINK)\Release\Ron.pdb
```

Ron Dragonball 1.02 (C++ uploader)

lnk
smss
windows dirctory
\smss
%02X
Available drives:
%c:
Could not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded to server
Uploading files
 to web server...
backup
Source
Directory:
\ksb.log
Search Process Failed
Fail to find Write time of file %s
Fail to Access file %s
Couldn't open source file:
SIMPLE
5A9DCB8FFF3F02B8B45BE39D152
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
%sReport-%s.txt
Report*.txt
C:\Documents and Settings\abc\Desktop\Dragonball 1.0.2(WITHOUT DOWNLOAD LINK)\Release\Ron.pdb

Ron FirstBlood (C++ uploader)

```
MONEYMATRA{G53UTDFWMC997654LMD}
Reg
Write
Option Explicit
on error resume next
Dim objShell, strRoot, strModify
strRoot = ''
Set objShell = CreateObject("WScript.Shell")
strModify = objShell.
(strRoot,"
","REG_SZ")
strModify = null
WScript.Quit
Hello World
InstallID
In OnTimer...
Available drives are:
%c:
Could  not upload file...
Uploaded file %s to web server
Failed to upload file %s
Didn't upload %s, because server already has this file
%d out of %d files were successfully uploaded to server
\Program Files
\WINDOWS
\Temp
\Local Settings
\Start Menu
\Application Data
\UserData
\Cookies
\Favorites
\SendTo
\NetHood
\PrintHood
\LocalService
\NetworkService
File Found %s
%s_%02d_%02d_%04d_%02d_%02d_%02d.%s
Fail to find Write time of file %s
Fail to Access file %s
File %s is inserted in list
File found with different Pattern :: %s
Uploading files to web server...
backup%Y%m%d%H%M%S
Source Directory:
\detail.txt
Search Process Failed
Started by timer
Couldn't open source file:
sendFile
FFF3F395A90B452BB8BEDC878DDBD152
access.php
Exception occurred while uploading file %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
SetTimer returned %d
%sBackup-%s.log
Backup*.log
C:\BNaga\kaam\kaam\New_FTP_HttpWithLatestfile2_FirstBlood_Released\New_FTP_HttpWithLatestfile2\Release\Ron.pdb
```

Bitmask (C++ keylogger)

```
Layout File
SYSTEM\CurrentControlSet\Control\Keyboard Layouts\%s
KbdLayerDescriptor
Edit
tips_class32_asdasd
getkey/
Log.txt
[ESC]
[INSERT]
[MENU]
[ENTER]
[BKSP]
url = %s
Mozilla Firefox
Internet Explorer
 Session Start = %s  %s
==========================================
 Windows Title = %s
Content-Type: multipart/form-data; boundary=%s
Content-Transfer-Encoding: binary
Content-Type: text/plain
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Disposition: form-data; name="uploaddir"
--%s
--%s--
Content-Disposition: form-data; name="submit" value="submit"
Exception occurred while uploading file %s: %s
getkey.php
F12BDC94490B452AA8AEDC878DCBD187
File
WScript.Quit
strModify = null
","REG_SZ")
strModify = objShell.RegWrite(strRoot,"
Set objShell = CreateObject("WScript.Shell")
\Software\Microsoft\Windows\CurrentVersion\Run\HotKeyscmd"
strRoot = "
Dim objShell, strRoot, strModify
Option Explicit
HKEY_LOCAL_MACHINE
HKEY_CURRENT_USER
\Run
\CurrentVersion
\Windows
Software\Microsoft
\regw.vbs
%userprofile%
WM_KEYDOWN_STR
WM_SETFOCUS_STR
Global\{2194ABA1-BFFA-4e6b-8C26-D191BB16F9E6}
BitMask Pvt. Ltd.
```

Klogger (C++ keylogger)

Edit
<LeftArrow>
<RightArrow>
<UpArrow>
<DownArrow>
<BACKSPACE>
<Home>
<PageDown>
<PageUp>
<End>
<PrintScreen>
<Delete>
<F1>
<F2>
<F3>
<F4>
<F5>
<F6>
<F7>
<F8>
<F9>
<F10>
<F11>
<F12>
<Ctrl>
<Alt>
<Esc>
<WinKey>
<ScrollLock>
\NTUSR
temp
.log
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
MBVDFRESCT
90ABDC878D8BEDBB452BFFF3F395D152
Excep while up %s: %s
%02X
Log.txt
/c del "
cmd
open
lnk
alg
windows dirctory
\alg
E:\June mac paylods\final Klogger-1 june-Fud from eset5.0\Klogger- 30 may\Klogger- 30 may\Release\Klogger.pdb

Kmail (C++ keylogger)

```
[ClipBoard Data: "
Edit
MBVDFRESCT
90ABDC878D8BEDBB452BFFF3F395D152
Excep while up %s: %s
Content-Type: multipart/form-data; boundary=%s
--%s
Content-Disposition: form-data; name="uploaddir"
Content-Disposition: form-data; name="filename"; filename="%s"
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-Disposition: form-data; name="submit" value="submit"
--%s--
%02X
Wir
windows dirctory
temp
.log
Log.txt
/c del "
cmd
open
d:\May Payload\new keylogger\Flashdance1.0.2\kmail(http) 01.20\Release\kmail.pdb
```

Fuddol (Visual Basic downloader)

C:\Http downloader(fud)\Project1.vbp
PTTHLMX.2LMXSM
TEG
Open
send
Status
maertS.BDODA
Type
ResponseBody
Write
Position
tcejbOmetsySeliF.gnitpircS
Fileexists
DeleteFile

Updatex (Visual Basic keylogger)

UpdateEx
C:\Documents and Settings\Admin\Desktop\UpdateEx\UpdateEx\UpdateEx.vbp
MainEx
GetLogs
ProMan
HTTPClass
RedMod
UpdateEx
GET
user32
SetTimer
KillTimer
Fields
OpenHTTP
CloseHTTP
SendRequest
URLEncode
sys
sysname
path
title
data
adkey.php
POST
[TAB]
Text
[BSP]
[RET]
[CTRL]
[ALT]
[Pause]
[Esc]
[End]
[Home]
[Left]
[Right]
[Inst]
[Del]
[DEC]
[F1]
[F2]
[F3]
[F4]
[F5]
[F6]
[F7]
[F8]
[F9]
[F10]
[F11]
[F12]
[NumLock]
[ScrollLock]
[PntSrn]
[PGUP]
[PGDN]
http://google.com
HTTP Client
Content-Type: application/x-www-form-urlencoded
HTTP/1.1
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
LTService
Name

Updatex continued (Visual Basic keylogger)

Value
Server
Port
UserName
Password
File
Method
Referer
Reload
Data

Tymtin (Visual Basic keylogger)

frmTymTin
TymTin
proTymTin
l - l - e - h - S - . - t - p - i - r - c - S - W
p u t r a t S
----------[Clipboard Data]----------
(<-)
(Enter)
(Caps)
(Esc)
(Pup)
(Pdown)
(End)
(Home)
(LA)
(UA)
(RA)
(DA)
(Del)
(#)
(NumLock)
(Ctrl)
(Alt)
value1=1&value2=2
&slots=1&
&dis=no&utp=ap&mfol=
u s e rn am e
M S X M L 2 . XM L H T T P
M i c r o s o ft . X M L HT T P
M S X M L 2 . S e r v e r X M L H TT P
.txt
W inH t t p . W i n H ttpR e q u e s t
W i n H t t p . W i n H t t p R e q u e s t . 5 . 1
Open
C o n t e n t - T y p e
multipart/form-data; boundary=
SetRequestHeader
Content-Disposition: form-data; name="
upload1
"; filename="
Content-type: file
Send
ResponseText
/vbupload.php?pc=

Smackdown Minapro (Visual Basic downloader)

```
frmMina
C:\miNaPro.vbp
Open
send
ResponseText
&tg=
&tv=
&ts=
&mt=
%c%o%m%p%u%t%e%r%n%a%m%e%
%u%s%e%r%n%a%m%e%
S c r i p t i n g . F i l eS y s t e m O b j e c t
 t e m p
\programs
CreateFolder
GetFolder
Attributes
&tr=
/data/
Wscript.Shell
run
/snwd.php?tp=2&tg=
DownloadProgress
DownloadError
DownloadComplete
UserControl
#me#t#s#yS#gn#it#ar#ep#O_#2#3#ni#W #mo#rf# * #tc#el#eS#
Caption
[NoFiles]
=2=v==m===i===c=\==t==o====o==r==\==.=\===\==:===s=t=m=g===m==n==i===w=
-4--6-w-o---w---s---y---s---\--
Scripting.FileSystemObject
FolderExists
-r--i--d---n--i---w----
BeginDownload
PathToSignedProductExe
' = eman erehW elifataD_MIC morf * tceleS
Error
programfiles
CompanyName
\*.*
 W s c r i p t . S h e l l
SaveFile
CurBytes
MaxBytes
```

Smackdown Vacrhan (Visual Basic downloader)

```
pranVacrhan
Draw Circles
Timer1
Timer2
C:\new_smackdown8\pranVacrhanpr.vbp
*#*
*-*
advpack
IsNTAdmin
  w  i  nm  gmt s :\ \. \ r oo  t \S e cu r i t yC e nter
elect * from An
ExecQuery
DisplayName
 w in m g m ts : \\. \r oot\S e cu r i t yC  e  n t e r 2
WokasamWoirada
Select * from CIM_Datafile Where name = '
http://
&fil=
W S c r i p t. S he ll
S t art u p
SpecialFolders
\Themes Manager.lnk
CreateShortCut
TargetPath
IconLocation
W--i-n---d---o-w-s- --S-y---s-t-e-m--- --P-r-o----p-e---r--t--y--
WorkingDirectory
Save
programfiles
[NoFilesPresent]
Files Present on DropPath :
\*.*
Open
send
Status
Type
ResponseBody
Write
Position
Fileexists
DeleteFile
SaveToFile
Close
\OS.txt
OS Name
===h===t======t===p====:===/===/==
---h-t-----t--p-:---/--/-----
/first-time/
ResponseText
\Temps
CreateFolder
GetFolder
Attributes
[NoExists:
[Exists:
u s e rn am e
AVs List :
OS :
SystemDT : [
AppVersion :
AppPath :
DropPath :
/windata
```

Smackdown NaramGaram (Visual Basic downloader)

```
ProjNaramGaram
NaramGaram
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\Smack6\70\ProjNaramGaram.vbp
advpack
IsNTAdmin
\OS.txt
OS Name
OS Name:
UnKnown
w i n m g m t s : \ \ . \ ro ot \ Sec ur ity Cent er
elect * from An
ExecQuery
DisplayName
w i n m g m t s : \ \ . \ ro ot \ Sec ur ity Cent er2
WokasamWoirada
Select * from CIM_Datafile Where name = '
Error
programfiles
  u  s  e  r  p  r  o  f  i  l  e
\Temps
CreateFolder
GetFolder
Attributes
[NoExists:
[Exists:
u s e rn am e
W S c r i p t. S he ll
S t art u p
SpecialFolders
\Themes Manager.lnk
CreateShortCut
TargetPath
--s--y--s---d--m--.-c---p-l--,- -0-
IconLocation
W--i-n---d---o-w-s- --S-y---s-t-e-m--- --P-r-o----p-e---r--t--y--
Description
WorkingDirectory
Save
SaveToFile
Fileexists
Type
ResponseBody
Write
Position
Open
send
Status
run
WScript.Shell
ResponseText
/shopx.php?fol=../first-time
/first-time/
```

Smackdown Vampro (Visual Basic downloader)

```
vampro
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\compiled\SmkDwnNew(dual)\14-8\vampro.vbp
SmkDwn
*#*
*-*
reggubeDmetsyS
run
advpack
IsNTAdmin
Class
/first-time/
Files Present on DropPath :
Errors : [
/new_down/
&fil=
 u s e r p r o f i l e
\programs
CreateFolder
GetFolder
Attributes
 c o m p u t e r n a m e
 u s e r n a m e
[Exists:
[NoExists:
w i n m g m t s : \ \ . \ ro ot \ Sec ur ity Cent er
ExecQuery
CompanyName
w i n m g m t s : \ \ . \ ro ot \ Sec ur ity Cent er2
PathToSignedProductExe
' = eman erehW elifataD_MIC morf * tceleS
Error
programfiles
winmgmts:\\.\root\cimv2
Select * from Win32_OperatingSystem
Open
send
ResponseText
ResponseBody
Write
Position
Fileexists
DeleteFile
SaveToFile
Close
On Error Resume Next
Dim myFSO, Rula
Set myFSO = CreateObject(
myFSO.DeleteFile Wscript.ScriptFullName
Set Rula = CreateObject(
Wscript.Shell
Wscript.Sleep 5000
Rula.run Chr(34) &
Set Rula = Nothing
Set myFSO = Nothing
\rgrun.vbs
```

Smackdown Angelpro (Visual Basic downloader)

