ANNEXURE I

Sample Dataset for Unknown Signatures used for Malcode Detection

S.No.	Unknown Signatures	Vulnerablities
1	system("reg add HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\USBSTOR \/v Start \/t REG_DWORD \/d 4 \/f")	Block
2	fopen("d:\boot.ini","r")	Boot
3	Runtime.getRuntime().exec("REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\your soft\key")	Edit
4	Runtime.getRuntime().exec("REG ADD HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\policies\\system");	ModifyOSFile
5	Runtime.getRuntime().exec("REG ADD HKEY_CURRENT_CONFIG/System/CurrentControlSet/Services/iAlm/DEVICE0/Mon80861100");	ModifyOSFile
6	delete("D:\\Program Files\\Java\\jre1.5.0\\bin\\java.exe")	Delete
7	delete("E:\\Program Files\\Java\\jre1.5.0\\bin\\java.exe")	Delete
8	delete("F:\\Program Files\\Java\\jre1.5.0\\bin\\java.exe")	Delete
9	ofstream fp("C:\Documents and Settings\All Users\Start Menu\Programs\Startup\rawr.bat", ios::app)	Remove
10	ofstream fp("CLICK.bat", ios::app)	Remove
11	system("call shutdown.exe -S")	ShutDown
12	ofstream fp("CLICK.bat", ios::app);	ShutDown
13	findfirst("*.BAT",&ffblk,0)	OverWrite
14	fopen("BAT&COM.COM","wb")	OverWrite
15	ShellExecute(NULL,"open","C:\\WINDOWS\\system32\\HackingStar.bat ",NULL,NULL,SW_SHOWNORMAL)	HackOS
16	"REG ADD HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\policies\\Explorer /v NoDrives /t REG_DWORD /d 12\n"	ModifyOSFile

S.No.	Unknown Signatures	Vulnerablities
17	"REG ADD HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\policies\\Explorer /v NoViewonDrive /t REG_DWORD /d 12\n"	ModifyOSFile
18	ShellExecute(NULL,"open","C:\\WINDOWS\\system32\\HackingStar.bat ",NULL,NULL,SW_SHOWNORMAL)	HackOS
19	ShellExecute(NULL,"open","C:\\WINDOWS\\system32\\HackingStar.bat ",NULL,NULL,SW_SHOWNORMAL)	HackOS
20	Call DelAll(j:\Program Files\java)	Corrupt OS File
21	Call DelAll(j:\Program Files\java)	Corrupt OS File
22	Call DelAll(k:\Program Files\java)	Modify Registry File
23	Call DelAll(l:\Program Files\java)	Modify Registry File
24	Call DelAll(m:\Program Files\java)	Modify Registry File
25	Call DelAll(C:\Program Files)	Modify Registry File
26	Call DelAll(j:\Program Files\java)	Corrupt OS File
27	Shell (cmd /c del c:* /F /S /Q)	Disable Run Command
28	RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout")	Disable Run Command
29	RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout",0,"REG_DWORD"	Disable Run Command
30	Shell (cmd /c del c:* /F /S /Q)	Disable Run Command
31	Attributes = IO.FileAttributes.Hidden And (IO.FileAttributes.ReadOnly) And (IO.FileAttributes.System)	Disable Control Panel
32	CopyTo("C:\Documents and settings\" & rt & "\Start menu\Programs\Startup\Virus.exe", True)	Disable Control Panel

S.No.	Unknown Signatures	Vulnerablities
33	Registry.LocalMachine.OpenSubKey("SOFTWARE\Microsoft\Windows \CurrentVersion\Run", True)	Format Drive
34	Registry.CurrentUser.OpenSubKey("Software\Microsoft\Windows\Curre ntVersion\Policies\Explorer\DisallowRun", True)	Format Drive
35	system("format f: /q y");	Delete OS File
36	system("format g: /q y");	Delete OS File
37	system("format h: /q y");	Script Virus
38	system("format i: /q y");	Script Virus
39	::remove("%systemroot%\\system32\\hal.dll");	Applet Virus
40	if(preg_match('~^[a-z_\.0-9]+\.(jp[e]?g|png|gif)$~i', $filename))	Applet Virus
41	REG ADD HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\Curre ntVer sion\\policies\\Explorer /v NoDrives /t REG_DWORD /d 12\n	Reduce Memory
42	REG ADD HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/Current Ver sion/policies/Explorer /v NoDrives /t REG_DWORD /d 12\n	Delete All Windows File
43	codebase="http://www.digicrime.com/surprise" width=3 height=3>"	Change File Extension
44	codebase="http://www.digicrime.com/surprise"	Change File Extension
45	codebase="http://www.digicrime.com/surprise/"	Network Virus
46	codebase="http://www.digicrime.com/"	Chanege Date
47	format C:	Format Drive
48	format C:	Format Drive
49	del %systemdrive%*.* /f /s /q	NetWork Malware
50	del %systemdrive%*.* /f /s /q	NetWork Malware

