Analysis # 34336

11/12/2013 09:18 am

Table of Contents

Analysis Summary

Submitted File:	dot.exe
MD5:	b0dbfd7e359d4830d7ff4a5f40a78204
File Size:	82944
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-11-12 09:18:37
Start Reason:	AnalysisTarget
Termination Reason:	Timeout
Start Time:	Tue, 12 Nov 2013 14:22:23 +0000
Termination Time:	Tue, 12 Nov 2013 14:23:24 +0000
Analysis Time:	2013-11-12 09:18:37
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	1
Sample Notes:	

Digital Behavior Traits

Alters Windows Firewall	—	Hooks Keyboard	—
Checks For Debugger	✓	Injected Code	—
Copies to Windows	—	Makes Network Connection	✓
Could Not Load	—	Modifies File in System	—
Creates DLL in System	—	Modifies Local DNS	—
Creates EXE in System	—	More than 5 Processes	—
Creates Hidden File	✓	Opens Physical Memory	—
Creates Mutex	✓	Starts EXE in Documents	—
Creates Service	—	Starts EXE in Recycle	—
Deletes File in System	—	Starts EXE in System	—
Deletes Original Sample	—	Windows/Run Registry Key Set	✓

Deleted Files
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\cksglobal_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\brijindia_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\bocr[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@freepatentauction[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@www.patentauction[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@agence-des-druides[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\robertmcintyre_com_au[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\churchclothes_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\cksglobal_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\easyformations_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\unitedearthgroup_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\steelpennygames_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\cath4choice_org[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\hostphd_com_br[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\link-list-uk_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\woodlandhillwinery_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\home[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\d-j-b_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\woodlandhillwinery_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\colourprint_nl[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@google[2].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@google[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\google_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\kurecci_or_jp[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\sun-ele_co_jp[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@paintball[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\racknstackwarehouse_com_au[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\le-mariage_com[1].htm

[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\ginalimo_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\cksglobal_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@doctsf[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\churchclothes_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\index[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\woodlandhillwinery_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\niray_com_cn[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\violadagamba_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\icigrain_com[1]
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\justconnect_co_za[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\enzoyrodrigo_com_br[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\theprintinghouseltd_co_uk[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\woodlandhillwinery_com[1].htm

Stored Modified Files
[process 1] C:\Documents and Settings\Administrator\gofkiwazosor.exe
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@chocolatecovers[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@appelfarm[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@geothermusa[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\cksglobal_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\sortedorganizing_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\brijindia_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\89OC5JKA\wkhk_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@westhillsstl[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\bocr[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@freepatentauction[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@freepatentauction[2].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@www.patentauction[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@www.patentauction[2].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@agence-des-druides[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@agence-des-druides[2].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@taykon[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@re-wakefield.co[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@atr-technologies[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\index.dat
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\robertmcintyre_com_au[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\churchclothes_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\atr-technologies_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@traderush[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\csmbc_org[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\22ZWITMI\photoclubs_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\cksglobal_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\easyformations_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\AESBU5XV\thedonaldsongroup_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@golfpark-moossee[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\unitedearthgroup_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\steelpennygames_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\M7KWPPD6\rueggeberg_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.

IE5\89OC5JKA\hostphd_com_br[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\89OC5JKA\cath4choice_org[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\89OC5JKA\eygwindows_co_uk[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@wsipowerontheweb[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\22ZWITMI\link-list-uk_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\22ZWITMI\woodlandhillwinery_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\22ZWITMI\home[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@4pipp[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\22ZWITMI\teasing-video_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\22ZWITMI\d-j-b_net[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@glmghotels[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\AESBU5XV\woodlandhillwinery_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@racknstackwarehouse.com[1]
.txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\AESBU5XV\colourprint_nl[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@google[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@google[2].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\M7KWPPD6\google_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@screaminpeach[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@pcpeds[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\M7KWPPD6\kurecci_or_jp[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\AESBU5XV\sun-ele_co_jp[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@paintball[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@paintball[2].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@totalearthcare.com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\AESBU5XV\mibsga_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@sdlp[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\89OC5JKA\le-mariage_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@cbsprinting.com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.
IE5\AESBU5XV\ginalimo_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@stepnet[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@choice-select[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@doctsf[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@doctsf[2].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@www.servico-ind[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.