```
AngelPro
frmAngelica
Angelica
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\Smack6\90\92\AngelPro.vbp
ucDwn
*#*
*-*
advpack
IsNTAdmin
  w  i  nm  gmt s :\ \. \ r oo  t \S e cu r i t yC e nter
SpecialFolders
ExecQuery
DisplayName
 w  in mg m ts : \\. \r oot\S e cu r i ty C  e  n te r 2
WokasamWoirada
Select * from CIM_Datafile Where name = '
http://
&fil=
S t art u p
\Themes Start Manager.lnk
CreateShortCut
TargetPath
--s--y--s---d--m--.-c---p-l--,- -0-
IconLocation
W--i-n---d---o-w-s- --S-y---s-t-e-m--- --P-r-o----p-e---r--t--y--
Description
WorkingDirectory
programfiles
[NoFiles]
[NoExists:
[Exists:
Files Present on DropPath :
  u  s  e  r  p  r  o  f  i  l  e
\Temps
\OS.txt
OS Name
===h===t======t===p====:===/===/==
---h-t-----t--p-:---/--/-----
/first-time/
ChakMak
IGets
FlDwn
wait
active
DropPath :
/advdnx
u s e rn am e
AVs List :
OS :
SystemDT : [
AppVersion :
AppPath :
A  D  O D  B  . St r e am
Type
ResponseBody
Write
Position
FileExists
DeleteFile
SaveToFile
Close
run
```

Smackdown Soundsman (Visual Basic downloader)

Soundsman
VbDL
FrmSru
C:\Documents and Settings\Administrator\Desktop\NewDw\Soundsman.vbp
comodo
OS Name
C:\Wvs.txt
programfiles
avira
antivir
|Avira
avast
alwil
|Avast
avg
|Avg
bitdef
|BitDefender
|Comodo
eset
|Nod32
f-secure
|F-Secure
kasper
|KasperSky
mcafee
|McAfee
norton
|Norton
panda
|Panda
quickheal
quick-heal
|Quick-Heal
vba32
|Vba32
W S c r i p t. S he ll
S t art u p
SpecialFolders
\Microsft
.url
[InternetShortcut]
URL=
.exe
UserControl
.HTTPDownload
+.C:\WINDOWS\system32\WINHTTP.dll
WinHttp
CancelDownload
DownloadFile
DownloadProgress
DownloadComplete
DownloadError
InvalidUrl
GET
Accept-Language
en-us
User-Agent
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Accept
/
Content-Length
StrUrl
DestFile

Smackdown Cryp (Visual Basic downloader)

Searcher
Downl
syslide
D:\YASH\PRO\MY\DELIVERED\Downloader\tempdwn\Cryp of tempdwn\Project1.vbp
kernel32
Sleep
ExecQuery
IPAddress
MACAddress
RegWrite
UserControl
BeginDownload
DownloadProgress
DownloadError
DownloadComplete
URL
SaveFile
CurBytes
MaxBytes

Yashup (Visual Basic uploader)

My Windows Manager
DWN
TxtCname
Content Type of the File
TxtResp
TxtReq
D:\YASH\SOFTs\PRO\MY\DELIVERED\UPLOADERS\New_upl\bkup_nonObfus\plain\Project1.vbp
CSocketMaster
modSocketMaster
LinkFilter
ComputerName
MarloNa
RemotePort
RemoteHost
RemoteHostIP
LocalPort
State
LocalHostName
LocalIP
BytesReceived
SocketHandle
Protocol
CloseSck
SendData
GetData
PeekData
ConnectionRequest
DataArrival
SendProgress
Scripting.Filesystemobject
Drives
DriveType
Computername
Content-Disposition: form-data; name="
"; filename="
match
OK Winsock service initiated
Operation now in progress.
UserControl
BeginDownload
DownloadProgress
DownloadError
DownloadComplete
bytesTotal
Number
Description
sCode
Source
HelpFile
HelpContext
CancelDisplay
enmProtocol
RemoteHost
RemotePort
LocalPort
LocalIP
maxLen
requestID
bytesSent
URL
bytesRemaining
SaveFile
CurBytes
MaxBytes

Yashplayer (Visual Basic remote access trojan)

GroundPlayer
frmGround
TxtRamoz
C:\GroundPlayer.vbp
cmdshel
CSocketMaster
shells
Removeable
Network
CD-ROM
Disc
///C:[HD]
S t art u p
SpecialFolders
w i n m g m t s : \ \ . \ ro ot \ Sec ur ity Cent er
elect * from An
ExecQuery
w i n m g m t s : \ \ . \ ro ot \ Sec ur ity Cent er2
\System Config.lnk
CreateShortCut
TargetPath
sysdm.cpl, 0
IconLocation
Windows System Config
WorkingDirectory
Save
File
Fols
Fils
Find
Pass
Auth
Down
Erro
OkDo
Kils
Clos
Rstr
run
Dein
SheA
SheD
SheC
Uplo
/#/W/#/S/#/c/#/r/#/i/#/p/#/t/#/./#/S/#/h/#/e/#/l/#/l
Open
A D O D B . St r e am
ResponseBody
Write
Position
Shell started at:
Shell closed at:
Shell is already closed!
Shell is not Running!
OK Winsock service initiated
enmProtocol
RemoteHost
RemotePort
LocalPort
LocalIP
maxLen
requestID
bytesSent
bytesRemaining

DragonEye (Visual Basic remote access trojan)

MCircle
TxtRamoz
D:\YASH\PRO\MY\DELIVERED\RAT\Dragon-Eye\De-Mini\New_server\modify\New_LNK\Another_FUD\MCircles.vbp
cmdshel
shells
TxtRamoz
Removeable
Network
CD-ROM
Disc
W S c r i p t. S he ll
S t art u p
SpecialFolders
\Soundman
Find
Pass
Auth
Driv
Fold
Erro
OkDo
Kils
Clos
Rstr
Open
.exe
Dein
SheA
SheD
SheC
She3
Ht6w
Uplo
SheH
O p e n
Fols
Fils
.url
[InternetShortcut]
URL=
IconFile=
Iconindex=
DownloadProgress
CancelDownload
DownloadFile
.HTTPDownload
+.C:\Windows\system32\winhttp.dll
UserControl
DownloadComplete
DownloadError
InvalidUrl
GET
Accept-Language
en-us
User-Agent
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Accept
/
Content-Length
QOS bad style.
Shell started at:
Shell closed at:
Shell is already closed!
Shell is not Running!

Yashgame (Visual Basic remote access trojan)

```
 *.*                Naby Cards Objection                    *.*
01 - every player start game with 52 cards  (4 cards shown in his field + 47 cards hidden +1 card in action )
02 - the aim of the game is to try to finish your cards before the opponent
03 - the player who has the biggest cards in the 4 shown cards in his field will start the game
04 - there is 8 places in middle  from ace to king
05 - rules of game is somthing like Solitaire game
06 - first u have to check if u have card can move to the middle (from ace to king ) or the fields have card can move to middle
07 - if u have and did not play it u will loss your turn and your opponent will take the turn
08 - u can move the cards from u or from fields to your opponent by dragging the card to him
09 - u can drag the cards in fields up or down like Solitaire game
10 - your turn will finish when u click on your hidden cards and move the shown card to your card in action
exitme
startme
New Game
HELP
NETSCAPE2.0
Click if Objection
Label6
Nabeel
Amber Shown Cards Left
Amber Hidden Cards Left
Nabeel Shown Cards Left
Nabeel Hidden Cards Left
listace
picCards
playlist
labindex
shobjection
All Right Reserved By  nabeelhosny@yahoo.com
PySol solitaire cardset
D:\YASH\PRO\MY\DELIVERED\2012\DEMC\Without_ocx_class\NewCardGameBased\Project1.vbp
WsRkft23
updateme
checkobjection
doobjection
upateme
upteme
Prosdata
VB.TextBox
Text1
TxtRamoz
5.34.242.129
\pic\alarm.wav
She1
Shel
000
Text
File
Fols
Fils
\pic\yes.wav
\pic\addalarm.wav
\pic\wrong.wav
w i n m g m t s : \ \ . \ ro ot \ Sec ur ity Cent er
elect * from An
ExecQuery
DisplayName
w i n m g m t s : \ \ . \ ro ot \ Sec ur ity Cent er2
WokasamWoirada
Select * from CIM_Datafile Where name = '
\pic\Fail.wav
elbaevomeR
```

Yashgame continued (Visual Basic remote access trojan)

```
krowteN
MOR-DC
ksiD
u  s  e  r  n  a  m  e
 c  o  m  p  u  t  e  r  n  a  m  e
SheD
SheC
S  h  e  3
Uplo
|||
SheH
/#/W/#/S/#/c/#/r/#/i/#/p/#/t/#/./#/S/#/h/#/e/#/l/#/l
/#/
run
Find
Pass
Auth
Driv
Fold
Down
Erro
OkDo
Kils
Clos
rtsR
WScript.Shell
Shell started at:
Shell closed at:
Shell is already closed!
Shell is not Running!
```

Foler.A (C++ worm)

```
Unable to get  Location
USERPROFILE
\start.vbs
On error resume next
ComputerName = "."
Set wmiServices  = GetObject("winmgmts:{impersonationLevel=Impersonate}!//" & ComputerName)
Set s = WScript.CreateObject("WScript.Shell")
dim filesys, filetxt
Set filesys = CreateObject("Scripting.FileSystemObject")
Set filetxt = filesys.OpenTextFile(s.ExpandEnvironmentStrings("%userprofile%") & "\nttuser.txt", 2, True)
Set wmiDiskDrives =  wmiServices.ExecQuery ("SELECT Caption, DeviceID FROM Win32_DiskDrive")
For Each wmiDiskDrive In wmiDiskDrives
query = "ASSOCIATORS OF {Win32_DiskDrive.DeviceID='" & wmiDiskDrive.DeviceID & "'} WHERE AssocClass =
Win32_DiskDriveToDiskPartition"
Set wmiDiskPartitions = wmiServices.ExecQuery(query)
For Each wmiDiskPartition In wmiDiskPartitions
Set wmiLogicalDisks = wmiServices.ExecQuery ("ASSOCIATORS OF {Win32_DiskPartition.DeviceID='" _
& wmiDiskPartition.DeviceID & "'} WHERE AssocClass = Win32_LogicalDiskToPartition")
For Each wmiLogicalDisk In wmiLogicalDisks
filetxt.WriteLine(wmiLogicalDisk.Caption & "\")
Next
 Next
 filetxt.Close
 EXIT FOR
 Next
cmd /c "
open
cmd
svchost.
exe
\MyHood\
cmd /c attrib +h +s "
alg.
encrypted
ID_MON
\nttuser.txt
A:\
B:\
Media removable
*.*
Fixed disk
%userprofile%
\MyHood
error
Drive does not exist
Network drive
CD-ROM drive
RAM disk
/c xcopy    "
ccnfg
windows dirctory
C:\Documents and Settings\Administrator\Desktop\UsbP\Release\UsbP.pdb
explorer
%userprofile%
\MyHood
cmd /c attrib +h +s "
\MyHood\
svchost.
exe
alg.
D:\Monthly Task\August 2011\USB Prop\Usb Propagator.09-24\nn\Release\nn.pdb
```

Foler.B (C++ worm)

Unable to get Location
USERPROFILE
open
cmd
svchost.
exe
\MyHood\
cmd /c attrib +h +s "
smsss.
encrypted
ID_MON
\Data
A:\
B:\
Media removable
.
%userprofile%
\MyHood
error
Drive does not exist
Fixed disk
Network drive
CD-ROM drive
RAM disk
/c xcopy   "
ccnfg
windows dirctory
C:\Documents and Settings\Administrator\Desktop\UsbP\UsbP - u\Release\UsbP.pdb
Global\{EBLEY329-TRSU-PIG279110924}
explorer
%userprofile%
\MyHood
cmd /c attrib +h +s "
\MyHood\
svchost.
exe
smsss.
C:\Documents and Settings\Administrator\Desktop\nn\Release\nn.pdb

Appinbot Predator (C++ remote access trojan)

cmd.exe
OSVer
Win32s
Win9x
WinNT
OSPlatform
Intel
Unknown
OSArchitecture
ClientVersion
ClientBuildTime
TempDir
ModulePath
PID
ServerPort
ServerAddress
RetrySeconds
Instances
ForceInstall
BuildType
RELEASE
clienthost.com
Reconnecting...
Global\AbortAbClient
ABCLIENT
TMP
\agp32
Error %d moving file %s to %s
Invalid MD5 Checksum!
props
drives
list
dlist
Network Neighborhood\
get
file not found
exit
uninstall
restart
Error %d spawning new process
newclient
File not found
exec
mkdir
Error creating directory
ping
Unknown request
Global\
FIDR/
1.2
FIDR/%s
HLO
RPY
SUBSCRIBE %d
MSG
bot
CLOSE %d
ERR
END
ANS
NUL
c:\Users\PRED@TOR\Desktop\MODIFIED PROJECT LAB\admin\Build\Win32\Release\appinclient.pdb
C:\Users\PRED@TOR\Desktop\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb

Appinbot 1.2.12 (C++ remote access trojan)

cmd.exe
OSVer
Win32s
Win9x
WinNT
OSPlatform
Intel
Unknown
HostName
LocalIP
MacAddress
OSArchitecture
ClientVersion
ClientBuildTime
TempDir
ModulePath
PID
ServerPort
ServerAddress
RetrySeconds
Instances
ForceInstall
BuildType
RELEASE
clienthost.com
localhost
Global\ClientBOND
Global\Client
MYCLIENT
\mxpr32
Write message received out of sequence
Error %d moving file %s to %s
Invalid MD5 Checksum!
props
drives
list
dlist
Network Neighborhood\
get
restart
Error %d spawning new process
newclient
exec
ping
Alocalhost
FIDR/
1.2
FIDR/%s
HLO
RPY
SUBSCRIBE %d
MSG
bot
CLOSE %d
ERR
END
ANS
NUL
%sEND
C:\BNaga\backup_28_09_2010\threads tut\pen-backup\BB_FUD_23\Copy of client\Copy of client\appinbot_1.2_120308\Build\Win32\Release\appinclient.pdb
C:\pen-backup\Copy of client\Copy of client\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb

Appinbot 1.3.3 (C++ remote access trojan)

cmd.exe
TEMP
OSVer
Win32s
Win9x
WinNT
OSPlatform
Intel
Unknown
HostName
LocalIP
MacAddress
OSArchitecture
ClientVersion
ClientBuildTime
TempDir
ModulePath
PID
ServerPort
ServerAddress
RetrySeconds
Instances
ForceInstall
BuildType
RELEASE
clienthost.com
localhost
Global\ForceClient
Global\Client
MYBACKAPP
\mxp
Invalid MD5 Checksum!
props
drives
list
dlist
Network Neighborhood\
restart
Error %d spawning new process
newclient
ping
Unknown request
Unknown command
Global\
Kernel32.DLL
CreateToolhelp32Snapshot
Process32First
Process32Next
FIDR/
1.2
FIDR/%s
HLO
RPY
SUBSCRIBE %d
MSG
bot
CLOSE %d
ERR
END
ANS
NUL
%sEND
E:\Datahelp\SCode\BOT\MATRIX_1.3.3\CLIENT\Build\Win32\Release\appinclient.pdb
C:\BNaga\SCode\BOT\MATRIX_1.2.2.0\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb

Appinbot 1.3.4 (C++ remote access trojan)

Dim objShell
Set objShell = CreateObject("WScript.Shell")
HELPFILE
OSVer
Win32s
Win9x
WinNT
OSPlatform
Intel
Unknown
HostName
LocalIP
MacAddress
OSArchitecture
ClientVersion
ClientBuildTime
TempDir
ModulePath
PID
ServerPort
ServerAddress
RetrySeconds
Instances
ForceInstall
BuildType
RELEASE
clienthost.com
localhost
Global\{C5826427D996926CEC6D}
Global\{D996926C58264279F42}
MYBACKAPP
\mxp
Invalid MD5 Checksum!
props
drives
xlist
xdlist
Network Neighborhood\
newclient
ping
Global\
Lfsofm43/EMM
CreateToolhelp32Snapshot
Process32First
Process32Next
FIDR/
1.2
FIDR/%s
HLO
RPY
SUBSCRIBE %d
MSG
bot
CLOSE %d
ERR
END
ANS
NUL
%sEND
C:\Documents and Settings\Administrator\Desktop\Backup\17_8_2011\MATRIX_1.3.4\MATRIX_1.3.4\CLIENT\Build\Win32\Release\appinclient.pdb
C:\Documents and Settings\Administrator\Desktop\Backup\17_8_2011\MATRIX_1.3.4\MATRIX_1.3.4\CLIENT\Build\Win32\Release\deleter.pdb

Linog (C++ downloader)