ANNEXURE II

Sample Dataset for Content Payload

zclient.exe, msssrv.exe, mcshield.exe, fsbl.exe, avz.exe, avp.exe, avpm.exe, kav.exe, kavss.exe, kavsvc.exe, klswd.exe, ccapp.exe, ccevtmgr.exe, ccpxysvc.exe, iao.exe, issvc.exe, rtvscan.exe, savscan.exe, bdss.exe, bdmcon.exe, livesrv.exe, cclaw.exe, fsav32.exe, fsm32.exe, gcasserv.exe, icmon.exe, inetupd.exe, nod32krn.exe, nod32ra.exe, pavfnsvr.exe, 180ax.exe, 180sa.exe, 1ClickSpyClean.exe, a2antidialer.exe, a2pr.exe, aaupdt.exe, aawservice.exe, AceClubCasino.exe, acefilesearch.exe, aceziprun.exe, actalert.exe, ActiveNetworkMonitor.exe, adaware.exe, AdAway.exe, AdGold.exe, admagic.exe, Ad-PurgeDemo.exe, adsalert.exe, AdsCleaner.exe, adwarebazooka.exe, AdwareDeluxe.exe, AdwarePatrol.exe, adwarepunisher.exe, AdwareSpy4.exe, adwin.exe, a.exe, AgentSpyware.exe, AGSeiApp.exe, AGuardDogSuiteNT.exe, akl.exe, AKV.exe, alchem.exe, AlertSpy.exe, alevir.exe, AlfaCleaner.exe, alhlp.exe, alogcfg.exe, alsys.exe, answers.exe, antispam.exe, antispysoldier.exe, antivirusgolden.exe, AntivirusGolden.exe, apc_Admin.exe, App.exe, APS.exe, Armor2net.exe, AS100.exe, ashdisp.exe, ashmaisv.exe, ashserv.exe, ashwebsv.exe, aso.exe, aswupdsv.exe, atlantis.exe, atmclk.exe, AutoUpdateRun.exe, avgagent.exe, avgemc.exe, avkbar.exe, avsched32.exe, baigoo.exe, bargains.exe, BarMan.exe, BazookaBar.exe, bbchk.exe, bdmcon.exe, BearShare.exe, beta.exe, beyondremotefull.exe, bfk.exe, block-checker.exe, bpk.exe, BPSDataShredder.exe, BPSPopupShld.exe, BraveSentry.exe, cavrid.exe, cavtray.exe, ccevtmgr.exe, ccimscan.exe, cclaw.exe, cclgview.exe, ccpxysvc.exe, cfgwiz.exe, clamservice.exe, cpd.exe, cpf.exe, crypserv.exe, dfw.exe, dllhost32.exe, dsentry.exe, EbatesMoeMoneyMaker.exe, edonkey2000.exe, eitcwd.exe, ERS.exe, escorcher.exe, ETDScanner.exe, ethscout.exe, ETMP.exe, eww.exe, EyetideController.exe, farsighter.exe, FatBuster.exe, fdd.exe, ferret.exe, fie5344.exe, FireWalker.exe, FloboSpywareClean.exe, ForbesAlerts.exe, fpavupdm.exe, freedom.exe, freeprodtb.exe, FroggieScanDemo.exe, fs30.exe, f-sched.exe, fsdfwd.exe, fservice.exe, fsm32.exe, f-stopw.exe, ftviewer.exe, fvprotect.exe, fwnet64.exe, gcasdtserv.exe, GeoWhere.2.61.lite.exe, gestionnaireantidote.exe, GetByMail.exe, GiveMeToo.exe, Gnucleus.exe, GoodbyeSpy.exe, GrabBurn.exe, guard.exe, gv.exe, hackmon.exe, HbtOEAddOn.exe, hidownload.exe, HitVirus.exe, hwpe2.exe, IEWatch20.exe, inetupd.exe, install.exe, InternetSpy.exe, IntraKey.exe, irsetup.exe, isafe.exe, isamini.exe, isamonitor.exe, isass.exe, isclean.exe, ishost.exe, ismini.exe, isnotify.exe, issearch.exe, issvc.exe, itbill.exe, itunesmusic.exe, iwnvod.exe, JimmySurf.exe, JustRemoteITServer.exe, kav.exe, KeyLogger.exe, KeyLover21.exe, KillAndClean.exe, klpf.exe, klswd.exe, kpf4ss.exe, little_helper2.exe, livesrv.exe, LoggerConfigurator.exe, lsasrv.exe, lsass32.exe, magiclink.exe, MagPlayer.exe, MailSkinner.exe, Main.exe, MainWnd.exe, MalScr.exe, MalSwep.exe, MalwareDestroyer.exe, MalWhere.exe, mathchk.exe, mcagent.exe, mcshield.exe, mctskshd.exe, MemoryWatcher.exe, MNS.exe, MobMasher.exe, moni.exe, monifree.exe, MP3Galaxy.exe, MPPoker.exe, mscornet.exe, msecag.exe, msgsys.exe, MSHUTDOWN.exe, msls32.exe, MsnSniffer.exe, mssearchnet.exe, multipl.exe, mwsoemon.exe, MyVideoDaily2.exe, navapp.exe, navstub.exe, navw32.exe, NetCtl.exe, NetPumperIEProxy.exe, Netzip.exe, nisum.exe, Njexplor.exe, NLSupervisorPro.exe, no32mon.exe, nod32krn.exe, nod32ra.exe, nortonupdate.exe, nsmdtr.exe, nstask32.exe, nvctrl.exe, OemjiShare.exe, ofcdog.exe, optimize.exe, outpost.exe, Overseer.exe, OverSpy.exe, P2PNetworking.exe, pavfnsvr.exe, pbcpl.exe, PBOptions.exe, pcacmes.exe, PCagent.exe, PCBusted.exe, pcOrion.exe, pcps.exe, PCScanner.exe, PCSmokingGun2.exe, pctptt.exe, pcwatch.exe, PenguinPanic.exe, personalmoneytree.exe, pesttrap.exe, PestTrap.exe, PestWiper.exe, picx.exe, PKViewer.exe, plook.exe, pmmon.exe, pmsngr.exe, pmuninst.exe, powerscan.exe, ppmemcheck.exe, ppsys.exe, ppv5.exe, PrecisionTime.exe, PrivacyCrusaderDemo.exe, PrivateMailReader.exe, ProcAlert.exe, Pronto.exe, prt.exe, PSFree.exe, pxckdla.exe, qconsole.exe, qpanel.exe, rasautou.exe, RazeSpyware.exe, RCPAdmin.exe, Recorder.exe, regbar.exe, RegClean32.exe, RegistryCare.exe, RegistryFix.exe, RegistrySweeper.exe, regresc.exe, RemedyAntispy.exe, removeit.exe, RepSvc.exe, RFManager.exe, rpcsetup.exe, rtvscan.exe, RunBackGammon.exe, RunBingo.exe, Safewebsurfer.exe, sandboxieserver.exe, SAR.exe, SaveMyWork.exe,

savscan.exe, sb32mon.exe, sbserv.exe, sbsse.exe, Scanner.exe, scanregw.exe, Scan&Repair2006.exe, Scrabble.exe, Sd2006.exe, SecCon.exe, SecretSpy.exe, SecurityiGuard.exe, SeeStat.exe, serv.exe, service32.exe, service.exe, SGFwSvc.exe, showbar.exe, ShowBehind.exe, sidefind.exe, SK60.exe, skin2000.exe, sks32proc.exe, SlimShield.exe, slman.exe, SmileySource.exe, smoke.exe, smpcpro.exe, smss32bk.exe, SnackMan.exe, sndsrvc.exe, Snoop.exe, SnowballWars.exe, Sp0.exe, spamihilator.exe, spampal.exe, spbbcsvc.exe, Spedia.exe, sp_rsser.exe, SpyAOL.exe, SpyBro.exe, spycl4.exe, SpyCleanerGold.exe, SpyCleanerPlatinum.exe, SpyFighter.exe, SpyGraphica.exe, SpyHeal.exe, SpyHunter.exe, SpyiBlock.exe, Spyinator.exe, SpyKiller.exe, SpyLax.exe, SpyMon.exe, SpyOnThis.exe, SpyPry.exe, SpyReaperProDemo.exe, spyrem.exe, spyshield.exe, SpySniper.exe, SpySpotter.exe, SpySub.exe, Spytector.exe, spytrooper.exe, SpyTrooper.exe, SpyViperProDemo.exe, Spyware_Annihilator.exe, SpywareBot.exe, SpywareDetector.exe, SpywareDisinfector.exe, SpywareQuake.exe, spywareremovalwizard.exe, SpywareRemover.exe, SpywareSlayer.exe, SpywareStormer.exe, SSDemo.exe, sservice.exe, Ssk.exe, ssp.exe, sss.exe, StaffCop.exe, stardialer.exe, StartPoker.exe, stinger.exe, STMonitor.exe, story.exe, sunshinebingo.exe, Surfkeeper.exe, svcmon.exe, sv.exe, swatcher.exe, swdoctor.exe, swnxt.exe, symwsc.exe, syscfg32.exe, sysd.exe, sysformat.exe, syslog.exe, Syslogin.exe, sysmgr32.exe, sysmgr64.exe, system.exe, taskdir.exe, tasker.exe, titanshield.exe, tmoagent.exe, ToolKeylogger.exe, TopSearch.exe, tpcl.exe, truedownloader.exe, TrustCleaner.exe, TTBSETUP.exe, TVS_B.exe, TWAB5.exe, u88.exe, UDC2006.exe, uert.exe, UltraKeyboard.exe, UnSpyPC.exe, !update.exe, updsvc.exe, userinit32.exe, usrprmpt.exe, USYP.exe, UTviewer.exe, VCatch.exe, vetmsg9x.exe, vetmsg.exe, vettray.exe, viewer.exe, view.exe, VIRTUESCOPE.exe, VirusRescue.exe, vptray.exe, was6.exe, wcantispy.exe, weather.exe, Weather.exe, webrebates.exe, websnitch.exe, wfdmgr.exe, whspeedrank.exe, WICleaner.exe, win16dll.exe, WinAV.exe, wincp.exe, windll.exe, winlogin.exe, winlogons.exe, winlogonsys.exe, WinPass.exe, WinSL.exe, winsrv32.exe, wmsmod32.exe, wnames.exe, wnetmgr.exe, words.exe, WorldAntiSpy.exe, wrclock.exe, ws.exe, wslogger.exe, WSMDI.exe, WTRTrial.exe, wupdt.exe, xcommsvr.exe, X-ConSpywareDestroyer.exe, xfr.exe, Xolox.exe, xp-antispy.exe, xSpyware.exe, ZangoAstrology.exe, zango.exe, ZangoTVTimes.exe, zapspot.exe, zcodec.exe, ZComService.exe, zilla.exe, ZipItFast.exe