IE5\AESBU5XV\index[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\AESBU5XV\solutioncorp_com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\22ZWITMI\ixtractor_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@ctr4process[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\AESBU5XV\mojacar-vacaciones_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\AESBU5XV\niray_com_cn[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@rodeoshow.com[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\M7KWPPD6\violadagamba_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\M7KWPPD6\icigrain_com[1]
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\M7KWPPD6\justconnect_co_za[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\M7KWPPD6\enzoyrodrigo_com_br[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@area72aa[1].txt
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\M7KWPPD6\theprintinghouseltd_co_uk[1].htm
[process 1] C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content. IE5\M7KWPPD6\woodlandhillwinery_com[1].htm
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@graceweb[1].txt
[process 1] C:\Documents and Settings\Administrator\Cookies\administrator@figabara[1].txt

Created Mutexes	
	mutex
[process 1]	Name: gofkiwazosor
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:!documents and settings!administrator!local settings!temporary internet files!content.
	ie5!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:!documents and settings!administrator!cookies!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\c:!documents and settings!administrator!local settings!history!history.ie5!
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\WininetConnectionMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: RasPbFile
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZonesCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZoneAttributeCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZonesCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE
[process 1]	Name: Local\ZonesLockedCacheCounterMutex
	Desired Access: DELETE READ_CONTROL SYNCHRONIZE WRITE_DAC WRITE_OWNER MUTEX_MODIFY_STATE

Set Values	
	key
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Cryptography\RNG Value: Seed
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion Value: AppManagement
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion Value: gofkiwazosorzap
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cache
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Cookies
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: History
[process 1]	Key Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: Common AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Value: AppData
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr

	entVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: ProxyBypass
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: IntranetName
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: UNCAsIntranet
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Value: AutoDetect
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyEnable
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr

	entVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections Value: SavedLegacySettings
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Run Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr

	entVersion\Run
	Value: gofkiwazosor
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\Curr
	entVersion\Run
	Value: gofkiwazosor

Deleted Values	
	key
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyServer
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: ProxyOverride
[process 1]	Key Name: \REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: AutoConfigURL

Network Events			
	Remote IP	**Local IP**	**HTTP Command**
[process 1]	65.55.96.11	10.20.25.247	none
[process 1]	203.189.104.242	10.20.25.247	POST /
[process 1]	184.168.233.1	10.20.25.247	POST /
[process 1]	109.74.242.160	10.20.25.247	POST /
[process 1]	64.99.80.30	10.20.25.247	POST /
[process 1]	85.233.160.22	10.20.25.247	POST /
[process 1]	49.50.8.93	10.20.25.247	none
[process 1]	178.63.17.213	10.20.25.247	POST /
[process 1]	217.198.115.41	10.20.25.247	POST / GET /bocr GET /bocr/
[process 1]	192.168.0.1	10.20.25.247	none
[process 1]	50.62.125.1	10.20.25.247	POST /
[process 1]	46.249.205.175	10.20.25.247	POST /
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	157.7.160.37	10.20.25.247	POST /
[process 1]	10.20.25.1	10.20.25.247	none
[process 1]	151.236.48.69	10.20.25.247	POST /
[process 1]	10.20.25.1	10.20.25.247	none
[process 1]	108.162.206.115	10.20.25.247	POST /
[process 1]	67.227.252.139	10.20.25.247	POST /
[process 1]	112.175.11.240	10.20.25.247	POST /
[process 1]	141.101.123.98	10.20.25.247	POST /
[process 1]	173.0.131.15	10.20.25.247	GET /
[process 1]	195.22.26.253	10.20.25.247	GET /
[process 1]	112.140.176.61	10.20.25.247	POST /
[process 1]	203.189.104.242	10.20.25.247	GET /
[process 1]	74.220.199.6	10.20.25.247	POST

			/
[process 1]	193.23.143.117	10.20.25.247	POST /
[process 1]	209.50.251.101	10.20.25.247	POST /
[process 1]	59.106.165.171	10.20.25.247	POST /
[process 1]	69.94.124.47	10.20.25.247	POST /
[process 1]	89.221.250.12	10.20.25.247	POST /
[process 1]	67.18.185.98	10.20.25.247	POST /
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	173.231.139.57	10.20.25.247	POST /
[process 1]	178.124.130.199	10.20.25.247	POST /
[process 1]	178.124.130.199	10.20.25.247	POST /
[process 1]	208.113.149.173	10.20.25.247	POST /
[process 1]	204.227.165.46	10.20.25.247	POST / POST /private/sandbox_status.php
[process 1]	213.186.33.4	10.20.25.247	POST /
[process 1]	108.162.196.220	10.20.25.247	POST /
[process 1]	68.67.76.41	10.20.25.247	none
[process 1]	208.113.225.142	10.20.25.247	GET /
[process 1]	219.94.206.70	10.20.25.247	POST /
[process 1]	85.158.207.109	10.20.25.247	POST /
[process 1]	209.50.248.224	10.20.25.247	POST /
[process 1]	129.121.224.188	10.20.25.247	POST /
[process 1]	213.186.33.4	10.20.25.247	GET /
[process 1]	207.150.203.36	10.20.25.247	POST /
[process 1]	89.161.158.128	10.20.25.247	POST /
[process 1]	141.101.125.46	10.20.25.247	POST /
[process 1]	216.70.112.211	10.20.25.247	none
[process 1]	211.1.230.105	10.20.25.247	none