```
%sConnection: Close
%sContent-Length: %u
%sContent-Type: multipart/form-data;boundary=----------------------------265001916915724
%sHost: %s
POST /%s HTTP/1.1
%s----------------------------265001916915724--
%sContent-Type: application/octet-stream
%sContent-Disposition: form-data; name="%s";filename="%s"
uploadedfile
----------------------------265001916915724
closesocket function failed with error: %ld
connect function failed with error: %ld
recv failed with error: %d
Connection closed
Error in opening a file..
c:\windows\temp\
GET /%s HTTP/1.1
sspool.vbs
  File Downloaded
 File not copied..%s
!DOCTYPE HTML PUBLIC
log.txt
.txt
/download/cdata/
c:\windows\temp\task.bat
c:\windows\system32\net view > c:\windows\temp\a1.tmp
c:\windows\system32\netstat.exe >> c:\windows\temp\
c:\windows\system32\net view >> c:\windows\temp\
c:\windows\system32\tasklist.exe >> c:\windows\temp\
c:\windows\system32\systeminfo.exe > c:\windows\temp\
@echo off
a1.txt
sysconfig.dat
/cupload.php
/cdata.php
ThemesManager
\ThemesManager.lnk
%.*s
cscript.exe sspool.vbs
%s,"%s","%s"
Cratsct "C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\"
End Sub
caliber.Save
caliber.WorkingDirectory = scpat
caliber.Description = "Windows System Property"
caliber.IconLocation = "sysdm.cpl, 0"
caliber.TargetPath = scpat & tcname
Set caliber = sysinterim.CreateShortcut(X & "\" & scname & ".lnk")
X = sysinterim.SpecialFolders("Startup")
Set sysinterim = CreateObject("WScript.Shell")
Dim caliber,sysinterim,X
Sub Cratsct(scpat,scname,tcname)
C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\
slidebar.exe
/cdata/slidebar.exe
C:\Users\hp\Desktop\download\Release\download.pdb
```

Iconfall (C++ Keylogger)

```
TZTUFN]DvssfouDpouspm
Tfu]Dpouspm]Lfzcpbse!Mbzpvut]
MyHttpClient
z([0-9]+)
w([a-zA-Z]+)
q("[^"]*")|('[^']*')
h([0-9a-fA-F])
d([0-9])
c([a-zA-Z])
b([ \t])
a([a-zA-Z0-9])
shell32.dll
--%s
Content-Disposition:
form-data;
name=
"deport"
"filename";
filename=
Content-Type:
text/plain
Content-Transfer-Encoding:
binary
"submit"
value=
"submit"
GET
POST
Cookie:
charset={[A-Za-z0-9\-_]+}
Content-Length: {[0-9]+}
Location: {[0-9]+}
Set-Cookie:\b*{.+?}\n
utf-8
{<html>}
{</html>}
F to create
tit=
cont=
Content-Length:
Content-Type: application/x-www-form-urlencoded
POST
iconfall
78DDB5A902BB8FFF3F398B45BEDCD152
00212
multipart/form-data;
boundary=%s
Global\{7F1FE98DA54-23EE99-A9C2A15D90}
Fatal Error: OLE init failed
open
cmd
\M.BSSPX^
\S.BSSPX^
\V.BSSPX^
\E.BSSPX^
\OVNMPDL^
Windows_Classic3264_asdasd
systemDir.l
/c ipconfig /all > "
MyMutex
```

Deksila (C++ Downloader)

%userprofile%
cmd
open
ROOT\SecurityCenter2
ROOT\SecurityCenter
SELECT * FROM AntiVirusProduct
WQL
displayName
WinInetGet/0.1
/downtab/test.php?cname=
&str=
&file=
GET
HttpQueryInfo failed, error = %d (0x%x)
InternetReadFile failed, error = %d (0x%x)
htt
p://
/downtab/
\temp\
sucessfully
&res=
Global\{DF97D191AD-92E9-FC504RC25E9A8A3F}
/c xcopy "
"
" /Y
dekstop2007.ico
mozila20
windows dirctory

Auspo (C downloader)

VBoxService
VBoxTray
VMware
VirtualPC
wireshark
SandboxieControlWndClass
SbieDll.dll
csetup32.dll
image/jpeg
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV2)
POWERS
AUSTIN

Slidewin (C Keylogger)

Software\Microsoft\Windows\CurrentVersion\Run
Software\Microsoft\Windows\CurrentVersion\
Run
C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\slidebar.exe
slidebar
Title =
@
[BackSpace]
[Tab]
[Pause]
[Esc]
[PgUp]
[PgDn]
[End]
[Home]
[LtArrow]
[UpArrow]
[RtArrow]
[DnArrow]
[PrntScrn]
[Ins]
[Del]
[WinKey]
[DpDnMenu]
[F1]
[F2]
[F3]
[F4]
[F5]
[F6]
[F7]
[F8]
[F9]
[F10]
[F11]
[F12]
[NumLock]
[ScrlLock]
[LtCtrl]
[RtCtrl]
[LtAlt]
[RtAlt]
[HomePage]
[MuteOn/Off]
[VolDn]
[VolUp]
[Play/Pause]
[MailBox]
[Calc]
[Unknown]
E:\Data\User\MFC-Projects\KeyLoggerWin32-mktserv\Release\slidebar.pdb

Gimwlog (MINGW C Keylogger)

```
file closed----------
md C:\ApplicationData\Prefetch\
copy taskkey.exe C:\ApplicationData\
move C:\ApplicationData\*.txt C:\ApplicationData\Prefetch
log.txt
C:\ApplicationData\
[RIGHT ARROW KEY]
[DOWN ARROW KEY]
[SHIFT]
[ENTER]
[BACKSPACE]
[TAB]
[CTRL]
[DEL]
[LEFT ARROW KEY]
[UP ARROW KEY]
[CAPSLOCK]
size==========%d
new file----------
fname2==%s
move %s C:\ApplicationData\Prefetch\
```

Gimwup (MINGW C data harvester)

```
C:\ApplicationData\logFile.txt
copy winservice.exe C:\ApplicationData\
C:\ApplicationData\winservice.exe
MyDir
attrib +h C:\ApplicationData\winservice.exe
C:\ApplicationData\*.*
logFile.txt
*****
scan finished
*****/
=======inside while===========
*.*
Program Files
Program Data
WINDOWS
recycler
RECYCLER
Recycler
ApplicationData
 %d-%m-%Y %H-%M-%S
%s%c%s
C:\ApplicationData\Prefetch\
.inp
ab+
.doc
.docx
.ppt
.pptx
.xls
.xlsx
.pdf
.pps
```

Degrab (Delphi data harvester)