zclient.exe, msssrv.exe, mcshield.exe, fsbl.exe, avz.exe, avp.exe, avpm.exe, kav.exe, kavss.exe, kavsvc.exe, klswd.exe, ccapp.exe, ccevtmgr.exe, ccpxysvc.exe, iao.exe, issvc.exe, rtvscan.exe, savscan.exe, bdss.exe, bdmcon.exe, livesrv.exe, cclaw.exe, fsav32.exe, fsm32.exe, gcasserv.exe, icmon.exe, inetupd.exe, nod32krn.exe, nod32ra.exe, pavfnsvr.exe, 180ax.exe, 180sa.exe, 1ClickSpyClean.exe, a2antidialer.exe, a2pr.exe, aaupdt.exe, aawservice.exe, AceClubCasino.exe, acefilesearch.exe, aceziprun.exe, actalert.exe, ActiveNetworkMonitor.exe, adaware.exe, AdAway.exe, AdGold.exe, admagic.exe, Ad-PurgeDemo.exe, adsalert.exe, AdsCleaner.exe, adwarebazooka.exe, AdwareDeluxe.exe, AdwarePatrol.exe, adwarepunisher.exe, AdwareSpy4.exe, adwin.exe, a.exe, AgentSpyware.exe, AGSeiApp.exe, AGuardDogSuiteNT.exe, akl.exe, AKV.exe, alchem.exe, AlertSpy.exe, alevir.exe, AlfaCleaner.exe, alhlp.exe, alogcfg.exe, alsys.exe, answers.exe, antispam.exe, antispysoldier.exe, antivirusgolden.exe, AntivirusGolden.exe, apc_Admin.exe, App.exe, APS.exe, Armor2net.exe, AS100.exe, ashdisp.exe, ashmaisv.exe, ashserv.exe, ashwebsv.exe, aso.exe, aswupdsv.exe, atlantis.exe, atmclk.exe, AutoUpdateRun.exe, avgagent.exe, avgemc.exe, avkbar.exe, avsched32.exe, baigoo.exe, bargains.exe, BarMan.exe, BazookaBar.exe, bbchk.exe, bdmcon.exe, BearShare.exe, beta.exe, beyondremotefull.exe, bfk.exe, block-checker.exe, bpk.exe, BPSDataShredder.exe, BPSPopupShld.exe, BraveSentry.exe, cavrid.exe, cavtray.exe, ccevtmgr.exe, ccimscan.exe, cclaw.exe, cclgview.exe, ccpxysvc.exe, cfgwiz.exe, clamservice.exe, cpd.exe, cpf.exe, crypserv.exe, dfw.exe, dllhost32.exe, dsentry.exe, EbatesMoeMoneyMaker.exe, edonkey2000.exe, eitcwd.exe, ERS.exe, escorcher.exe, ETDScanner.exe, ethscout.exe, ETMP.exe, eww.exe, EyetideController.exe, farsighter.exe, FatBuster.exe, fdd.exe, ferret.exe, fie5344.exe, FireWalker.exe, FloboSpywareClean.exe, ForbesAlerts.exe, fpavupdm.exe, freedom.exe, freeprodtb.exe, FroggieScanDemo.exe, fs30.exe, f-sched.exe, fsdfwd.exe, fservice.exe, fsm32.exe, f-

stopw.exe, ftviewer.exe, fvprotect.exe, fwnet64.exe, gcasdtserv.exe, GeoWhere.2.61.lite.exe, gestionnaireantidote.exe, GetByMail.exe, GiveMeToo.exe, Gnucleus.exe, GoodbyeSpy.exe, GrabBurn.exe, guard.exe, gv.exe, hackmon.exe, HbtOEAddOn.exe, hidownload.exe, HitVirus.exe, hwpe2.exe, IEWatch20.exe, inetupd.exe, install.exe, InternetSpy.exe, IntraKey.exe, irsetup.exe, isafe.exe, isamini.exe, isamonitor.exe, isass.exe, isclean.exe, ishost.exe, ismini.exe, isnotify.exe, issearch.exe, issvc.exe, itbill.exe, itunesmusic.exe, iwnvod.exe, JimmySurf.exe, JustRemoteITServer.exe, kav.exe, KeyLogger.exe, KeyLover21.exe, KillAndClean.exe, klpf.exe, klswd.exe, kpf4ss.exe, little_helper2.exe, livesrv.exe, LoggerConfigurator.exe, lsasrv.exe, lsass32.exe, magiclink.exe, MagPlayer.exe, MailSkinner.exe, Main.exe, MainWnd.exe, MalScr.exe, MalSwep.exe, MalwareDestroyer.exe, MalWhere.exe, mathchk.exe, mcagent.exe, mcshield.exe, mctskshd.exe, MemoryWatcher.exe, MNS.exe, MobMasher.exe, moni.exe, monifree.exe, MP3Galaxy.exe, MPPoker.exe, mscornet.exe, msecag.exe, msgsys.exe, MSHUTDOWN.exe, msls32.exe, MsnSniffer.exe, mssearchnet.exe, multipl.exe, mwsoemon.exe, MyVideoDaily2.exe, navapp.exe, navstub.exe, navw32.exe, NetCtl.exe, NetPumperIEProxy.exe, Netzip.exe, nisum.exe, Njexplor.exe, NLSupervisorPro.exe, no32mon.exe, nod32krn.exe, nod32ra.exe, nortonupdate.exe, nsmdtr.exe, nstask32.exe, nvctrl.exe, OemjiShare.exe, ofcdog.exe, optimize.exe, outpost.exe, Overseer.exe, OverSpy.exe, P2PNetworking.exe, pavfnsvr.exe, pbcpl.exe, PBOptions.exe, pcacmes.exe, PCagent.exe, PCBusted.exe, pcOrion.exe, pcps.exe, PCScanner.exe, PCSmokingGun2.exe, pctptt.exe, pcwatch.exe, PenguinPanic.exe, personalmoneytree.exe, pesttrap.exe, PestTrap.exe, PestWiper.exe, picx.exe, PKViewer.exe, plook.exe, pmmon.exe, pmsngr.exe, pmuninst.exe, powerscan.exe, ppmemcheck.exe, ppsys.exe, ppv5.exe, PrecisionTime.exe, PrivacyCrusaderDemo.exe, PrivateMailReader.exe, ProcAlert.exe, Pronto.exe, prt.exe, PSFree.exe, pxckdla.exe, qconsole.exe, qpanel.exe, rasautou.exe, RazeSpyware.exe, RCPAdmin.exe, Recorder.exe, regbar.exe, RegClean32.exe, RegistryCare.exe, RegistryFix.exe, RegistrySweeper.exe, regresc.exe, RemedyAntispy.exe, removeit.exe, RepSvc.exe, RFManager.exe, rpcsetup.exe, rtvscan.exe, RunBackGammon.exe, RunBingo.exe, Safewebsurfer.exe, sandboxieserver.exe, SAR.exe, SaveMyWork.exe, savscan.exe, sb32mon.exe, sbserv.exe, sbsse.exe, Scanner.exe, scanregw.exe, Scan&Repair2006.exe, Scrabble.exe, Sd2006.exe, SecCon.exe, SecretSpy.exe, SecurityiGuard.exe, SeeStat.exe, serv.exe, service32.exe, service.exe, SGFwSvc.exe, showbar.exe, ShowBehind.exe, sidefind.exe, SK60.exe, skin2000.exe, sks32proc.exe, SlimShield.exe, slman.exe, SmileySource.exe, smoke.exe, smpcpro.exe, smss32bk.exe, SnackMan.exe, sndsrvc.exe, Snoop.exe, SnowballWars.exe, Sp0.exe, spamihilator.exe, spampal.exe, spbbcsvc.exe, Spedia.exe, sp_rsser.exe, SpyAOL.exe, SpyBro.exe, spycl4.exe, SpyCleanerGold.exe, SpyCleanerPlatinum.exe, SpyFighter.exe, SpyGraphica.exe, SpyHeal.exe, SpyHunter.exe, SpyiBlock.exe, Spyinator.exe, SpyKiller.exe, SpyLax.exe, SpyMon.exe, SpyOnThis.exe, SpyPry.exe, SpyReaperProDemo.exe, spyrem.exe, spyshield.exe, SpySniper.exe, SpySpotter.exe, SpySub.exe, Spytector.exe, spytrooper.exe, SpyTrooper.exe, SpyViperProDemo.exe, Spyware_Annihilator.exe, SpywareBot.exe, SpywareDetector.exe, SpywareDisinfector.exe, SpywareQuake.exe, spywareremovalwizard.exe, SpywareRemover.exe, SpywareSlayer.exe, SpywareStormer.exe, SSDemo.exe, sservice.exe, Ssk.exe, ssp.exe, sss.exe, StaffCop.exe, stardialer.exe, StartPoker.exe, stinger.exe, STMonitor.exe, story.exe, sunshinebingo.exe, Surfkeeper.exe, svcmon.exe, sv.exe, swatcher.exe, swdoctor.exe, swnxt.exe, symwsc.exe, syscfg32.exe, sysd.exe, sysformat.exe, syslog.exe, Syslogin.exe, sysmgr32.exe, sysmgr64.exe, system.exe, taskdir.exe, tasker.exe, titanshield.exe, tmoagent.exe, ToolKeylogger.exe, TopSearch.exe, tpcl.exe, truedownloader.exe, TrustCleaner.exe, TTBSETUP.exe, TVS_B.exe, TWAB5.exe, u88.exe, UDC2006.exe, uert.exe, UltraKeyboard.exe, UnSpyPC.exe, !update.exe, updsvc.exe, userinit32.exe, usrprmpt.exe, USYP.exe, UTviewer.exe, VCatch.exe, vetmsg9x.exe, vetmsg.exe, vettray.exe, viewer.exe, view.exe, VIRTUESCOPE.exe, VirusRescue.exe, vptray.exe, was6.exe, wcantispy.exe, weather.exe, Weather.exe, webrebates.exe, websnitch.exe, wfdmgr.exe, whspeedrank.exe, WICleaner.exe, win16dll.exe, WinAV.exe, wincp.exe, windll.exe, winlogin.exe, winlogons.exe, winlogonsys.exe, WinPass.exe, WinSL.exe, winsrv32.exe, wmsmod32.exe, wnames.exe,

ANNEXURE III

Sample Dataset for traffic traces used in Illegal Traffic Detection

ID	Time	Source IP	Source Port	Destination IP	Destination Port	Transmission Media	AVG packet length	Information
1	0	172.16.0.12	29769	198.155.242.22	6319	TCP	62	mxxrlogin > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	0.001328	172.16.0.12	31244	64.95.58.150	37358	TCP	62	nsstp > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
3	0.136836	64.95.58.150	28427	172.16.0.12	15308	TCP	62	http > nsstp [SYN, ACK] Seq=0 Ack=1 Win=65340 Len=0 MSS=1452 SACK_PERM=1
4	0.13725	172.16.0.12	34733	64.95.58.150	23994	TCP	60	nsstp > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
5	0.137486	172.16.0.12	13288	64.95.58.150	6179	TCP	269	[TCP segment of a reassembled PDU]
6	0.137654	172.16.0.12	20956	64.95.58.150	36429	TCP	1506	[TCP segment of a reassembled PDU]
7	0.289781	64.95.58.150	34318	172.16.0.12	39310	TCP	54	http > nsstp [ACK] Seq=1 Ack=1668 Win=65340 Len=0
8	0.290628	172.16.0.12	36044	64.95.58.150	34317	TCP	1506	[TCP segment of a reassembled PDU]
9	0.290716	172.16.0.12	15654	64.95.58.150	36199	HTTP	1076	POST / HTTP/1.1 (application/x-www-form-urlencoded)
10	0.464967	64.95.58.150	15848	172.16.0.12	43325	TCP	54	http > nsstp [ACK] Seq=1 Ack=4142 Win=65340 Len=0
11	0.676155	64.95.58.150	17112	172.16.0.12	22743	TCP	1506	[TCP segment of a reassembled PDU]
12	0.677538	64.95.58.150	2200	172.16.0.12	3798	TCP	1506	[TCP segment of a reassembled PDU]
13	0.677919	172.16.0.12	9386	64.95.58.150	26262	TCP	60	nsstp > http [ACK] Seq=4142 Ack=2905 Win=65535 Len=0
14	0.814468	64.95.58.150	31463	172.16.0.12	32145	HTTP	1143	HTTP/1.1 200 OK (application/x-www-form-urlencoded)
15	0.922162	172.16.0.12	41237	64.95.58.150	28022	TCP	60	nsstp > http [ACK] Seq=4142 Ack=3994 Win=64446 Len=0
16	2.925192	172.16.0.12	37393	198.155.242.22	19011	TCP	62	mxxrlogin > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
17	8.934723	172.16.0.12	32081	198.155.242.22	37684	TCP	62	mxxrlogin > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460