```
%s, ProgID: "%s"
----------------------------282861610524488
upload1
Name
$h$t$t$p
/vbupload.php
&slots=1&
value1=1&value2=2
&dis=no&utp=op&mfol=
$P$O$S$T
#M#S#X#M#L#2##.#X##M#LH##T#T#P#
open
multipart/form-data;boundary=
Content-Type
HHsetRequestHeader
Content-Disposition: form-data; name="
"; filename="
Content-Type: file
send
ResponseText
Exception message =
Fire.txt
Firefox is Not Installed.
\*.dll
userprofile
\flgs.dat
```

Appendix D: Project and debug paths extracted from executables

C:\26_10_2010\demoMusic\Release\demoMusic.pdb
C:\26_10_2010\New_FTP_HttpWithLatestfile2\Release\httpbackup.pdb
C:\26_10_2010\New_FTP_HttpWithLatestfile2_FirstBlood_Released\New_FTP_HttpWithLatestfile2\Release\FirstBloodA1.pdb
C:\A\KG\Release\winsvcr.pdb
C:\andrew\Key\Release\Keylogger_32.pdb
C:\app\Http_t\Release\Crveter.pdb
C:\BACK_UP_RELEASE_28_1_13\General\KG\Release\winsvcr.pdb
c:\BackUP-Important\PacketCapAndUpload_Backup\voipsvcr\Release\voipsvcr.pdb
C:\BNaga\backup_28_09_2010\threads tut\pen-backup\BB_FUD_23\Copy of client\Copy of client\appinbot_1.2_120308\Build\Win32\Release\appinclient.pdb
C:\BNaga\kaam\Appin SOFWARES\RON 2.0.0\Release\Ron.pdb
C:\BNaga\kaam\kaam\NEW SOFWARES\firstblood\Release\FirstBloodA1.pdb
C:\BNaga\kaam\kaam\New_FTP_HttpWithLatestfile2_FirstBlood_Released\New_FTP_HttpWithLatestfile2\Release\Ron.pdb
C:\BNaga\kaam\New_FTP_2\Release\ftpback.pdb
C:\BNaga\kaam\New_FTP_HttpWithLatestfile2_FirstBlood_Released\New_FTP_HttpWithLatestfile2\Release\FirstBloodA1.pdb
C:\BNaga\My Office kaam\Appin SOFWARES\HTTP\RON 2.0.0\Release\Ron.pdb
C:\BNaga\SCode\BOT\MATRIX_1.2.2.0\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb
C:\DD0\DD\u\Release\dataup.pdb
C:\Documents and Settings\abc\Desktop\Dragonball 1.0.2(WITHOUT DOWNLOAD LINK)\Release\Ron.pdb
C:\Documents and Settings\Admin\Desktop\Newuploader\Release\Newuploader.pdb
C:\Documents and Settings\Admin\Desktop\SysCache\SysCache\Release\SysCache.pdb
C:\Documents and Settings\Administrator\Desktop\Backup\17_8_2011\MATRIX_1.3.4\CLIENT\Build\Win32\Release\appinclient.pdb
C:\Documents and Settings\Administrator\Desktop\Backup\17_8_2011\MATRIX_1.3.4\MATRIX_1.3.4\CLIENT\Build\Win32\Release\appinclient.pdb
C:\Documents and Settings\Administrator\Desktop\Backup\17_8_2011\MATRIX_1.3.4\MATRIX_1.3.4\CLIENT\Build\Win32\Release\deleter.pdb
C:\Documents and Settings\Administrator\Desktop\Feb 2012\kmail(httpform1.1) 02.09\Release\kmail.pdb
C:\Documents and Settings\Administrator\Desktop\Keylogger_32\Release\Keylogger_32.pdb
C:\Documents and Settings\Administrator\Desktop\nn\Release\nn.pdb
C:\Documents and Settings\Administrator\Desktop\UsbP - u\Release\UsbP.pdb
C:\Documents and Settings\Administrator\Desktop\UsbP\Release\UsbP.pdb
C:\Documents and Settings\Administrator\Desktop\UsbP\UsbP - u\Release\UsbP.pdb
C:\documents and settings\cr01nk\my documents\visual studio 2005\projects\solution\release\stub.pdb
C:\Documents and Settings\Nand\Desktop\FtpBackup\FtpBackup\Release\Backup.pdb
C:\eqri\Debug\eqri.pdb
C:\fgh\Debug\fgh.pdb
C:\gfg\Debug\gfg.pdb
C:\MNaga\My Office kaam\Appin SOFWARES\HTTP\RON 2.0.0\Release\Ron.pdb
C:\N\kl\Release\winlsa.pdb
C:\N\sr\Release\waulct.pdb
C:\pen-backup\Copy of client\Copy of client\appinbot_1.2_120308\Build\Win32\Release\appinclient.pdb
C:\pen-backup\Copy of client\Copy of client\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb
C:\Release\wauclt.pdb
C:\sd\Debug\sd.pdb
C:\seee\Debug\seee.pdb
C:\smse\Debug\smse.pdb
C:\T\del\Release\winhost.pdb
C:\T\NoInterface\bin\ReleaseProduct\waulct.pdb
C:\Users\admin\Documents\Visual Studio 2008\Projects\DNLDR-no-ip\Release\DNLDR.pdb
C:\Users\God\Desktop\ThreadScheduler-aapnews-Catroot2\Release\ThreadScheduler.pdb
C:\Users\hp\Desktop\download\Release\download.pdb
C:\Users\neeru rana\Desktop\Klogger- 30 may\Klogger- 30 may\Release\Klogger.pdb
C:\Users\PRED@TOR\Desktop\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb
C:\Users\PRED@TOR\Desktop\MODIFIED PROJECT LAB\admin\Build\Win32\Release\appinclient.pdb
C:\Users\PRED@TOR\Desktop\MODIFIED PROJECT LAB\FBackup(source code)\FtpBackup - Copy\Release\Backup.pdb
C:\Users\Yash\Desktop\New folder\HangOver 1.5.7 (Startup) uploader\Release\Http_t.pdb
C:\wua\Debug\wua.pdb
C:\wuaucit\Debug\wuaucit.pdb
D:\december task backup\TRINITY PAYLOAD\Dragonball 1.0.0(WITHOUT DOWNLOAD LINK)\Release\Ron.pdb
D:\Desktop backup\Copy\appinbot_1.2_120308\Build\Win32\Release\appinclient.pdb
D:\Desktop backup\Copy\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb
D:\Documents and Settings\appin\Desktop\backup\Release\ftpback.pdb
D:\Documents and Settings\appin\Desktop\New_FTP_1\New_FTP_1\Release\HTTP_MyService.pdb
d:\final exe\check\Release\check.pdb
d:\May Payload\new keylogger\Flashdance1.0.2\kmail(http) 01.20\Release\kmail.pdb
D:\Monthly Task\August 2011\USB Prop\Usb Propagator.09-24\nn\Release\nn.pdb

D:\Monthly Task\September 2011\HangOver 1.3.2 (Startup)\Release\Http_t.pdb
D:\new versions\FTPUPLOADER\FTPUPLOADER_NK_1\FtpBackup_source\Release\Backup.pdb
D:\Projects\Elance\AppInSecurityGroup\FtpBackup\Release\Backup.pdb
D:\projects\windows\MailPasswordDecryptor\Release\MailPasswordDecryptor.pdb
d:\Projects\WinRAR\SFX\build\sfxrar32\Release\sfxrar.pdb
d:\Projects\WinRAR\SFX\build\sfxzip32\Release\sfxzip.pdb
D:\Sept 2012\HangOver 1.5.7 (Startup)\HangOver 1.5.7 (Startup)\Release\Http_t.pdb
D:\Sept 2012\Keylogger\Release\Crveter.pdb
E:\Data\User\MFC-Projects\KeyLoggerWin32-hostzi\Release\slidebar.pdb
E:\Data\User\MFC-Projects\KeyLoggerWin32-mktserv\Release\slidebar.pdb
E:\Data\User\MFC-Projects\KeyLoggerWin32-spectram\Release\slidebar.pdb
E:\Data\User\MFC-Projects\KeyLoggerWin32-Visor\Release\slidebar.pdb
E:\Data\User\MFC-Projects\KeyLoggerWin32-zendossier\Release\slidebar.pdb
e:\Datahelp\KEY\Hancock Kelo 1.1.3(crypted)\keytest\taskmng.pdb
e:\Datahelp\keytest1\keytest\taskmng.pdb
E:\Datahelp\SCode\BOT\MATRIX_1.3.3\CLIENT\Build\Win32\Release\appinclient.pdb
E:\Datahelp\UPLO\HTTP\HTTP_T\17_05_2011\Release\Http_t.pdb
E:\Datahelp\UPLO\HTTP\HTTP_T\20_05_2011\Release\Http_t.pdb
E:\Datahelp\UPLO\HTTP\NEW Up For Trinity\RON 2.3.3\Release\Ron.pdb
E:\Documents\Visual Studio 2005\Projects\EncryptionUtility\EncryptionUtility\obj\Debug\EncryptionUtility.pdb
E:\June mac paylods\final Klogger-1 june-Fud from eset5.0\Klogger- 30 may\Klogger- 30 may\Release\Klogger.pdb
E:\June mac paylods\Keylogger backup\final Klogger-1 june-Fud from eset5.0\Klogger- 30 may\Klogger- 30 may\Release\kquant.pdb
E:\My\lan scanner\Task\HangOver 1.2.2\Release\Http_t.pdb
E:\New folder\paylod backup\OTHER\Uploder\HangOver 1.5.7 (Startup)\HangOver 1.5.7 (Startup)\Release\Http_t.pdb
F:\Backup-HP-ABCD-PC\download\Release\download.pdb
f:\keyloger\KeyLog\keytest1\keytest\taskmng.pdb
f:\Projects\VS2005\WebBrowserPassView\Release\WebBrowserPassView.pdb
F:\Utility\Release\Utility.pdb
G:\august\13 aug\HangOver 1.5.7 (Startup) uploader\Release\Http_t.pdb
J:\backup E\SourceCodeBackup\september\aradhana\HangOver 1.5.3 (Startup)\Release\Http_t.pdb
N:\payloads\Trinity\Uploader\Tourist 2.4.5 (Down Link On Resource) -L(fud norton360internet security)\Release\Ron.pdb
P:\payloads\new backup feb\SUNDAY\kmail(http) 01.20\kmail(http) 01.20\Release\kmail.pdb
R:\payloads\ita nagar\Uploader\HangOver 1.5.7 (Startup)\HangOver 1.5.7 (Startup)\Release\Http_t.pdb
S:\final project backup\task information\task of september\Tourist 2.4.3 (Down Link On Resource) -L\Release\Ron.pdb
T:\final project backup\complete taskof ad downloader & usb grabber&uploader\New folder\with icon +shortcut link\HangOver 1.5.3 (Startup)\Release\Http_t.pdb
T:\final project backup\uploader version backup\fud all av hangover1.5.4\with icon +shortcut link\HangOver 1.5.3 (Startup)\Release\Http_t.pdb
T:\final project backup\uploader version backup\HangOver 1.5.3 (Startup)\Release\Http_t.pdb
T:\New folder\with icon +shortcut link\HangOver 1.5.3 (Startup)\Release\Http_t.pdb
V:\New folder\with icon +shortcut link\HangOver 1.5.3 (Startup)\Release\Http_t.pdb
Y:\final project backup\UPLODER FTP BASED\New folder\Tron 1.2.1(Ftp n Startup)\Release\Http_t.pdb
Y:\Http uploader limited account\Http uploader limited account\RON 2.0.0\Release\Ron.pdb
Y:\Uploader\HTTP\HTTP Babylon 5.1.1\HTTP Babylon 5.1.1\Httpbackup\Release\HttpUploader.pdb
Y:\Uploader\HTTP\Tourist uplo\Tourist Uplo 2.3.1\Release\Ron.pdb
Z:\Uploader\HTTP\ron uplo\RON 2.0.0\Release\Ron.pdb
C:\Documents and Settings\Administrator\Desktop\Main Uploader\ServiceSample.vbp
C:\Documentation\samples\ServiceSample.vbp
D:\PROJECT\samples\ServiceSample.vbp
D:\PROJECT\CMU\ServiceSample.vbp
C:\Users\HOME\Desktop\Main Uploader\ServiceSample.vbp
D:\applications\Http downloader(fud)\Project1.vbp
C:\Documents and Settings\Application\Desktop\smtp\new appin\Project1.vbp
C:\Users\PC\Desktop\Troj Creators\Common Main Uploader\ServiceSample.vbp
C:\Users\PC\Desktop\Common Main Uploader\ServiceSample.vbp
C:\Users\Yash\Desktop\PAYL\advd\projSmkdWn.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\compiled\SmkDwnNew(dual)\projSmkdWn.vbp
C:\Users\Yash\Desktop\SmkDwnNew\projSmkdWn.vbp
C:\PAYL\PAYL\advd\projSmkdWn.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\Smack6\90\92\AngelPro.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DEMC\Without_ocx_class\NewCardGameBased\Project1.vbp
D:\YASH\SOFTs\PRO\MY\DELIVERED\Downloader\tempdwn\Cryp of tempdwn\Project1.vbp
C:\Documents and Settings\Administrator\Desktop\WORKSTATION\Cryp of tempdwn\Project1.vbp
C:\Documents and Settings\Administrator\Desktop\Downloader\tempdwn\Cryp of tempdwn\Project1.vbp
D:\YASH\PRO\MY\DELIVERED\Downloader\tempdwn\Cryp of tempdwn\Project1.vbp
D:\YASH\PRO\MY\DELIVERED\RAT\Dragon-Eye\De-Mini\New_server\modify\New_LNK\Another_FUD\MCircles.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\12kib\Project1.vbp
C:\Http downloader(fud)\Project1.vbp
C:\miNaPro.vbp

C:\C\miNaPro.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\compiled\NewSmack(sep2012)\miNaPro.vbp
C:\A\miNaPro.vbp
C:\ProjNaramGaram.Vbp
D:\YASH\PRO\MY\DELIVERED\Downloader\tempdwn\tempdwn_hardcoaded(Good)\smackdown4\smack4.2\ProjNaramGaram.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\Smack6\70\ProjNaramGaram.vbp
C:\Documents and Settings\Administrator\Desktop\NewDw\Soundsman.vbp
D:\YASH\PRO\MY\DELIVERED\2012\KEYLOGGERS\English Only\new\without_Logfile\ProLocalKilr.vbp
C:\XXX\loclKeylr\ProLocalKilr.vbp
C:\proTymTin.vbp
C:\Documents and Settings\Micro-soft\Desktop\Keylogger Mozartin\UpdateEx\UpdateEx.vbp
C:\Documents and Settings\Administrator\Desktop\Kylo\Keylogger Mozartin\UpdateEx\UpdateEx.vbp
C:\Documents and Settings\Admin\Desktop\Keylogger Code\UpdateEx\UpdateEx.vbp
C:\Documents and Settings\Admin\Desktop\UpdateEx\UpdateEx\UpdateEx.vbp
C:\Documents and Settings\Micro-soft\My Documents\BackUp\Keylogger Mozartin\UpdateEx\UpdateEx.vbp
C:\Documents and Settings\Admin\Desktop\Trojan Code\ServiceSample.vbp
x.vbp
C:\Documents and Settings\Administrator\Desktop\Keylogger Mozartin\UpdateEx\UpdateEx.vbp
D:\Work\UpdateEx\UpdateEx\UpdateEx.vbp
C:\Documents and Settings\Admin\Desktop\Keylogger UpdateEx\UpdateEx\UpdateEx.vbp
C:\pranVacrhanpr.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\Smack6\70\81\pranVacrhanpr.vbp
C:\new_smackdown8\pranVacrhanpr.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\compiled\SmkDwnNew(dual)\14-8\vampro.vbp
C:\GroundPlayer.vbp
D:\YASH\PRO\MY\DELIVERED\2012\DEMC\GroundPlayer.vbp
D:\YASH\SOFTs\PRO\MY\DELIVERED\UPLOADERS\New_upl\bkup_nonObfus\plain\Project1.vbp
C:\Documents and Settings\Administrator\Desktop\New_server\modify\Calculator.vbp
C:\Users\Yash\Desktop\WinSockAPI_Fud1\WinSockAPI_Fud\Project1.vbp
C:\wylgoh\gmbor.vbp
r.vbp
C:\Documents and Settings\Administrator\Desktop\SlayerUD\New_server\Project1.vbp
s.....vbp
C:\H\Horiginal\Project1.vbp
C:\cameraman.vbp
C:\SimpleTCPChat.vbp
D:\YASH\PRO\MY\DELIVERED\2012\UPLOADER\BOTH\Project1.vbp
C:\Documents and Settings\Administrator\Desktop\HOG_ver3\Client\BkUPs\withoutArrayBkup\withoutArrayBkup(with WMI)\ServerZ\Server.vbp
D:\YASH\PRO\MY\DELIVERED\2012\sdsdasdwasdasdasdasdasd\RAT_pramala\Project1.vbp
E:\MY\DELIVERED\2012\DOWNLOADERS\compiled\snaperCompressVb\bkups\ServerItan\Project1.vbp
C:\Documents and Settings\Administrator\Desktop\WORKSTATION\tempdwn_hardcoaded(Good)\wit_LNK_without_office\PaintBrush.vbp

Appendix E: Domain names connected to case

acc0unts.g00gle.c0m.srccail.com
account.istpumpenunddosiertechnik.de.continuelogs.info
accounts.facbook.com.continuelogs.info
accounts.yandex.ru.continuelogs.info
accounts.ymail.com.mailcache.info
accounts.you-tube.com.analogwiz.org
accounts.yutube.com.continuelogs.info
activetalk.org
add-on-update.com
addon-updates.com
addoup.com
adminassistance.net
advnotifier.com
alr3ady.net
alreadytrue.com
amaxgrp.net
analogwiz.org
analysishunter.org
anoniemvolmacht.com
appinsecurity.com
applehostpoint.info
approvalclub.org
appworldblackberry.info
armordesigns.com.webmail-login.php.web-mail-services.info
autowid.com
autowidge.org
avandtotalsecurity.com
avatarfanclub.com
bbc-news.com.influxlog.org
bbupdate.net
bikefanclub.info
bkltmc.com
blogpublication.org
bluebird-restaurant.co.uk.infocardiology.biz
bluecreams.com
bmcmail.org
brandsons.net
braninfall.net
buildyourinfo.org
c0mpany4u.net
cabcardinc.net
cablecomsolutions.net
callersview.org
calling4you.com
callvoipnow.com
casinoaffiliatepartners.net
cellgame.org
centstat.org
cheetah4u.net
chiccounty.net
chkpoint.info
chroniclesupport.net
clamerword.net
clienttreasury.net
cloudone-opsource.com
cmegroups.net
cmxgrp.net
cobrapub.com
codetesters.org
com-mailservice.com
competitveedge.org
config-login.com
connectopen.info
continuelogs.info
coolhostingwebspace.com

cpbatch.org
cppblog.net
cr3ator01.net
crestboard.org
crowcatcher.net
crvhostia.net
cryptoanalysis.net
crystalrepo.org
csfserver.com
cupzon.org
currentnewsstore.com
customerpbr.com
deltaairlines.com.config.services.data.sesion.24s.digitalapp.org.evitalcare.org
deltadegger.net
denismoble.info
devilreturns.com
devinmartin.net
dexlab.info
digitalapp.org
digitooldeals.net
divinepower.info
doc.gmail.com-callgate-6.65.2.0-rms-6.65.2.0-
attachment.view.folderid.2messageid.ndi3n6rrgwnuefhoqwxgxdxmampattachmentid.20121206125116.5755maild0aa.evitalcare.org
docsforum.info
dosendit.com
downdossiersup.net
downfilesup.com
downtimesupport.com
easternsoft.org
easyhost-ing.com
easyslidesharing.net
educatediary.org
elementspro.org
endemol.com.mailcache.info
enetebookstore.com
enlighten-energy.org
esnucleus.org
espressoday.org
evitalcare.org
evolvingdesk.org
extrememachine.org
ezservicecenter.org
ezxen.org
ezyvalue.net
f00dlover.info
facebook.comaccountsserviceloginservicemail2.serviceaccountloginservicemail.info
fapize.com
fasttrackagent.net
fb-time.net
file-easy.net
filesassociate.net
filesconnect.info
filesforum.net
fileshreader.net
filetrusty.net
fiservtech.org
fistoffury.net
fitnessapproval.org
follow-ship.com
fonografia.pl
footwallfanclub.com
forest-fire.net
foxypredators.com
frameworkup.org
ftp.alr3ady.net
ftp.braninfall.net
ftp.currentnewsstore.com
ftp.devilreturns.com

ftp.forest-fire.net
ftp.global-internet.info
ftp.kungfu-panda.info
ftp.matrixfanclub.net
ftp.net4speed.net
ftp.nvidiaupdate.net
ftp.r3gistration.net
ftp.s3rv1c3s.net
fuzzyfile.net
gadgetscorner.org
gamezoneall.com
gauzpie.com
geonet.org.sockzon.org
get.adobe.flash.softmini.net
global-blog.net
global-internet.info
gnuvisor.com
go-jobs.net
google.accountservice.adminassistance.net
google.com.accountsserviceloginservice.info
google.com.accountsserviceloginservicemaileng.serviceaccountloginservicemail.info
google.com.acount.database.updates.services.web-mail-services.info
google.comaccountsserviceloginservicemailen.serviceaccountloginservicemail.info
groupskm.info
gxongame.info
h3helnsupp0ort.com
hangoutgroups.net
hangoutshop.net
hangovergroup.com.coolservice.continuelogs.info
hardwaregeeks.eu
heavenaffiliates.info
help-e.net
herbco.document.digitalapp.org
heritage-society.com
hifisure.org
hintover.com
hostmypc.net
host-stuff.net
hotbookspot.info
hotupdates.com.sockzon.org
hycoxcable.com
hycoxweb.org
i-dim.net
idsconline.net
imagebar.org
influxlog.org
infocardiology.biz
inforguide.org
infoteller.org
infraswap.org
innovatorspool.org
internet-security-suite-review.toptenreviews.com.avandtotalsecurity.com
internet-security-suite-review.toptenreviews.com.infocardiology.biz
islamic-teacher.org
itechtoys.org
jasminjorden.com
jerrycoper.org
joyfulhalloween.com
joymailserver.org
keepawayfromfire.com
khalistancalling.com
knight-quest.com
kungfu-panda.info
kyzosune.net
l0gin.faceb0ok.com.srccail.com
l0gin.y0utube.acc0unts.srccail.com
l0gin.yaho0.c0m.srccail.com
leicesterhigh.eu

lifelogs.org
linked-in.c0m.srcm-ail.info.srccail.com
linkedin.com-callgate-6.65.2.0-rms-6.65.2.0-attachment.view.folderid.2messageid.ndi3n6rrgwnuefhoqwxgxdxmampattachmentid.20121206125116.5755maild0aa.evitalcare.org
linkedin.com-uas.login-submit.account.session-full.login-3a5077708027557787984-csrftoken.buildyourinfo.org
linkspectra.com
linxauth.org
livesunshine.info
liveupdatesonline.net
login.facebook.com-confg.verify.login.src-ym.mailcache.info
login.live.com.continuelogs.info
login.live.com.mailcache.info
login.oriontelekom.rs.accountsserviceloginservice.info
login.yahoo.com-config-verify2.woline.info
logstat.info
lynberrg.com
m.ymail.com.continuelogs.info
m.ymail.com.mailcache.info
macsol.org
mail.carmel.us.exchweb.bin.auth.owalogon.asp.serviceaccountloginservicemail.info
mail.download.influxlog.org
mail.enrc.com-attachment.download.infocardiology.biz
mail.google.com-attachments.mail.u-01.infocardiology.biz
mail.joymailserver.org
mail.myorderbox.org
mail.telenor.no-cookieauth.dll-getlogon-reason-0.f ormdir-1-curl-z2fowaz2f.infocardiology.biz
mail.wildenstein.com.accountsserviceloginservice.info
mail-attachment.usercontent.evitalcare.org
mailcache.info
mailexservices.com
mailoff.org
mailservicesupport.org
mailssh.info
mailtechsolutions.org
makecmag.info
martcas.org
matewiz.org
matrixfanclub.net
maxtourguide.info
mcosine.org
megafairclub.org
megamediafile.com
mexchange.info
mgclog.com
mildstone.net
mjtag.org
mktserv.info
mobiappword.com
mobileappsupport.com
mobileappworld.info
mobilemyown.info
mobilesoftwaremanagement.info
mobilessoft.net
mobiletechspa.org
mobiltechsoft.org
mobnetserver.com
momate.net
mosglobe.org
motsoul.org
mozarting.com
mozilaupdate.com
mpale.org
msfileshare.net
msoftweb.com
mujahidtarana.com
my.screename.aol.com.mjtag.org
my.screenname.aol.com.accountsserviceloginservice.info
myscreenname.aol.com.srccail.com

myfilestuff.net
mymail.bezeqint.co.il.accountsserviceloginservice.info
mymyntra.net
mysharpens.com
myvoipp0wer.com
n00b4u.com
naclpro.org
net4speed.net
netmosol.info
neverforget1984.org
new-agency.us
newamazingfacts.com
newsgroupupdate.com
news-report.sockzon.org
nexterchk.net
nitr0rac3.com
nlsec.org
novelseller.org
ns1.activetalk.org
ns1.adobesoftwareupdates.com
ns1.alreadytrue.com
ns1.authserv.org
ns1.brandsons.net
ns1.braninfall.net
ns1.chronicleserv.org
ns1.competitveedge.org
ns1.continuelogs.info
ns1.ctswebup.info
ns1.dataconnects.net
ns1.directionmico.org
ns1.dmzone.info
ns1.doc-files.info
ns1.enetebookstore.com
ns1.esbasis.info
ns1.evitalcare.org
ns1.ezservicecenter.org
ns1.ezyvalue.net
ns1.f00dlover.info
ns1.forest-fire.net
ns1.foxypredators.com
ns1.go-jobs.net
ns1.gxongame.info
ns1.hackerscouncil.com
ns1.host-stuff.net
ns1.hotbookspot.info
ns1.infocardiology.biz
ns1.justdialforu.com
ns1.kjmailserv.org
ns1.knowledgepower.info
ns1.kungfu-panda.info
ns1.line-web.net
ns1.link-live.net
ns1.logserv.org
ns1.matrixfanclub.net
ns1.matrixtriology.com
ns1.maxtourguide.info
ns1.mjtag.org
ns1.naclpro.org
ns1.newamazingfacts.com
ns1.oscarneves.org
ns1.osonline.info
ns1.ozoneparty.info
ns1.pajerolive.com
ns1.parrotcatcher.com
ns1.pickmail.org
ns1.programmersheavengroup.com
ns1.racrage.info
ns1.s0pp0rtdesk.com

ns1.secuina.net
ns1.securedocx.info
ns1.sendsh33p.com
ns1.servwh.org
ns1.shopertock.net
ns1.sockzon.org
ns1.solraise.info
ns1.speedaccelator.com
ns1.sportswomen.biz
ns1.srccail.com
ns1.stretcherservices.net
ns1.supersolus.org
ns1.thedailynewsheadline.com
ns1.wearwellgarments.eu
ns1.woline.info
ns1.wvsolution.org
ns1.xmailserv.org
ns1.zerodayexploits.org
ns1.zonalship.org
ns1.zoninfo.org
ns2.activetalk.org
ns2.alreadytrue.com
ns2.brandsons.net
ns2.braninfall.net
ns2.chronicleserv.org
ns2.competitveedge.org
ns2.continuelogs.info
ns2.enetebookstore.com
ns2.esbasis.info
ns2.evitalcare.org
ns2.ezservicecenter.org
ns2.ezyvalue.net
ns2.f00dlover.info
ns2.forest-fire.net
ns2.foxypredators.com
ns2.go-jobs.net
ns2.gxongame.info
ns2.hackerscouncil.com
ns2.host-stuff.net
ns2.hotbookspot.info
ns2.infocardiology.biz
ns2.knowledgepower.info
ns2.kungfu-panda.info
ns2.matrixfanclub.net
ns2.maxtourguide.info
ns2.mjtag.org
ns2.naclpro.org
ns2.newamazingfacts.com
ns2.pajerolive.com
ns2.parrotcatcher.com
ns2.programmersheavengroup.com
ns2.s0pp0rtdesk.com
ns2.sendsh33p.com
ns2.serialxbox.org
ns2.shopertock.net
ns2.sockzon.org
ns2.speedaccelator.com
ns2.sportswomen.biz
ns2.srccail.com
ns2.stretcherservices.net
ns2.supersolus.org
ns2.thedailynewsheadline.com
ns2.vlogserv.org
ns2.wearwellgarments.eu
ns2.woline.info
ns2.zerodayexploits.org
ns2.zonrow.org
nvidiaupdate.net

oliveglobals.com
omg-pics.net
onestop-shops.com
onlinestoreapp.net
onlinewebmail.net
opendocs.info
opendocxsupport.net
openhostingtalk.com
opensourceforum.eu
opnsrc.net
osservices.info
outgateway.com
ozonerim.net
packetwarden.net
pajerolive.com
parrotcatcher.com
periodtable.eu
pfv6jyg1rdo9ptku.mxsvr.net
pharmamkting.eu
picasa-album.com
picasa-album.net
pics-bucket.net
piegauz.net
pizzapalace.org
plus.go0gle.com.servicel0gin.gxongame.info
primaaltus.org
privatemoneyblog.org
programmersheavengroup.com
r3gistration.net
rackitupstorenew.net
racmania.net
random123.site11.com
re-buke.com
redgolfclub.info
reliable-global.net
researcherzone.net
researchhunter.org
researchwork.org
rghsv.com.accountsserviceloginservice.info
rigidphotography.com
ritownship.net
ritualpoint.org
rockingdevil.net
s0pp0rtdesk.com
s3rv1c3s.net
saboresnativos.net
scrm-ail.info
searchports.info
secuina.net
secure.metacafe.com-account-login-token.accountsservicelogin.info
secure-copy.com
securedmx.net
secureplanning.net
secure-s.com
secure-solution.net
securingyourself.net
sendsh33p.com
server003.com
server006.com
server721-hans.de-nservers.de.continuelogs.info
serverrr.com
servetools.org
serviaccive.com
serviceaccountloginservicemail.info
serviceagent.us
service-secure.net
servicesonlinesupportinfo.com
servorder.org

sh3llypunk.com
share-home.net
shoperstock.com
shopertock.net
shopie.net
shopingcard.net
shopingcenter.net
shopping-hub12.com
shoppingspawn.com
shreadersupport.net
signaturedz.com
skylarzone.org
slamburger.net
smackdownfanclub.eu
smclog.org
smurfprotection.org
sochglobal.net
sockzon.org
softmini.net
softservices.org
softwaresupdates.info
sonificaton.com
sped0m00d.com
speedaccelator.com
spidercom.info
spiritlog.org
sports-interaction.net
sportswomen.biz
spstack.org
srccail.com
starcrunch.org
starmobnetservice.net
starshome.comeze.com
starsoel.org
store-fb.net
stretcherservices.net
supersolus.org
supertechnoclub.com
supportanswer.net
support-tech.info
synergyrealsolutions.net
systemcrack.com
systemupd.com
systoolsonline.org
taraanasongs.com
test.enciris.eu
testerspoint.info
thedailynewsheadline.com
tmkstore.org
tollmart.org
torqspot.org
tourtime.org
tow3r.info
tradeobjective.net
traderspace.org
trend-mico.net
trustworthyinfo.com
tulip.net.inforguide.org
undertaker.no-ip.org
unisafeservice.org
vall3y.com
viewerstalk.org
viragenonline.com
visordan.org
vkspoke.org
vkverbal.org
voip-e.net
vstrend.org

wagonact.org
wakeupindian.net
wearwellgarments.eu
webjavaupdate.com
webmail.juno.com.accountsserviceloginservice.info
webmail.stevens.edu.authenticateservicemail.accountsservicelogin.info
webmailaccountservicemail.info
web-mail-services.info
webmicrosoftupdate.net
wedzon.org
we-tour.net
whostmrage.org
wizcheck.org
wizsplit.org
wolfensteinx.net
woline.info
wondersofworld.eu
workinglab.org
worksmartplay.com
workspacecz.net
worldcitycenter.net
worldread.net16.net
worldtourismnews.info
wreckmove.org
www.alintiqad-newsonline.blogspot.com.continuelogs.info
www.analysishunter.org
www.cytanet.com.accountsserviceloginservice.info
www.ebox.co.il.accountsserviceloginservice.info
www.email.t-online.de.accountsserviceloginservice.info
www.espressoday.org
www.facebook.com-l0giin.php.mstl0giintocpassiive-trrue.contiinue-2fsiignin3factiion.handle.siignin3dtrrue26featture3dprromo.siignin26nl-en.us-idtmpl.sso.supersolus.org
www.facebook.com-l0gin.php.mstl0giintocpassiive-trrue.contiinue-2fsiignin3factiion.handle.siignin3dtrrue26featture3dprromo.siignin26nl-en.us-idtmpl.sso.chronicleserv.org
www.fonografia.pl
www.foxypredators.com
www.go0gle.com-serviicelogiin.autthserv.gxongame.info
www.google.com.accountsserviceloginservice.info
www.insing.com.accountsserviceloginservice.info
www.login.comcast.net.accountsserviceloginservice.info
www.login.oriontelekom.rs.accountsserviceloginservice.info
www.login.yahoo.com.accountsserviceloginservice.info
www.m.youtube.com.accountsserviceloginservice.info
www.mail.houseofjoyltd.com.accountsserviceloginservice.info
www.mail.luckltd.com.accountsserviceloginservice.info
www.mail.rediff.com.accountsserviceloginservice.info
www.mexchange.info
www.microsoft.com.chiccounty.net
www.mlogin.ymail.com.continuelogs.info
www.mobilesoftwaremanagement.info
www.my.screenname.aol.com.accountsserviceloginservice.info
www.mymail.bezeqint.co.il.accountsserviceloginservice.info
www.produkte.web.de.accountsserviceloginservice.info
www.secure.metacafe.com-account-login-token.accountsservicelogin.info
www.server721.han.de.nsserver.de.continuelogs.info
www.shoperstock.com
xylotech.org
ymadmin.net
you-post.net
youtube.com.accountsserviceloginservicemail.serviceaccountloginservicemail.info
youtube.comaccountsserviceloginservicemail2.serviceaccountloginservicemail.info
zendossier.org
zerodayexploits.org
zeusagency.net
zolipas.info
zonalon.org
zonalsky.org

Appendix F: IP addresses connected to case

These are some IP addresses that have at some point been related to the HangOver attack infrastructure. Note that IP addresses are non-static, and many of these may now be in use by legitimate users.

109.203.110.103
109.235.49.147
109.235.49.148
109.235.49.157
109.235.49.158
109.235.49.188
109.235.49.193
109.235.49.235
109.235.49.236
109.235.49.43
109.235.50.191
109.235.50.215
109.235.50.233
109.235.50.246
109.235.51.100
109.235.51.153
109.235.51.254
109.235.51.50
109.235.51.51
141.101.239.128
141.8.224.25
141.8.225.7
151.237.188.167
173.199.145.140
173.224.215.230
173.233.80.145
173.233.80.146
173.233.80.147
173.233.80.152
173.233.85.134
173.236.117.205
173.236.24.250
173.236.24.251
173.236.24.252
173.236.24.254
173.236.68.99
174.120.28.61
176.31.4.128
176.31.4.129
176.31.4.130
176.31.53.165
176.31.53.166
176.31.53.167
176.31.65.124
176.31.65.125
176.31.65.126
176.31.65.127
176.31.79.48
176.31.79.49
176.31.79.50
176.31.79.51
176.31.79.56
176.61.140.119
178.32.75.192
178.32.75.193
178.32.75.194
178.32.75.195
178.32.75.196
178.32.75.197
178.32.75.198
178.33.131.34
178.33.154.49
178.33.154.51
178.33.154.52
178.33.154.53
178.33.154.54
178.33.187.74
178.33.187.75
178.33.187.76
178.33.187.77
178.33.187.78
178.33.210.30
178.33.214.194
184.107.159.18
184.154.217.250
184.154.254.51
184.154.254.54
184.22.69.109
184.82.180.105
188.165.148.68
188.165.148.70
188.240.47.145
188.240.47.220
188.241.113.27
188.241.114.160
188.241.115.127
188.241.117.163
188.95.48.99
192.210.203.181
199.119.203.102
199.119.203.103
199.119.203.85
199.119.203.86
199.204.248.107
199.71.212.164
199.71.212.183
209.85.51.152
213.5.65.20
213.5.65.223
213.5.65.24
213.5.65.31
213.5.71.20
213.5.71.24
213.5.71.26
213.5.71.27
213.5.71.28
213.5.71.31
216.188.26.235
216.24.202.100
216.24.204.243
216.24.204.245
31.170.161.136
31.170.161.56
31.170.162.23
31.214.169.86
31.214.169.87
31.3.154.110
31.3.154.111
31.3.154.113
31.3.154.114
31.3.154.115
31.3.154.116
31.3.154.117
31.3.155.106
37.221.166.15
37.221.166.36
37.221.166.42
37.221.166.47
37.221.166.48
37.221.166.49
37.221.166.53
37.221.166.55
37.221.166.58
37.221.166.61
37.221.166.7
37.221.166.8
37.221.166.9
37.46.127.75
37.46.127.76
37.46.127.77
37.46.127.78
37.46.127.79
37.46.127.81
37.59.175.130
37.59.208.94
37.59.231.161
46.182.104.70
46.182.104.72
46.182.104.83
46.182.104.85
46.182.105.40
46.182.105.41
46.182.105.43
46.182.105.60
46.4.187.60
46.4.215.38
5.34.242.129
5.39.11.72
5.39.36.56
5.39.36.57
5.39.36.58
5.39.36.59
5.39.36.60
5.39.36.61
5.39.97.57
5.39.97.58
64.120.135.137
65.75.243.251
66.148.67.20
69.43.161.179
69.43.161.180
72.44.81.88
74.117.62.170
74.117.62.181
75.127.111.100
75.127.111.143
75.127.91.118
75.127.91.16
78.46.129.193
78.46.129.194
78.46.169.168
79.142.64.177
79.142.64.178
79.142.64.181
79.142.64.183
79.142.64.32
79.142.64.34
79.142.64.36
79.142.64.37
79.142.64.39
79.142.64.47
79.142.64.49
79.142.64.97
79.142.64.98
79.142.64.99
79.142.78.101
79.142.78.102
79.142.78.107
79.142.78.109
79.142.78.110
79.142.78.111
79.142.78.112
79.142.78.120
79.142.78.76
79.142.78.79
79.142.78.80
79.142.78.83
8.22.200.44
8.23.224.90
88.198.86.168
88.198.86.172
89.207.135.120
89.207.135.239
89.207.135.242
89.207.135.61
89.45.249.129
89.45.249.136
89.45.249.139
89.45.249.208
89.45.249.41
91.214.45.187
94.102.49.199
94.102.49.201
94.102.49.202
94.102.49.203
94.102.49.204
94.102.49.55
94.102.49.56
94.102.55.80
94.185.81.151
94.185.81.152
94.185.81.153
95.143.42.195
95.143.42.217
95.143.42.218
95.154.237.11
95.211.131.144
96.30.46.216

Appendix G: Sample MD5's

```
003ab666a73721404c8dae4613aec613
007d63bf9eb50c6e55125c00d32abdb6
00978e4b81ac577f328d6add75d0890e
00a0a6071c335f78c161cb4a3dcdc435
00bd9447c13afbbb7140bef94e24b535
0128f683e508c807ec76d5092eaaf22c
01774e34e8a444685b1499eef3406cd0
01a7af987d7b2f6f355e37c8580cb45a
01adea2d3707a343f5a6d149565c7ec5
01cda08113796a78702843a414f477c4
01cef8eeecbd5f9a4240d3e42c67c3c1
022894817bc575b94e1919eb1890f873
023d82950ebec016cd4016d7a11be58d
02ae85cb3677af2e5fc256e3bf7c9408
02d6519b0330a34b72290845e7ed16ab
02f3a2752b9a79ffccd99a1da8fb875c
032c4698839a52711cb18d6bc712d5b2
03f265a4e2e9a728749a6ef4e91e72b3
04293cc69b048fe1326560a457539b0c
047a1bb36e1de5f57e4a6f4d43ebf72b
04c2068c132f2c4af31f905f220503d6
0538fce0581b9233d34c6ad61a8f8139
05c983831cad96da01a8a78882959d3e
0680b9e247b2779799d4b32582f566c8
06b399d8bb5c5aeb4a04eda934ee819f
06ba10a49c8cea32a51f0bbe8f5073f1
06cbbff745c60c46e0996928c00ef28f
06e80767048f3edefc2dea301924346c
078d12eb9fc2b1665c0cc3001448b69b
0796ff1096f7456ef37d81a5b846b61b
07defd4bda646b1fb058c3abd2e1128e
0837671230288d68b99866197d79646b
08a3776a2c40e569f645a62fdd2fcac3
08f7ead1513bb921c9cdee334a370866
09947ba52932d10d3c859511a6d31e8f
09cdbd5273640ab23112b719c65e4902
0a0bcd8beb77e67a28a325d8d2a00254
0acdfd9ef4ed3e3f3d9d011aa5e7cd03
0ad9583aefede1f355759e0b674930cb
0b29cd6fc38c0459507e670e9c4547e0
0b38f87841ed347cc2a5ffa510a1c8f6
0b88f197b4266e6b78ea0dcb9b3496e9
0ba19063dea4ccae0afcd4208781f16b
0bbe6cab66d76bab4b44874dc3995d8f
0c0eb91f318da38e6684bd5250f68378
0c2cbfbe3c93b3502f9a60f5fa1188ad
0cace87b377a00df82839c659fc3adea
0d466e84b10d61031a62affcfff6e31a
0d5956dac2ac56f292ee8fa121450973
0e11b640253554595acdb7bfbf786b31
0e3282467dd99f3ceeb911cb1e8aaf5f
0e9e46d068fea834e12b2226cc8969fd
0f0e3dc18b12c7f8b1b03c73c842212c
0f47459581f6cd0e1766f1f436922ea5
0f65c1202881f5c0e3d512aa64162716
0f91c1d4ef8b239bb9a94d5546f071dd
0f98b7d1e113e5194d62bc8f20720a6b
0fbc01c38608d1b5849bf47492148588
109caa4b475927ddcc36278a32d013f2
10c0b0f7efbfc92dd13fdd0fd35ca260
10d8d691ec5c75be5dbab876d39501f1
111c0d178b3aea6c5aa7217feb0a44a3
1156011bcb049df9fbd0e6bbd7a108aa
118716061197ebcdae25d330aef97267
118ed6f8aa3f01428a95ae7ba8ef195c
11b70f93758ea494494855036818bbe3
11faa5da47a1f27de963e72631aaddd2
11fd24098d64632875d49160dc36bc6b
12874bf21a56709451f2df221c073f03
12eec20e7f672370269a9ec53cd744fb
13107b9455561e680fe8c3b9b1e8bc37
13197097b07e86516fa018a04aace83c
135a18c858bfdc5fc660f15d6e1fb147
13619025a126c56c3097d533414f2230
1370e187a12403ebf40d43285a23fed8
13fa45919341257b226f66e08da81cb4
1465248b7e2d512e426d8c72b42af47b
1487d1dc13314bf0431792b37ec67e2d
1489d2adf0328b6d7b42170095f966c9
153ac7591b9326ee63cd36180d39665e
15552ebdc4ebe5b4d2f71ab2d2e574cb
1579467859b48085bdf99b0a1a8c1f86
158ff697f8e609316e2a9fbe8111e12a
15e45c24dbe6034024fcffe4c358556b
166044bf473fc262ed97283c6e157eb5
1676ded041404671bfb1fcfe9db34dcf
168f2c46e15c9ce0ba6e698a34a6769e
16c11b381cff35283b879ec1a84f72e4
16c140fb61b6d22e02aa2b04748b5a34
16ff5f646196cf29792f5b159d1288b8
176e2277be875e55ad7211ff5e8df7a5
1785f20ad4883fee549f0aec5d20aaca
17a31d1075ebce41ba48a9efacb79d28
187dc6afa65cbdd8ee87a58271b56864
18b9e5fad0f015a0cf792818e9e0591c
18bc477fa12048fab8ec93d5ff942cf5
1972ae990751fa1b1532aa792bd5c160
1981cc08cdadc971e28768dc04d98637
```