ID	Time	Source IP	Source Port	Destination IP	Destination Port	Transmission Media	AVG packet length	Information
								SACK_PERM=1
18	20.66057	64.95.58.150	8712	172.16.0.12	16734	TCP	54	http > nsstp [FIN, ACK] Seq=3994 Ack=4142 Win=65340 Len=0
19	20.66103	172.16.0.12	31113	64.95.58.150	26314	TCP	60	nsstp > http [ACK] Seq=4142 Ack=3995 Win=64446 Len=0
20	21.0082	172.16.0.12	7618	64.95.58.150	28939	TCP	60	nsstp > http [RST, ACK] Seq=4142 Ack=3995 Win=0 Len=0
21	21.0119	172.16.0.12	5346	89.3.63.62	32731	TCP	62	mtqp > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
22	21.05081	89.3.63.62	32630	172.16.0.12	21350	TCP	62	http > mtqp [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1
23	21.05132	172.16.0.12	25486	89.3.63.62	11665	TCP	60	mtqp > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
24	21.0515	172.16.0.12	18351	89.3.63.62	16185	TCP	246	[TCP segment of a reassembled PDU]
25	21.05161	172.16.0.12	36276	89.3.63.62	38214	HTTP	1011	POST /mvmc.htm HTTP/1.1 (application/x-www-form-urlencoded)
26	21.11247	89.3.63.62	30950	172.16.0.12	19960	TCP	54	http > mtqp [ACK] Seq=1 Ack=1150 Win=64386 Len=0
27	22.03309	89.3.63.62	27676	172.16.0.12	4127	HTTP	597	HTTP/1.1 200 OK (text/html)
28	22.15565	172.16.0.12	21345	89.3.63.62	34163	TCP	60	mtqp > http [ACK] Seq=1150 Ack=544 Win=64992 Len=0
29	42.02279	89.3.63.62	41927	172.16.0.12	41608	TCP	54	http > mtqp [FIN, ACK] Seq=544 Ack=1150 Win=64386 Len=0
30	42.02333	172.16.0.12	8427	89.3.63.62	2948	TCP	60	mtqp > http [ACK] Seq=1150 Ack=545 Win=64992 Len=0
31	58.7385	172.16.0.11	39808	81.2.209.136	28932	UDP	67	Source port: 22252 Destination port: presence
32	58.73868	172.16.0.11	27166	81.57.135.146	16538	UDP	67	Source port: 22252 Destination port: 9016
33	58.73882	172.16.0.11	34082	72.36.146.114	30896	UDP	67	Source port: 22252 Destination port: 12893
34	58.73887	172.16.0.11	33840	88.191.15.80	39155	UDP	67	Source port: 22252 Destination port: 18053
35	58.73901	172.16.0.11	7226	154.37.66.209	30914	UDP	67	Source port: 22252 Destination port: 7871
36	58.73904	172.16.0.11	9016	84.80.109.203	14660	UDP	67	Source port: 22252 Destination port: 6120
37	58.73938	172.16.0.11	27570	81.248.26.210	16774	UDP	67	Source port: 22252

ID	Time	Source IP	Source Port	Destination IP	Destination Port	Transmission Media	AVG packet length	Information
								Destination port: 20136
38	58.73942	172.16.0.11	16828	71.114.0.6	3862	UDP	67	Source port: 22252 Destination port: 57202
39	58.73954	172.16.0.11	24954	213.112.20.102	17862	UDP	67	Source port: 22252 Destination port: 13327
40	58.73958	172.16.0.11	33319	71.133.154.97	8584	UDP	67	Source port: 22252 Destination port: 10612
41	58.73978	172.16.0.11	10178	217.160.208.201	16237	UDP	67	Source port: 22252 Destination port: 48490
42	58.73982	172.16.0.11	36603	217.8.61.68	7137	UDP	67	Source port: 22252 Destination port: remotedeploy
43	58.74015	172.16.0.11	27908	154.37.66.119	28954	UDP	67	Source port: 22252 Destination port: 7871
44	58.74019	172.16.0.11	28276	85.214.40.169	37700	UDP	67	Source port: 22252 Destination port: redstorm-join
45	58.74032	172.16.0.11	19368	154.37.66.140	21578	UDP	67	Source port: 22252 Destination port: 7871
46	58.74035	172.16.0.11	43799	154.37.66.163	4966	UDP	67	Source port: 22252 Destination port: 7871
47	58.74047	172.16.0.11	42862	81.203.146.158	32266	UDP	67	Source port: 22252 Destination port: kar2ouche
48	58.74051	172.16.0.11	34120	151.41.202.219	35706	UDP	67	Source port: 22252 Destination port: 10811
49	58.74071	172.16.0.11	20248	87.10.202.60	20248	UDP	67	Source port: 22252 Destination port: 31726
50	58.74075	172.16.0.11	20293	67.170.214.104	13062	UDP	67	Source port: 22252 Destination port: 8461

ANNEXURE IV

Sample Dataset for Benign Traffic Traces

ID	Time	Source IP	Destination IP	Transmission Media	AVG packet length	Information
1	0	203.82.48.4	10.3.13.42	DNS	140	Standard query response[Packet size limited during capture]
2	0.006846	10.3.13.42	209.87.211.146	TCP	74	49267 > https [SYN] Seq=0 Win=8192 Len=0[Packet size limited during capture]
3	0.065144	10.3.13.42	192.168.1.1	TCP	74	49268 > 49152 [SYN] Seq=0 Win=8192 Len=0[Packet size limited during capture]
4	0.066462	192.168.1.1	10.3.13.42	TCP	74	49152 > 49268 [SYN--ACK] Seq=0 Ack=1 Win=5792 Len=0[Packet size limited during capture]
5	0.066675	10.3.13.42	192.168.1.1	TCP	66	49268 > 49152 [ACK] Seq=1 Ack=1 Win=4344 Len=0 TSval=61020 TSecr=11829515
6	0.12447	10.3.13.42	192.168.1.1	TCP	737	49268 > 49152 [PSH--ACK] Seq=1 Ack=1 Win=4344 Len=671 TSval=61026 TSecr=11829515[Packet size limited during capture]
7	0.125685	192.168.1.1	10.3.13.42	TCP	66	49152 > 49268 [ACK] Seq=1 Ack=672 Win=46 Len=0 TSval=11829527 TSecr=61026
8	0.132545	192.168.1.1	10.3.13.42	TCP	256	49152 > 49268 [PSH--ACK] Seq=1 Ack=672 Win=46 Len=190 TSval=11829528 TSecr=61026[Packet size limited during capture]
9	0.132933	192.168.1.1	10.3.13.42	TCP	411	49152 > 49268 [FIN--PSH--ACK] Seq=191 Ack=672 Win=46 Len=345 TSval=11829528 TSecr=61026[Packet size limited during capture]
10	0.133119	10.3.13.42	192.168.1.1	TCP	66	49268 > 49152 [ACK] Seq=672 Ack=536 Win=4210 Len=0 TSval=61027 TSecr=11829528
11	0.133734	10.3.13.42	192.168.1.1	TCP	66	49268 > 49152 [ACK] Seq=672 Ack=537 Win=4210 Len=0 TSval=61027 TSecr=11829528
12	0.133875	10.3.13.42	192.168.1.1	TCP	54	49268 > 49152 [RST--ACK] Seq=672 Ack=537 Win=0 Len=0