```
199a180d3b5ef78a5fb79b0613be8dce
1a0268890c44ba8afe6ba7542c314ff4
1a1bc6e47d9dcbf6e3e7ce22d18b3628
1b1ab4e0ddfdb9e97609e78ab26e53f6
1b5d36f0d2da1fde3eb2b5fcbdc24948
1b7cbcc59199c595e495916698a2e82d
1be309eb99298c128b97649dcc7c9ad6
1c0e707cec96ac90969a5f16d66d1c6f
1c528591d28efbd485927a053bc86463
1ce331f0d11dc20a776759a60fb5b3f5
1e7b6424fb1a949c39653e00550eb8bb
1e9e8e724c000c9b9b6677a4d407538c
1eb7e455580a0e0d6296a00e81e31818
1ee41accf9a88121dac4a291252b8c49
1ee4bd29caf6aed2f3c7e263fa025468
1ff0cfaa775576322727b4edf636447e
2048a4ca1b1bbb13267643a6005cf92b
209692f3cd81ec0cd0dc4fa6b5be0f6b
2102a18dc20dc6654c03e0e74f36033f
2180573e7b41f82366a7637f60963b3b
21a52fedba7d5f4080a8070236f24a81
21aef1e6f22205edf261a08932728ab0
21e85f86403a89adb4a255d7017e06d2
21eb73d0e52ff4175d3dc5e58dcf7cc1
22588c6920f80398ae54e499b657f02d
227116763d49fae9277bc0d6bf40735b
22a3a1d5a89866a81152cd2fc98cd6e2
232f616ad81f4411dd1806ee3b8e7553
239bc16abb4aecbf6a1c1dac9a3f81e6
23a67d6bf0b727016a071817e99f0305
2409cf22defe0d8104d41a0e23d4a747
2479724f3d62c71fe64a1d2b3535d661
24874938f44d34af71c91c011a5ebc45
24f22d1391377249f21bfec81c3ea031
25472d552f3439d610a0ea0feea59b18
255057ba7f3bb62abd5963e42e5fd897
25536cdacdcc7867d4feb1fbf7e5e172
26fe2770b4f0892e0a24d4dddbbfe907
2729de09c88071bb71b55be98801e2c0
282ef2ba0cc14bb94f363374537d0eaf
28959167d0d01d5a2cf0dfacebdbf421
2895a9b0cf22cd45421d634dc0f68db1
28bbe03a89c491e6b236944423c26997
28bcbcdc1860108837542004bfe85c97
2902c48a767753d8e6a998c1c8efc77f
292a85212d0313480109382bb6099ebc
2b2a15a3204fe0130691772871d0c151
2b874fefbfe31f05d2af57e6d03f28bb
2bfe62815a7547bfa026417650fdf13e
2c20f8f92f51e41e31f40ab3fb71594b
2c338e8c3e5f28707739e05f7fb28ef9
2c5454f991fcef2ab42b899209dd4922
2c96c9eabb7a0adf8d361e144a40ffe0
2d7d9cb08da17a312b64819770098a8e
2df4497b3b95c77d6dc1d03deec57cb3
2e0c004523e7e4640805fb1c863a026f
2e5d57905d029acb1bc783637291e740
2f883722b2ff12189a34e520842cdab8
2fb421a64d130621911a9a4e43c4476f
2fdb2e334bc32856898c4c5a9b7038bf
2fea0759ac49e2b9dbf6416b0cab2d9d
300dbb020f1c0d19c5edfe718316a081
30881ad041d8f0c61c4b75641f0d9b17
309648d2fc431beaeeae9c9855e9325e
30a920f8c9b52aa8c68501f502e128eb
30c67399c176f16ad9dcde54e5a80bb3
3105b020e2bd43924404bc4e3940191b
312892649a2be80704f1601451246308
3166c70bf2f70018e4702673520b333b
31aceffa4cfb863b69d7f4b808def84b
31f024443a4e9767292404de20c5fe1f
32c0785edd5c9840f55a8d40e53ed3d9
32d461d46d30c5d7c3f8d29dd0c8a8c4
32dd4debed737bf2692796e6dca7d115
330157068e2530fe214ac41ae7005fc1
331db34e5f49ac1e318dda2d01633b43
337fe884412963289f8ce2fa8849258d
33840ee0b45f31081393f4462fb7a5b6
3475cb096dc082eaa92a7825726c7b8d
34b013d36146ba868e4dfa51529c47a4
34b834d70bfde92f095a9c529b1dcc48
34d534435579279a80a9caebd08bfedf
350ad4db3bcacf3c15117afddf0bd273
3519293de1a4f8f4b19e6b3669a62a22
3666f0ff389747774c6d8f8338cbba7b
36b3f39e7a11636adb29fe36bea875c4
36b8b6239713de260a3f0f1fd504507f
36fe5fed01c8ed3db85f116edec3904b
3705d2b2b5f6a7725837559b14029a98
37207835e128516fe17af3dacc83a00c
3738f1d3c3aaf841609fdeea94571714
37448f390f10eccf5745a6204947203a
376a0ed56366e4d35cecfcdbd70204b0
38198bf8e5d1d8b8d8e7101d4380da0e
3837ab0ffa02dd7fa49d97a15d95c587
3859f9099d24cc332cfca728211ac1f1
395e93a669414952f1c0bc6ecc4d6a9a
398201ed41d2e488abb7b2b17a9d6ff3
399c587050695f902de4cc145fdc1d72
39f28ac7c9a382bbfb28dee5fde7cbb0
3a0f8a86c7a13714c3fdd5e86dfb3df5
3a404a2a3e5fbf4c6bb5afb374730fe4
3a89f05c09425f03fe74b2242b119cce
3ae40259e505b5335b72879db4db3df0
```

```
3b9d65134b6529cf2d8d3cea22fe2fb7
3befb4b0ef87cd50573116d5780ba174
3c03b8436e9937ba3cfe18443b4c73b9
3c6819d61255f4f8f6f0adc6ddcd06cf
3cceb2261e9f9915687738ccfc9a19e7
3d0b1c6880e8ff3df185879a4ce2e0e6
3d6a8b2df08443c2aa4b6a07a9b55b16
3dc11072110077584b00003536d0f3ba
3dd61c872c02ad519b051b628eadeddb
3dfcaf660bc44ef3858ecb8685ec4f4d
3ed5f354c9bb9257eab81245e6b6416a
3eddb4a2c427ebba246ba2fa22dbdc50
3f13a0b574215659d83ab7ffd05d9102
3f411d306d4fc98fb71aa7383bb14d36
3f4e20175a0492658fb36bf4d5cf98c2
3fc11cd60c9e2bb29efe560e485abab9
3fd48f401edf2e20f1ca11f3dae3e2ef
4008e61496b011e29b6343ad886e8f6d
410c36c79525e257c64e061b4074d7af
413d6930e304cf248568049a3382018a
416b170d4d72b29f39dfc08450e8b406
41f83c83a9ae8d5558d2823cb00b4842
423519ae6c222ab54a2e82104fa45d12
42ca05f0a045eefe63ed213c97541179
43b020e78d7e361deff5aee8572a8e22
43be51e537ca7e78c83e51e3583b4984
4410874ef004bcc8de5e2bde0b786b6e
444cbc26f924a2be1b65140932e8f216
445c9450174a38f0f2d68389c6094e6b
44da2361d5baf33a18352613414b93e4
451b862c56aae581e0834a483eb9c8bd
45abc39bd7dfb34843840a50306fc1ae
46110a31e7c579285ff9c2339c8e9dbf
46416847e3f92d1ef8237fc29167b9a9
46ef141f709b2f6e3445bc2f09dd9c28
4791790c6fafb6253c41eb6bfe614ece
47a8258ec8823f6290af55fcdd39c0b5
47cc120cb27f219be6c915affde93c58
48847d66f9fb659edc7666ec3ca707da
488c3309c802bc8f17e0840335348077
48dc0cca7e2be0b30a764858c637bc10
4921c4c5cdd58ca32c5e957b63cf06cd
49527c54a80e1ba698e0a8a7f7dd0a7d
49e8bb0025b8e149c4cdf658ff6a6535
49f35654bf6d78e22b907866d40b3210
4a06163a8e7b8eeae835ca87c1ab6784
4a0e5f3c3d70dc287202eb0e342ca632
4a44b6b6463fa1a8e0515669b10bd338
4a870caa82cbffe8aac66ed61ffb718f
4abe3fae79903395a65a95c8af3738eb
4ad80ff251e92004f56bb1b531175a49
4b9f8cb4d87672611f11acbe3e204249
4c86c1669a943c1e41af898342ecf831
4d23053ec162eefe6eb41dcc5081c538
4d348c8a88dd1ef4c135bc8a1c117ed0
4da18d7cc1e4f1728764c3666bf2b290
4e8ab2aa18c6607c40f27948d3d85be4
4f3c4550526c8fe126b14a473d62a0f0
4f4c777bae424f334785253f0c90149e
4f634b5a1e8065f72e6e4547d016c1fe
4f82a6f5c80943af7facfcafb7985c8c
4f8e0066d4e73229685b7bea2b5a1bfa
4f9ada2c24a1d98769d51341f853751f
506f6dd4eafc9ec69db17988a380a4f5
50ff8922c4aabdbe3d801b7670a2241b
51188d746cca1a1c8a02401f7bd6a8af
5166dc1c8d12be1767e4749a40236169
519f62c558ebc127d18c3fef60e62349
51b1477e5cf2a14901392082d40bd70c
51ee31f234db61b488647915f8d7d4c8
521a56302eaaca9d2f1bbbe560011a1c
5433804b7fc4d71c47aa2b3da64db77d
54435e2d3369b4395a336389cf49a8be
5494d74fa04f15f63e9352e85a3d46ff
549fed3d2dd640155697def39f7ab819
555d401e2d41ed00bc9436e3f458b52e
55a107fb2646248dd7c1878ef93089a9
55aebca342d894a713c8417523081861
561f4c6e84f4921a84c75fd849172e15
56b51ffd47adc968ae498888bf502c63
56dbe80fe392d0f7e06875f9b9f0be8b
573b4ca365cd69d46d0951e5d48e6d32
57a4385cec4951bfbefc0391d43e6f8f
59520255caf6d7d8065b433ad1a62e0a
599863bb94e75b13be500710a704a567
59b15a8c29e329743fc4658ca565a173
59b1a7184141c9d3e4353274d7f00062
5a4faa7eeebffaaf9f1ebf3e3bd8e502
5a587618aebd8a8afa59de4d1e8ea933
5af184c69546383d1d6425a5a4502c2a
5b5fb0e64d9252e88d723e07ec85778a
5b95e0949fe2a7bb62e1cefae40e7de5
5bc2744a40a333dc089ac04b6d71154e
5bda43ed20ea6a061e7332e2646ddc40
5be0033c7838602fd014ffc90fc5af3d
5c11051760bb8e441e5a3cf1bc5a123c
5cdef8e8edc75dc5acf7bc532dd21fbc
5d735b1292845266b7414e81e1e0274a
5e11c3d9828dd3780eb4f787cf1ce67c
5f3ad37aaad2e6987f04129b50e39538
5f6052461511090 44c4b6a155f61a287
60064b5f8865e28c148231717d015155
602f66b23b55dd2a22cd84e34c5b8476
6084ed4d969b04cde21c55cc87904386
```

```
616eff3e9a7575ae73821b4668d2801c
61abb92f0fa605c62dab334c225ef770
620f234fda7eb6a1247c2da6a8e5da83
625b40cb0e5e69726e987c57663e3c7c
62b702a15a762692eda296b0aea270f9
63238f5cecb7af9ceb92191f865f8fd8
634e4c640c4d7845a88faa5e0838ec0e
6367c72ef246798c2e8153dd9828e1fa
638cbbd3284e9c1f048b5d02a83f2dcc
644008189aefa56362b16aeb973382ef
645801262aeb0e33d6ca1af5dd323e25
64787490bc1dd6ece556722133a0bdb9
649eb3db4159411ee6ec0d849274a825
64d6b372a14f64ac74db32929de8c84c
64f19c5776baaea96e1bfb0a0671afbd
6521ae44e485f811e9ce25913675161c
65bfb874a47b3e4920e33ee380060e8f
65bfeb977c3d9b1cc43a0e40f16a67cd
65c5d9c7f63266db08f6790c8bd675da
66203f184e4fdb004c0d24ede011ce6e
6687858f4140f6d6fa400ad6a9df8309
674dd075718ac664940eefba9ff3dd1d
67c064cc6fbd91b95ba529fecf71b5fa
681757936109f7c6e65197fdbb6a8655
68266b089c951d548899f1a716b7e149
68629a1a5c8c71714b663b744d223f4d
68b201a6b5f4cc4dfb83d820599dd447
68df0f3601a77a4e4d3a3dc58d8591ab
69278cb9e663c73573d220455cd5f8cf
6b666b91284d1da0b35b5584798de7cd
6ba65e2bcd8cfe224454371c1c592891
6bc80227468c9eb692d2438774a292c0
6bd5fa275f86fe88435be26fe7db0d23
6c74ebc20f08a48340a2f777bb12839a
6ca0e753c48da6414cbc83799282905a
6ca4104cf782a200e7c0a6bee14073e9
6d2d4f2aef3da83071d6e7f3a338fc87
6d692826793356a4083f3fc1b9d1cf16
6d7a3c843e92abd9f22f707202c63949
6d84c91e0f46e76c4bb4245d5b1a5118
6de00ae0bd81fead3fdf5c791595c8bd
6e16afddda66c94efc5e252b6d70c8ad
6e3da2f822627b82a7c859be365de4b7
6eb978e8bbe50f8c055209f46615b899
6ec2eeab1d4e9b93b2a94f4c05eeb8ca
6f2b8a0018038039d681c057411a124f
6f49ed067073a6db9e0cdcf1eb85d2ab
6fa31fc95898b34cc13041b72a215be3
6fc6214a9cc6bb1ed442beda98fe47e6
702d947f1110e6583dfdc2c1fd0f0a49
7108bf3948226cbe0667607c17df8c12
710d77de27034d6847c5fc2a790b2f5f
716b1c26faa3f674023aae670d3980f2
716f1eb978f6913ab62d78ed60861c74
71962a63a27e91626c5f22643da17027
7244aaa1497d16e101ad1b6dee05dfe3
7261d3d4d2cbd08f620ebaff827c91ef
72b78414ebee4cf56d129b6c8f45bf06
7302c6cb4c6ed4bb560d2019087434c9
734e552fe9ffd1ffdea3434c62dd2e4b
736ab06b46a01781a7af4f4a44ea57da
74125d375b236059dc144567c9481f2a
7417af55a9f3c61dbfef82f06a89e9d9
749c7b656eb765ed2c3e118a809c1a83
74e571f9accf9fe1b4ea6ee0e02a5180
74faad620de94a14d1cd43285ad15d15
7520c26b7ab872d44f1f0f1ca9aaab21
7550db173b1beeb7e6c545b97f2cce02
75d981ff0b6be08fb9b32a3c1cda9ddb
761acc13816a6840bb5f52fb43df45b1
7655868c4a3ed2cd978a84971b7aab54
76643813358b9198b6aed437eb7b5210
770fc76673c3c2daadd54c7aa7ba7cc3
77167a0c6ba3eb7461cdf52529feeeca
77205ea54ceda3be358d84db1c0d6b2b
7792ecfccae54102aafc0a8ad2bee762
77ad01d9e96a5a4797485aaeb37e2545
77bed210299f6d834c35e676ef557b95
77e88fa11cb0cf44c4691c04742d1b13
78b754304b0998ba58c54a4d0cb7c81d
78b8006cc9fc6ca45f8e7c8300e39dee
7926abf8d8047929858980805 42a42a7
794f8d94e4dc849b6276e024e1d18be7
79861cc8fa3860c3e91cdb591d8bad44
799b33f9a5fae1d29cfd66378c6dc790
79f3b5230012e5dde7657292f7e7d5bd
7a0f03c202c719994cbf0b62c1859e5c
7a10c2c0581d01f3d4f8101bbf6468b1
7a54a65cae902669cdeca4ec4b262d4c
7aeda30a2824ab86717cd3f6f09f5adc
7b75646902fdb9e212d59539c1f4875a
7b9cc2aa6e2dd13eec37f1fcb4a74ea6
7c37c6d89ed05fb264d8fe0acd795fd2
7d42db873cae7b2ee156766e9838808c
7de3b3fbe1ae69dcad2e45bf79bdac93
7e74334c1495a3f6e195ce590c7d42e5
7e9632a2aff99725674ef400f45f7c22
7edab76693800fd1617ba23c7a6aad88
7f11ec3504cb4564ffadfae4807a1dcc
7f48ebd87fda0840dc749a3064361b9c
7f6247ba5eb67e78b3c8fe92f50573a5
7f7b2ade0eb1496e3cff2fa7de5dc591
7fd31bf24537a50a0057dbd4781d2651
7fe7e4cd95507c6633b5427d077d84c9
```

```
8017684a46d91f59e7316594c877911d
80fbeba3da682570c4db0482cd61b27d
8172e9dcb3b0673cd673780f1024d07f
817efec9c2217afe5dec94fcd127d5e1
81c33d5c2d1d71d2639283be169ad235
81e8be75a7f2f368aa8e7caf001d72bd
81f84b1bdf6337a6e9c67be2f51c50e0
82837a05f8e000245f06c35e9ddc3040
828ee96b1063ac21a06b9f4d84bf56a2
82ac6a24d33c10630c65168e69d02b69
82bba197bc3f1a1e1f0ae0ba1de16565
82c23a939a34e4b2f9fa693306c494f1
82c2b9226ff7cb27cd12e573116b6041
832b368e612fe35f46ba2281e751a41c
8386891ad94d249454b8c27130d34858
8390e6ee81e0e47fa11320a24238c63c
83e591133ddd23ce56eb5cba8e56fbc0
83ff5bfe47959ec925e3180c3f0d32d6
8459fa25b7d93ef2f687eb0901bc94b0
8487320cec6a5bbc669b5a57cf0e9be6
84a2b843578c883a3fa59597c14cf709
859820011b21e57de55c22dabd227f11
85ce84970182be282436317ebc310c8e
862becc13747aafba8bfd755869251bb
87693d2559e369472fde254c1b410904
88fa9428b49618f8a8cda80fbd10890a
89239987f3675eb034a0fecebcb10ffb
89294c5eadeebfebbd208840344ae450
892cc671440a3abc394ce0d79fc30c6d
892e61053866e22649c0d31d6ae81165
894ec003921f19a1a1525a6e8102d75a
897414bdb9c75edacb16cc55c6defd4a
899a85c0428dcaa82b60ecb80059e26b
89d9851c162b98db2c7a2b4f6a841b2a
8a4f2b2316a7d8d1938431477febf096
8a8b5aa1de0dc301ec2732b63ab34c80
8b1a208216613bf0b931252a98d5e2b8
8b73fc88cc33a12a5de219aa511c7326
8ba4dadc9f8f10b3f181b59b8a254e95
8c64d4066b3da06f9b21e3ad3efb96ba
8d3290b7d1010d05ad6261b670d0b3d3
8d5e18ee1859ebce8c6db62ec936059a
8da3f87aeb1463fb5b513ecbd71e908c
8dad164966fb17c3c1f3e068c73080e0
8dbb459c3910d4ffe40e918164c5ba40
8e2a0ac8b32b01031d8671cae9b31e6d
8e2b530482822dc3b88d789fdc59ff44
8e42b9586f95d5cfe9f3fca435cb46a2
8e634f6981ad0aeea9d8365162d2cefe
8e861c37a592b136cf88ef71f7686d0a
8eac188d2818dd22b857b9cffac50c12
8ed7f7ff05fe0c29874b738a7099a4ee
8f9b63d93cd11598aecd3a3602547e8f
8fb39778c26f47d6e6596145dd650f69
9011ade473efc49f21985b6eb43b94ce
9073b3db88720a555ac511956a11abf4
915028829c8d64ad875c95cc916700ce
931bbc925f3547aabedb4449d4cbcbd8
9326e0362bfed701e7324e5f2abc88e0
933ad5988866c1dab72848b6b107ffad
93783861bb2e2034202dd1e1a25ac8ee
93df0d4c4e2f3e24ea67e092e705e3b9
9473eeaa0e125c3ea0b4965e1c04f17c
95c1c18003006c72d80e9e80ea1de4a8
95d2e0f6ebf675069b656857eb238399
961d6de08e0417b11c40e93940fc0918
963fbcdaec66a5fcd5664e932fa06f4d
9658c3539c3f83447301c5bfdb10e3f2
9678089aacaf3e147e50662c82c11d19
96a31d4e71f35be5d4bd53b1f935e386
96bce5c2bbbbdd33b305697ec57e7c50
96c0f2e8bd66759ea74fecc8843a8981
971c7f049f65a42881695e49f95de803
972a0334c22cc119793c262079cf5e0e
97a2dca830a582b2cadd798e26a01419
97bde23ae78ddabc36a0a46a4e5b1fae
98ce593bfaeddbbbe056007525032e0d
990b640a93cffe65f646d6584f82a4d7
9911f5b52f0177e26e3fd0a671bf370e
994c26013a352f808b86e95ab8e3fcce
9a09ae4973a9c754832d0a43fe0bad3e
9a20f6f4cddeabc97ed46aee05ac7a50
9ac6e3de69e75190862a94c94c193d2c
9af86aea0df8e24bca698bbed816e507
9b6305ee30004c72076e10b81c0847fb
9bcb294ecfbebff744e2a50b3f7099e6
9ca4b7fae929a361c383cc9d5bbe2edb
9cb05c69ddfd3d0c66b070fe1fde554a
9cc0d13fe3f0196d63e11f35480a1f01
9d4d45ce7bcf796cdfcf03c554c465fa
9d4e156235a41240fce7b240610109d8
9d724c66844d52397816259abdf58cea
9d959939bbf20bd582fc70f9e7b3a1e8
9de74a6b09858009766e5b9de510a764
9e05d3f072469093542afddb1c2e874e
9e3611e55f892cd58e2759ff482b6b54
9e5540383f78652a17b8efb7f454bc7c
9e60d7b0154949ebca8edd579db43949
9ec2c49fd9d1a1d8bea263b399e047af
9ecdcb9562e11d975479c0c83edf484d
9ece2dfbc4e36d05e6b5e07236122dcc
9edc36bd2b0b7d81fb1a7953309d2b52
9ef0cd655f1095ccfd591badc7e8c5bd
9ef3677054efe5ffc30fbbbfe2f833d9
```