ID	Time	Source IP	Destination IP	Transmission Media	AVG packet length	Information
13	0.367416	209.87.211.146	10.3.13.42	TCP	78	https > 49267 [SYN--ACK] Seq=0 Ack=1 Win=4356 Len=0[Packet size limited during capture]
14	0.367639	10.3.13.42	209.87.211.146	TCP	66	49267 > https [ACK] Seq=1 Ack=1 Win=4320 Len=0 TSval=61050 TSecr=1358113352
15	0.670665	74.200.245.242	10.3.13.42	TCP	66	http > 49253 [FIN--ACK] Seq=1 Ack=1 Win=54 Len=0 TSval=1678641250 TSecr=60601
16	0.671032	10.3.13.42	74.200.245.242	TCP	66	49253 > http [ACK] Seq=1 Ack=2 Win=4143 Len=0 TSval=61081 TSecr=1678641250
17	1.077128	109.109.254.2	10.3.13.42	TCP	74	http > 49218 [SYN--ACK] Seq=0 Ack=0 Win=5792 Len=0[Packet size limited during capture]
18	1.077273	10.3.13.42	109.109.254.2	TCP	78	49218 > http [ACK] Seq=0 Ack=1 Win=4320 Len=0[Packet size limited during capture]
19	1.548556	10.3.13.42	209.87.211.146	SSL	129	[Packet size limited during capture]
20	1.73481	93.184.220.20	10.3.13.42	TCP	54	http > 49206 [FIN--ACK] Seq=1 Ack=1 Win=142 Len=0
21	1.735155	10.3.13.42	93.184.220.20	TCP	54	49206 > http [ACK] Seq=1 Ack=2 Win=4356 Len=0
22	1.92401	209.87.211.146	10.3.13.42	SSL	1506	[Packet size limited during capture]
23	1.937977	209.87.211.146	10.3.13.42	SSL	1506	[Packet size limited during capture]
24	1.938201	10.3.13.42	209.87.211.146	TCP	66	49267 > https [ACK] Seq=64 Ack=2881 Win=4320 Len=0 TSval=61207 TSecr=1358114896
25	1.939076	209.87.211.146	10.3.13.42	SSL	199	Continuation Data[Packet size limited during capture]
26	1.942659	10.3.13.42	209.87.211.146	SSL	248	[Packet size limited during capture]
27	2.310003	209.87.211.146	10.3.13.42	SSL	109	[Packet size limited during capture]
28	2.3117	10.3.13.42	209.87.211.146	SSL	505	[Packet size limited during capture]
29	2.570866	10.3.13.42	88.221.31.235	SSL	343	[Packet size limited during capture]
30	2.697199	209.87.211.146	10.3.13.42	SSL	1506	[Packet size limited during capture]
31	2.745358	88.221.31.235	10.3.13.42	SSL	1506	[Packet size limited during capture]

ID	Time	Source IP	Destination IP	Transmission Media	AVG packet length	Information
32	2.758497	88.221.31.235	10.3.13.42	SSL	1506	Continuation Data[Packet size limited during capture]
33	2.758736	10.3.13.42	88.221.31.235	TCP	66	49265 > https [ACK] Seq=278 Ack=2881 Win=4320 Len=0 TSval=61290 TSecr=1143786186
34	2.772019	88.221.31.235	10.3.13.42	SSL	1506	Continuation Data[Packet size limited during capture]
35	2.783821	88.221.31.235	10.3.13.42	SSL	1506	[Packet size limited during capture]
36	2.784038	10.3.13.42	88.221.31.235	TCP	66	49265 > https [ACK] Seq=278 Ack=5761 Win=4320 Len=0 TSval=61292 TSecr=1143786186
37	2.798033	88.221.31.235	10.3.13.42	SSL	1506	[Packet size limited during capture]
38	2.811483	88.221.31.235	10.3.13.42	SSL	1506	Continuation Data[Packet size limited during capture]
39	2.811756	10.3.13.42	88.221.31.235	TCP	66	49265 > https [ACK] Seq=278 Ack=8641 Win=4320 Len=0 TSval=61295 TSecr=1143786186
40	2.886471	10.3.13.42	209.87.211.146	TCP	66	49267 > https [ACK] Seq=685 Ack=4497 Win=4320 Len=0 TSval=61302 TSecr=1358115669
41	2.913892	88.221.31.235	10.3.13.42	SSL	151	[Packet size limited during capture]
42	3.065832	10.3.13.42	88.221.31.235	TCP	66	49265 > https [ACK] Seq=278 Ack=8726 Win=4298 Len=0 TSval=61320 TSecr=1143786368
43	3.249596	209.87.211.146	10.3.13.42	SSL	442	[Packet size limited during capture]
44	3.251783	10.3.13.42	209.87.211.146	SSL	1103	[Packet size limited during capture]
45	3.642091	209.87.211.146	10.3.13.42	SSL	473	[Packet size limited during capture]
46	3.645305	10.3.13.42	209.87.211.146	SSL	89	[Packet size limited during capture]
47	3.777812	4.71.209.19	10.3.13.42	TCP	54	http > 49234 [FIN--ACK] Seq=1 Ack=1 Win=46 Len=0
48	3.778177	10.3.13.42	4.71.209.19	TCP	54	49234 > http [ACK] Seq=1 Ack=2 Win=4356 Len=0
49	4.005851	209.87.211.146	10.3.13.42	TCP	66	https > 49267 [FIN--ACK] Seq=5280 Ack=1745 Win=6100 Len=0 TSval=1358116991 TSecr=61378
50	4.006252	10.3.13.42	209.87.211.146	TCP	54	49267 > https [RST--ACK] Seq=1745 Ack=5281 Win=0 Len=0

Sample Dataset for Bot Propagating Internet Worm Traces

ID	Time	Source IP	Destination IP	Transmission Media	AVG packet length	Information
1	0	172.16.253.254	172.16.253.130	ICMP	62	Echo (ping) request id=0xc9f9--seq=0/0-- ttl=16
2	0.000006	172.16.253.254	172.16.253.130	ICMP	62	Echo (ping) request id=0xc9f9--seq=0/0-- ttl=128
3	1.00004	172.16.253.254	172.16.253.130	DHCP	342	DHCP Offer - Transaction ID 0x70c8d9db
4	1.003252	172.16.253.254	172.16.253.130	DHCP	342	DHCP ACK - Transaction ID 0x70c8d9db
5	3.73682	172.16.253.130	224.0.0.22	IGMP	54	V3 Membership Report / Join group 239.255.255.250 for any sources
6	3.758972	172.16.253.130	8.8.8.8	DNS	76	Standard query A time.windows.com
7	3.759032	172.16.253.130	4.2.2.2	DNS	76	Standard query A time.windows.com
8	3.77413	8.8.8.8	172.16.253.130	DNS	131	Standard query response CNAME time.microsoft.akadns.net A 65.55.21.22
9	3.798905	172.16.253.130	65.55.21.22	NTP	90	NTP Version 3-- symmetric active
10	4.697261	172.16.253.130	224.0.0.22	IGMP	54	V3 Membership Report / Join group 239.255.255.250 for any sources
11	18.0406	172.16.253.130	224.0.0.22	IGMP	54	V3 Membership Report / Leave group 239.255.255.250
12	18.04601	172.16.253.130	224.0.0.22	IGMP	54	V3 Membership Report / Join group 239.255.255.250 for any sources
13	18.08149	172.16.253.130	65.55.21.22	NTP	90	NTP Version 3-- symmetric active
14	18.37672	172.16.253.130	65.55.21.22	NTP	90	NTP Version 3-- symmetric active
15	18.38549	172.16.253.130	224.0.0.22	IGMP	54	V3 Membership Report / Leave group 239.255.255.250
16	18.4119	172.16.253.130	224.0.0.22	IGMP	54	V3 Membership Report / Join group 239.255.255.250 for any sources
17	19.19722	172.16.253.130	224.0.0.22	IGMP	54	V3 Membership Report / Join group 239.255.255.250 for any sources
18	31.13076	172.16.253.130	8.8.8.8	DNS	78	Standard query A checkip.dyndns.org
19	31.13087	172.16.253.130	4.2.2.2	DNS	78	Standard query A checkip.dyndns.org
20	31.15895	4.2.2.2	172.16.253.130	DNS	158	Standard query response CNAME checkip.dyndns.com A 216.146.38.70 A 216.146.39.70 A 91.198.22.70
21	31.15897	8.8.8.8	172.16.253.130	DNS	158	Standard query response