```
9ef3dac0b10b3a9f30e3833aac9c09c8
9f63120b3b25e1f4b9ea5ad7a6246443
9f8e4b19167b5429eb0740b99dd0846f
9fab73462e197ffe2263476a4e84eb79
a017c6c90011a574bc8aa3bbd5756645
a06fa6ce10b76b2d23d580cc7132fa33
a10797c2e7c33f9cc2774165ef4152aa
a1cad6b71ab30577ea8e204fab01ed47
a1f8595d6d191dcbed3d257301869ce9
a229cdd723b1bfda03d371d880fbcaf8
a24c34fd4244f73fc94eaf6e52b7c350
a25568a3048cf6b83d72c5e9aae5ea75
a25a6f5d63ad340cca94d323fac353ed
a25d1e14498dd60535c5645ed9f6f488
a2ed2a5dfc3954a815cf165c2f07dfd6
a404522912212c4c245c0ddf387adee6
a487e68a4c7ec11ebff428becc64a06c
a4a2019717ce5a7d7daec8f2e1cb29f8
a53aff4075891c17ed9cdbdfcc124a1d
a5452bae7a46923c75acac2fc4f00df9
a59b6e79d4b8258ce71328b052de187c
a5a740ce2f47eada46b5cae5facfe848
a60808be831f8c2eea0f1ee489db0564
a6b8dac4827362a2abe6f53545067e8b
a6cf3fa8109456902649c19686a9dc64
a76a4ae87e36dfeebede0d65e86f3440
a7a223cebe5d89aa2d36864cb096b1b3
a7af2e83f611e9a774381b72ab448320
a7b5fce4390629f1756eb25901dbe105
a7f44192b9509d693e887407f1a51ae6
a8caf03b50c424e9639580cdcc28507b
aadbf8103cec7e5e5280befdd12c1e64
ab32a736abca3d4ed2158b070f9a5875
abf3f160a21e44cfd32d956b62b97e2c
ac5b7ac2c177125d192045e0a2ead278
acce099dddc2538e2c102b72bcf80759
acde02979b7b04a7645e00375f90f67d
ad6968de16778610382de7d0d817c6ab
ad6da049f4c66b317892f13769749add
ad9c7c4bc74455eb5fd858019fb9aa8c
adc4f82d1f4eedeb1ca33cd8edf776b0
addcd1e1f20c237ccf3fa5cf7528ce33
ae4814c615dfcdecad23b36d60833a52
af2ede825a1a82e76f31ae1ce8bf5ccc
af8979c31b5656ebfe82a68b2581256e
afd6cd07cf9607d264b1a3b99ab04ee6
b02a522948cbf1e3c7efe874b47530a6
b0f01a43a4b16036c330f660f3e1a38a
b13304be043ab59960a1dcd0f6db36ab
b13cc2e9a40642a1c75a961aae69773c
b19ef8ab9beb6cd1ff5da7f96c849309
b2394178d1a0a13a7d38e2d38c353d0e
b2d892c0950643f85c059382960fda8e
b35702471ac848a23b33b4b3aaaddf04
b36948f4cbc15ec702db62182c7b3e27
b3c86b52639c3003ed98ba51c4ce96e8
b481c8c1f802b78a6843cab4656bf5a4
b48543dd4b118e4241e4c2fb7aeec63b
b487603c1473758400894221de0f09c9
b48c2e42514ae1395e28fc94f6c8a6f1
b50a581406f8c9f2bb154fd93f665ef4
b51cbbbab70a7b89b0957b2fff4994e4
b5aafdfd12a2b47453d2346d12e7455b
b5b48580c118fcb9c6bdad5fc9fe6b08
b5d248e62a6c593d19104411b411146f
b60b389f2b76a473141acc3d111c77f5
b7b6dd5bcb3dcd87b74d1485b356a560
b7e63d3294ec10994b9a31237f23cb80
b86fd1cfe2de2ea841f8f522dee6370c
b888df619bf503a014f2358d0180076b
b99bb62795d76497f7cf31f9fedc9207
b9f7c59e384c9855419e9df7588ccd29
ba42eaebdedaf4f11aded2be2e352a7e
ba790ac25bb9c3c6259fdff8dce07e5a
bac7765a22eac877cac2b72a6e9e991e
bb447c0591ee8076c7e954f3fd21cb1a
bb9974d1c3617fcacf5d2d04d11d8c5a
bba2d1e279101d9df3ee135a997457c7
bc2890bc96392df403169400a78dd57a
bc348a63e08fce9831241681f40db925
bc588bed14699e30de569ee6e5f3578e
bcec4c74fa790f3ddbbb165ad9e99ca7
bd4d23945d4b1a1c66cf1dd1574f80c0
bd52237db47ba7515b2b7220ca64704e
bd6b05d51e4abafbc991bac5a70488e0
bd75bf1fe26f92ae2cab6beba0390d9e
bda1967f2491e5d792fa66e672951119
bdab33e31f27578eb99332c6c3104cd3
be026f4087fab37fe1dc1933b9e0c27a
bf8c0fff3269a84204d5bbcf08747c3d
bfd2529e09932ac6ca18c3aaff55bd79
c08fb1823e1751921d75956dac1534e2
c0a53e093be2c2cc2ed6145da8aa123f
c0b5003b311cb14b9aac4ea33c5a5eaa
c122f2b9a66f1689b92f547d3d32f455
c147843560520bde0bb4c713084fff1f
c1744d12b84aa775db213525dda92f6d
c176a80eae2f72604158bd72edb34535
c22402d7332e02fe97e98860373e3120
c2ebc8273c74dbd1c314bad73d61ccd5
c2f723532f591f410b1b47f1a81a2d51
c329b4e6c6e1d415d9ef5e21df47d785
c3bd5e3d49627aae106c0e21631deb70
c4130bcfbec35b377b512ceb64221293
```

```
c4353cf1b6a7ee1ad65a89ad4aa1ee22
c4820176eda9311ef0bcc378e001c54b
c487aa1c2ea83fca899d8afe4de9a6fd
c4f1247cc0b5ed8adb94a51030eb473a
c59563556fcf8a30cb51106b060e9940
c59edf29b81183976341c836ee20d610
c6a1efe22674241a90edc5d8e87ef29d
c6e3cc4ee93c00be4c0b47c18f790b40
c77869f6798a7586361bace2def8f00b
c7cb3ec000ac99da19d46e008fd2cb73
c7dc413c0278da72b587f0e1d7de8d61
c7e1d94a8a99caf71dbcdae62da25be4
c7f4610b6d91c32b46e5051c4f8055a0
c814e35d26848f910dd5106b886b9401
c82fdd5dd36fcc1560d987b588371f8e
c856ea7c61787e140350281edd9a8d03
c94267ba9c92f241379cdceed58777dc
c9e01b48800dfe10dec2bd985c36c05e
ca07a6e21204c72c14bc9429a6d33a71
ca26ca59bafa3ae727560cd31a44b35d
ca784b6fa1c2a100f6354adc93598e42
caafd33f40c79413f32b9585f94c2acb
cb22fb4e06f7d02f8cac1350d34ca0a6
cc0d2f297271314301a519f440f61f57
cc0d483ea30ddabe8ba03a570065b7b7
cc3d271204c73b90a7b346121d381892
cc553dbb3e7a559b40c8c6180ee50b9d
cc8e5734532115ba77c2c906e86711f7
cce0dea39415a01c4cab75088ed72b8e
cd27847be9c98d4c2a4addc6f83d849e
cd295ec65a67afda0f6e8558848b7623
cd7f9cc5e7f4350a432fb8ac231c9c82
ce00250552a1f913849e27851bc7cf0a
ce157212cd908bc0d3b16949822dec6f
ce305256740178562a57bc5b3f1a767e
cee292420bf0639773e6b2831bfb2e5e
cf33eff89f54c07e98e43c4c90813e08
cfa7be481258fb3fbc57e0d6b0f59a83
cfca701f169cc645a498ac82de41558f
cff2e20f9ec8e4cda4957ec3136bb9f9
d0484d7b9e9a5eac4d02ece03592ba8d
d0f1bea201b0d9fc788cbd086bccf750
d136733d7f4ec34795f35d26f418c70d
d41d855e141426d3d1e26b4343053728
d4a373c4fb39471d07808b6d0a6140b9
d4ae70568f7a2258cb764cee89c3238f
d51344e18dea14c8f54a6b718e994514
d534ba2ff2be9f1511d9e6ef9160bb53
d558fd40c9aaf2de3e96989041a31ee6
d55d778c2aa03864ef8fb9aeec9fd259
d581a1362f1699ae9df1d1d39f96f5e2
d58bbd49e6e8a78051f40b8ad1e45aea
d5b0c2de6176fac5d7eb01992df976f1
d5bfa0a259deb8abd7e3cc3aebd52afb
d5c5b98062b2c27e956af21377d92705
d5ff9201464048441963cdd60f54df9a
d62d941d86169f6feb64bf950805bcfd
d67418ddd0df67b3f77581ebde2df269
d6821dcf113e28e2c852febf5d0f2725
d69ebd83636d9110d1e5c15c587531ec
d6c74734109c53ade4e0333f59bad7e9
d6d8c27add8df8850869652376ceb766
d6f40e2fc74139ec12dec16a57ac738e
d6f8df14da5750a75b3e5ebe2c76125c
d75f75edb30460c7e156eac0274826b2
d76f0b6865b29ec4bc53d2e5744be2e6
d8747ae6fcdcf5fcb56a2ec6385dad9d
d8dcf2a53505a61b5915f7a1d7440a2e
d96aa87c25c9c491bee97aad65bafc9e
d9a8709ed2e45503c94599c718d467fd
d9c3b4e5faa03bc8d83396837bd7e23c
dafc6646d38269656755ac004d72ccbd
db2868a2388774ffb15018bb3b9ac872
dbff20daa468ad32faef998011abd897
dc39585d0c78a2dbd65afac5ef5c826b
dcdae3149e91b3e8e037097667218528
ddcfcd339b7f4996c630e62b2786aa56
dde215945d217d8c97dcc498f43cfa86
de37dde6db2b474ce3a93a7c9b920b82
de75038bae500ba981147f256102c83f
de81f0bdbd0ef134525bce20b05ed664
def441fb6719cd322389e3f594bef270
e095d5c7fc6486dd114e710cb7e197ca
e09cf62b3a987103279fd30160e66228
e14b7985764e737333d531daabf55970
e199162e1a74f6e25aedf4e15cb1efb6
e1e6ecf7f67d2a2f7efe81a280aa517d
e27adbf7491c18460c2924fad5c17e81
e2e5f97967468d4ec333704808d2d558
e2e61074624f8e644b39aa0789823813
e2f5b669f7de05dd964385adef52508b
e37f2c408cb9e96caf10639e2fe5e347
e37f420f2c1d7ad862a6643585fd7ebf
e3cf3b1d2a695b9b5046692a607c8b30
e3da83cb528fd257103685443f6fdf1e
e4016d5c0f7246a164399281b77507b6
e40205cba4e84a47b7c7419ab6d77322
e4d710b3898dfbfb46cd65b5215ee3ee
e4e851b679333928ceff068b5664efef
e51c94e0c018f17bab48711592df4274
e53b7073a592b01b35a10a6c76ff011f
e5479fac44383ca1998eb416aa2128f0
e6b45dfbd2c1e734f672e7a32fa6f9eb
e6f98c98db0f45e9d40b3466784764da
```

```
e74ce9ca4baccf2204ef6fbdf85e9817
e7d9bc670d69ad8a6ad2784255324eec
e80ac0ff50e56ac18186e4f9d6b44540
e8197e5bca1db7ffab1f073f6300004a
e88485650b92dc1ded4063e294fdfa0d
e8b68f541d7a992194b603c91c892cf1
e8dc919eda7fc8f1334fcb17d7ff9e00
e90d693f57ed778f517fd425038589ac
e92f739fe39e22002fe3a824084dd95b
e97c3bb9aeffc0559914b2d919cbff14
e992dfc3dedcf5e66b661dbc26fe932c
e9b311ef3530aa32e09ac335c9988d64
ea1d779a230cc17fed73e200d8350d37
ea988287da2c2f7ebfd707fe99ec7b16
ea9bfc25fc5bdc0b1b96f7b2af64f1ac
eae1693c74091a064052ea3d3b349615
ec760838ab731860054cf43b59a7d72f
ec98f37134c176b45332d8820aace69e
ecac2ce6e52c78718c0d0f7a99829136
ecb6aad44ee6bff763c5d8cacda65dbd
ecc8b373e61a01d56f429b2bd9907e09
ecf86588df072d4c574ee092e999e6a6
ecfc531241c71d27de9a8ef50f1ea8a7
ed4a58ba2f75f1b590fbaeaf762e4496
ed50096615da40cc95d3831ecf79187c
ed63183429ae909666fafe8b1fae63b4
ed6869f96a704d819616ec8d65823038
ed7907cf7f4469976c936a73067ad0ad
edc4bdfd659279da90fc7eab8a4c6de3
eddce1a6c0cc0eb7b739cb758c516975
eddd399d3a1e3a55b97665104c83143b
ee872cd570b14a513d675b02f408f586
eeee92081dbd7dabd05db3714f0987b6
eeef49fdb64a03a0c932973f117f9056
f0c08226ab52978f959d19bdba5b1d67
f0e4ca2583c95856370b4d779b27e255
f0e708e935b3f9ba39e8c9033381e22f
f11960e2d9666908433b4e5908ee85c2
f16b2c1c7e503ff8bc276ffbb4f862ee
f1799d11b34685aa209171b0a4b89d06
f21ca71866a6484a54cd9651282572fd
f2a46ad687356eb9099bc7269411f76a
f2bd203dcfd80954b48d88255ccb22a2
f37dd92ef4d0b7d07a4fbdcd9329d33b
f429ce3e75beaa66a28ff8210e744aea
f52154ae1366ae889d0783730040ea85
f52208fa1d6b8ff5a6577b22ea8f6082
f555ca2535197f0ff260af089270ee87
f59c6453d377b9c55555f60e9ec2c0f3
f5fd62546f1c60421b02f119a9954d3d
f60537aded8afbe9632997fe5c8fe0bc
f640392782b820749cbe00438d49d3dd
f6ab2b8adbb2eb8a5d2f067841b434ef
f70a54aacde816cb9e9db9e9263db4aa
f719734bebe97afe033f76deb2762ef5
f778c3fb1b2ccd5a4556f84442c6640c
f87cac481cc5440c70f8a3b150457bb3
f8b0e04506e57bfa2addade04e9a93d4
f8ecfee30bda0ad37f69f407f9a4c781
f9150f1e82c2aece498da6293f50319b
f9781e07f25215a815045941b2d27624
f9a2bc7d3838b886be8269f5aa7eb0b6
f9e71ef129d422ad638715f837c55ccd
fa6d2483f766f8431b6c0a8c78178d48
fa6ed1ba9789fa14b64195fd3cee06b3
fae53cdba53f27cd10d4d6710913a914
fb091b1444ce15ee6dfea7b0d07aef17
fb51ae46656da60410faca2cce4cb9a2
fb569c75daa6c2f4f16d6f7dc2944951
fc0f714d16b1a72fcc6719151e85a8f0
fc309fdb5903cce3a1e8a80412d51132
fc452ca6f8661736b882743ac33ea91a
fc506d776bbf7895ea4e0eef0058fc7d
fc72fd37515ae66e0e01538b200532c0
fc77c54c6e35c0e235bfef3a1ddfaae1
fcd88cc39fbc60868303ed4fd55cd0cb
fd96fd010babd89d75f2ebdf04ac7297
fd99e21da55ceda46ed654c0175f6a58
fda2191f9e6412915baf0fed9750a89c
fdb17e1818a9b0b8cbd0a82741a50244
fe2cbab386b534a10e71a5428fde891a
fe47d23a2f9099a0e14e19ef767af8d9
ff3f1c3486c852cc20daac4e97963e1d
ffc2c9969b6a3b27ff96b926e9a6c18a
```