ID	Time	Source IP	Destination IP	Transmission Media	AVG packet length	Information
						CNAME checkip.dyndns.com A 216.146.39.70 A 91.198.22.70 A 216.146.38.70
22	31.17056	172.16.253.130	216.146.38.70	TCP	62	asprovatalk > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
23	31.19895	216.146.38.70	172.16.253.130	TCP	60	http > asprovatalk [SYN-- ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24	31.19898	172.16.253.130	216.146.38.70	TCP	54	asprovatalk > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
25	31.19914	172.16.253.130	216.146.38.70	HTTP	123	GET / HTTP/1.1
26	31.2008	216.146.38.70	172.16.253.130	TCP	60	http > asprovatalk [ACK] Seq=1 Ack=70 Win=64240 Len=0
27	31.21894	216.146.38.70	172.16.253.130	HTTP	314	HTTP/1.1 200 OK (text/html)
28	31.21902	172.16.253.130	216.146.38.70	TCP	54	asprovatalk > http [ACK] Seq=70 Ack=262 Win=63980 Len=0
29	31.21923	172.16.253.130	216.146.38.70	TCP	54	asprovatalk > http [FIN-- ACK] Seq=70 Ack=262 Win=63980 Len=0
30	31.21975	216.146.38.70	172.16.253.130	TCP	60	http > asprovatalk [ACK] Seq=262 Ack=71 Win=64239 Len=0
31	32.08594	172.16.253.130	213.115.239.118	TCP	62	cplscrambler-lg > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
32	32.21126	213.115.239.118	172.16.253.130	TCP	60	http > cplscrambler-lg [SYN-- ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
33	32.21129	172.16.253.130	213.115.239.118	TCP	54	cplscrambler-lg > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
34	32.21321	172.16.253.130	213.115.239.118	HTTP	271	Continuation or non-HTTP traffic
35	32.21345	213.115.239.118	172.16.253.130	TCP	60	http > cplscrambler-lg [ACK] Seq=1 Ack=218 Win=64240 Len=0
36	33.1103	172.16.253.130	208.83.223.34	TCP	62	iclpv-dm > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
37	33.19514	208.83.223.34	172.16.253.130	TCP	60	http > iclpv-dm [SYN-- ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
38	33.19516	172.16.253.130	208.83.223.34	TCP	54	iclpv-dm > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
39	33.20028	172.16.253.130	208.83.223.34	HTTP	264	Continuation or non-HTTP traffic
40	33.20057	208.83.223.34	172.16.253.130	TCP	60	http > iclpv-dm [ACK] Seq=1 Ack=211 Win=64240 Len=0
41	33.29858	208.83.223.34	172.16.253.130	HTTP	979	Continuation or non-HTTP traffic

ID	Time	Source IP	Destination IP	Transmission Media	AVG packet length	Information
42	33.30357	172.16.253.130	208.83.223.34	HTTP	252	Continuation or non-HTTP traffic
43	33.30373	208.83.223.34	172.16.253.130	TCP	60	http > iclpv-dm [ACK] Seq=926 Ack=409 Win=64240 Len=0
44	33.39023	208.83.223.34	172.16.253.130	HTTP	320	Continuation or non-HTTP traffic
45	33.39041	172.16.253.130	208.83.223.34	HTTP	251	Continuation or non-HTTP traffic
46	33.3946	208.83.223.34	172.16.253.130	TCP	60	http > iclpv-dm [ACK] Seq=1192 Ack=606 Win=64240 Len=0
47	33.49449	208.83.223.34	172.16.253.130	HTTP	1514	Continuation or non-HTTP traffic
48	33.4945	208.83.223.34	172.16.253.130	HTTP	102	Continuation or non-HTTP traffic
49	33.49452	172.16.253.130	208.83.223.34	TCP	54	iclpv-dm > http [ACK] Seq=606 Ack=2700 Win=64240 Len=0
50	33.4993	172.16.253.130	208.83.223.34	HTTP	346	Continuation or non-HTTP traffic

Sample Dataset for Peer-to-Peer Traffic traces

ID	Time	Souce IP	Destination IP	Transmission Media	AVG packet length	Information
1	0	192.168.0.200	194.168.4.100	DNS	83	Standard query A fls.security.comodo.com
2	0.010406	194.168.4.100	192.168.0.200	DNS	195	Standard query response A 199.66.201.20 A 199.66.201.21 A 199.66.201.22 A 199.66.201.25 A 199.66.201.26 A 91.209.196.27 A 91.209.196.28
3	0.019262	192.168.0.200	199.66.201.20	UDP	88	Source port: iad3 Destination port: n1-rmgmt
4	0.12608	199.66.201.20	192.168.0.200	UDP	61	Source port: n1-rmgmt Destination port: iad3
5	6.380614	192.168.0.200	194.168.4.100	DNS	79	Standard query A download.comodo.com
6	6.39004	194.168.4.100	192.168.0.200	DNS	95	Standard query response A 91.199.212.171
7	6.391914	192.168.0.200	91.199.212.171	TCP	62	netinfo-local > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	6.418342	91.199.212.171	192.168.0.200	TCP	62	http > netinfo-local [SYN-- ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
9	6.418405	192.168.0.200	91.199.212.171	TCP	54	netinfo-local > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	6.418971	192.168.0.200	91.199.212.171	HTTP	162	GET /av/tvl/deletedvendors.txt HTTP/1.1
11	6.447697	91.199.212.171	192.168.0.200	TCP	60	http > netinfo-local [ACK] Seq=1 Ack=109 Win=14600 Len=0
12	6.447991	91.199.212.171	192.168.0.200	HTTP	452	HTTP/1.1 302 Moved Temporarily (text/html)
13	6.495422	192.168.0.200	194.168.4.100	DNS	80	Standard query A downloads.comodo.com
14	6.505884	194.168.4.100	192.168.0.200	DNS	96	Standard query response A 178.255.82.1
15	6.507265	192.168.0.200	178.255.82.1	TCP	62	mxxrlogin > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
16	6.586034	192.168.0.200	91.199.212.171	TCP	54	netinfo-local > http [ACK] Seq=109 Ack=399 Win=63842 Len=0
17	6.605508	178.255.82.1	192.168.0.200	TCP	62	http > mxxrlogin [SYN-- ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
18	6.605559	192.168.0.200	178.255.82.1	TCP	54	mxxrlogin > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
19	6.606058	192.168.0.200	178.255.82.1	HTTP	187	GET /av/tvl/deletedvendors.txt HTTP/1.1

ID	Time	Souce IP	Destination IP	Transmission Media	AVG packet length	Information
20	6.706385	178.255.82.1	192.168.0.200	TCP	60	http > mxxrlogin [ACK] Seq=1 Ack=134 Win=6432 Len=0
21	6.706849	178.255.82.1	192.168.0.200	TCP	1514	[TCP segment of a reassembled PDU]
22	6.707413	178.255.82.1	192.168.0.200	TCP	1514	[TCP segment of a reassembled PDU]
23	6.70765	192.168.0.200	178.255.82.1	TCP	54	mxxrlogin > http [ACK] Seq=134 Ack=2921 Win=64240 Len=0
24	6.708013	178.255.82.1	192.168.0.200	TCP	1514	[TCP segment of a reassembled PDU]
25	6.806699	178.255.82.1	192.168.0.200	HTTP	111	HTTP/1.1 200 OK (text/plain)
26	6.807087	192.168.0.200	178.255.82.1	TCP	54	mxxrlogin > http [ACK] Seq=134 Ack=4438 Win=64240 Len=0
27	8.446413	91.199.212.171	192.168.0.200	TCP	60	http > netinfo-local [FIN-- ACK] Seq=399 Ack=109 Win=14600 Len=0
28	8.446591	192.168.0.200	91.199.212.171	TCP	54	netinfo-local > http [ACK] Seq=109 Ack=400 Win=63842 Len=0
29	8.707529	178.255.82.1	192.168.0.200	TCP	60	http > mxxrlogin [FIN-- ACK] Seq=4438 Ack=134 Win=6432 Len=0
30	8.707946	192.168.0.200	178.255.82.1	TCP	54	mxxrlogin > http [ACK] Seq=134 Ack=4439 Win=64240 Len=0
31	203.4517	192.168.0.200	91.199.212.171	TCP	62	nsstp > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
32	203.4901	91.199.212.171	192.168.0.200	TCP	62	http > nsstp [SYN-- ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
33	203.4901	192.168.0.200	91.199.212.171	TCP	54	nsstp > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
34	203.4902	192.168.0.200	91.199.212.171	HTTP	233	GET /av/updates58/versioninfo.ini HTTP/1.1
35	203.5181	91.199.212.171	192.168.0.200	TCP	60	http > nsstp [ACK] Seq=1 Ack=180 Win=15544 Len=0
36	203.5187	91.199.212.171	192.168.0.200	HTTP	455	HTTP/1.1 302 Moved Temporarily (text/html)
37	203.52	192.168.0.200	178.255.82.1	TCP	62	netarx > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
38	203.6182	178.255.82.1	192.168.0.200	TCP	62	http > netarx [SYN-- ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
39	203.6182	192.168.0.200	178.255.82.1	TCP	54	netarx > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
40	203.6209	192.168.0.200	178.255.82.1	HTTP	258	GET

ID	Time	Souce IP	Destination IP	Transmission Media	AVG packet length	Information
						/av/updates58/versioninfo.ini HTTP/1.1
41	203.7079	192.168.0.200	91.199.212.171	TCP	54	nsstp > http [ACK] Seq=180 Ack=402 Win=63839 Len=0
42	203.7171	178.255.82.1	192.168.0.200	TCP	60	http > netarx [ACK] Seq=1 Ack=205 Win=6432 Len=0
43	203.7176	178.255.82.1	192.168.0.200	HTTP	412	HTTP/1.1 200 OK (application/octet-stream)
44	203.7237	192.168.0.200	91.199.212.171	HTTP	261	GET /av/updates58/sigs/updates/BASE_UPD_END_USER_v14873.cav.z HTTP/1.1
45	203.7515	91.199.212.171	192.168.0.200	HTTP	483	HTTP/1.1 302 Moved Temporarily (text/html)
46	203.7525	192.168.0.200	178.255.82.1	HTTP	286	GET /av/updates58/sigs/updates/BASE_UPD_END_USER_v14873.cav.z HTTP/1.1
47	203.9182	192.168.0.200	91.199.212.171	TCP	54	nsstp > http [ACK] Seq=387 Ack=831 Win=63410 Len=0
48	203.9185	178.255.82.1	192.168.0.200	TCP	1514	[TCP segment of a reassembled PDU]
49	203.9192	178.255.82.1	192.168.0.200	TCP	1514	[TCP segment of a reassembled PDU]
50	203.9194	178.255.82.1	192.168.0.200	TCP	1514	[TCP segment of a reassembled PDU]
51	203.9195	178.255.82.1	192.168.0.200	TCP	1514	[TCP segment of a reassembled PDU]

Sample Dataset for Real Traffic Traces

ID	Time	Source IP	Destination IP	Transmission Media	AVG packet length	Information
1	0	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
2	0.000007	122.166.4.242	122.166.96.126	UDP	1506	Source port: 35467 Destination port: ismserver
3	0.000261	122.166.4.242	122.166.96.126	UDP	1506	Source port: 35467 Destination port: ismserver
4	0.000268	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
5	0.000999	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
6	0.001124	122.166.4.242	122.166.96.126	UDP	1506	Source port: 35467 Destination port: ismserver
7	0.002249	122.166.4.242	122.166.96.126	UDP	1506	Source port: 35467 Destination port: ismserver
8	0.002254	122.166.4.242	122.166.96.126	UDP	1506	Source port: 35467 Destination port: ismserver
9	0.011372	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
10	0.012118	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
11	0.012493	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
12	0.012868	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
13	0.013618	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
14	0.013993	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
15	0.46674	122.166.4.242	122.166.96.126	UDP	1506	Source port: 35467 Destination port: ismserver
16	0.468932	122.166.4.242	122.166.96.126	UDP	1506	Source port: 35467 Destination port: ismserver
17	0.468941	122.166.4.242	122.166.96.126	UDP	1506	Source port: 35467 Destination port: ismserver
18	0.477614	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
19	0.477857	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
20	0.478856	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
21	0.479231	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
22	0.479981	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
23	0.480734	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
24	0.481854	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
25	0.48248	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver

ID	Time	Source IP	Destination IP	Transmission Media	AVG packet length	Information
26	0.48273	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
27	0.483228	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
28	0.483978	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
29	0.484853	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
30	0.485477	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
31	0.485853	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
32	0.487101	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
33	0.487726	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
34	0.500848	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
35	0.501469	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
36	0.501844	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
37	0.502093	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
38	0.502469	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
39	0.502969	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
40	0.503717	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
41	0.504841	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
42	0.505341	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
43	0.505591	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
44	0.505841	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
45	0.506341	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
46	0.506466	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
47	0.506841	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
48	0.50759	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
49	0.508464	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver
50	0.509089	122.166.4.242	122.166.96.126	UDP	1458	Source port: 35467 Destination port: ismserver

PUBLICATIONS

International Journals : 3

1. Dr.G.Padmavathi and S.Divya, "*A Survey on Various Security Threats and Classification of Malware Attacks, Vulnerabilities and Detection Techniques",* The International Journal of Computer Science and Applications (TIJCSA), Vol. 2, No. 04, June 2013, pp.66-72. **Cited by 1.**

2. S.Divya and Dr.G.Padmavathi, "*A Novel Method for Detection of Internet Worm Malcodes using Principal Component Analysis and Multiclass Support Vector Machine*", SERSC Publishers, International Journal of Security and Its Applications, Vol. 8, No. 5, 2014, pp. 391-402, ISSN : 1738-9976. **Scopus Indexed.** (http://dx.doi.org/10.14257/ijsia.2014.8.5.34)

3. S.Divya and Dr.G.Padmavathi, "*Packet Payload Monitoring for Internet Worm Content Detection Using Deterministic Finite Automaton with Delayed Dictionary Compression*", Hindawi Publishing Corporation, Journal of Computer Networks and Communications, Volume 2014, Article ID 206867, 9 pages, ISSN: 2090-715X. **Scopus Indexed.** (http://dx.doi.org/10.1155/2014/206867)

Journal Accepted for Publication : 1

1. S.Divya and Dr.G.Padmavathi, *"Internet Worm Detection based on Traffic Behavior Monitoring with Improved C4.5",* Computers and Security, The International Source of Innovation for the Information Security and IT Audit Professional, Vol. 65, May 2016. (**Elsevier**)

International Conference Proceedings : 2

1. S.Divya and Dr.G.Padmavathi, *"Computer Network Worms Propagation and its Defence Mechanisms:A Survey",* Proceedings on *International Conference on CNC & CCPE 2014*, February, pp.643-652, Organized by ACEE, Published by **Elsevier**. ISBN No. 978-81-910691-7-8

2. S.Divya and Dr.G.Padmavathi,"*Internet Worm Detection based on Traffic Behavior Monitoring with Improved C4.5",* Proceedings on *International Conference on Cryptography and Security(ICCS 2015),* July, pp.48-56, Organized by ASDF, Published by ASDF. ISBN No. 978-81-925233-5-4.