[process 1]	54.227.239.237	10.20.25.247	POST /
[process 1]	59.106.13.131	10.20.25.247	POST /
[process 1]	88.198.7.211	10.20.25.247	none
[process 1]	213.186.33.3	10.20.25.247	POST /
[process 1]	66.155.9.238	10.20.25.247	POST /
[process 1]	173.247.243.173	10.20.25.247	POST /
[process 1]	141.101.116.127	10.20.25.247	POST /
[process 1]	199.73.58.66	10.20.25.247	POST /
[process 1]	192.168.100.1	10.20.25.247	none
[process 1]	97.74.42.79	10.20.25.247	POST / POST /
[process 1]	141.101.117.86	10.20.25.247	POST /
[process 1]	141.101.117.118	10.20.25.247	POST /
[process 1]	141.101.116.118	10.20.25.247	GET /
[process 1]	204.213.246.4	10.20.25.247	POST /
[process 1]	50.23.134.43	10.20.25.247	POST /
[process 1]	31.7.35.112	10.20.25.247	POST /
[process 1]	199.83.129.93	10.20.25.247	POST /
[process 1]	69.27.112.3	10.20.25.247	POST /
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	162.105.5.245	10.20.25.247	POST /
[process 1]	209.50.251.101	10.20.25.247	GET /
[process 1]	69.27.112.3	10.20.25.247	GET /
[process 1]	173.247.243.173	10.20.25.247	POST /
[process 1]	70.86.7.138	10.20.25.247	POST /
[process 1]	91.109.14.224	10.20.25.247	POST /
[process 1]	88.208.216.219	10.20.25.247	POST /

[process 1]	173.0.131.15	10.20.25.247	GET /
[process 1]	46.249.205.175	10.20.25.247	POST /
[process 1]	144.76.86.115	10.20.25.247	none
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	109.234.111.40	10.20.25.247	POST /
[process 1]	88.198.7.211	10.20.25.247	none
[process 1]	64.120.153.69	10.20.25.247	POST /
[process 1]	213.171.195.105	10.20.25.247	POST /
[process 1]	149.126.72.165	10.20.25.247	POST /
[process 1]	199.83.129.93	10.20.25.247	POST /
[process 1]	50.97.221.19	10.20.25.247	POST /
[process 1]	62.233.107.131	10.20.25.247	POST /
[process 1]	81.209.182.37	10.20.25.247	POST /
[process 1]	107.22.254.167	10.20.25.247	none
[process 1]	76.12.228.8	10.20.25.247	POST /
[process 1]	199.48.164.108	10.20.25.247	POST /
[process 1]	66.49.139.143	10.20.25.247	POST /
[process 1]	209.222.48.210	10.20.25.247	POST / POST /
[process 1]	210.183.236.111	10.20.25.247	POST /
[process 1]	91.216.141.46	10.20.25.247	POST /
[process 1]	108.162.199.18	10.20.25.247	POST / POST /
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	41.203.18.186	10.20.25.247	POST /
[process 1]	210.172.144.247	10.20.25.247	POST /
[process 1]	173.203.121.238	10.20.25.247	POST /
[process 1]	211.13.204.89	10.20.25.247	POST /

[process 1]	198.252.69.69	10.20.25.247	POST / POST /
[process 1]	204.11.237.35	10.20.25.247	POST /
[process 1]	70.32.102.108	10.20.25.247	POST / POST / POST /
[process 1]	173.203.121.238	10.20.25.247	GET /web/store/home
[process 1]	184.94.149.35	10.20.25.247	none
[process 1]	93.186.180.72	10.20.25.247	POST /
[process 1]	141.101.117.69	10.20.25.247	POST /
[process 1]	99.192.154.182	10.20.25.247	POST /
[process 1]	74.119.145.130	10.20.25.247	POST /
[process 1]	173.201.140.128	10.20.25.247	POST /
[process 1]	141.101.116.108	10.20.25.247	POST /
[process 1]	180.222.185.78	10.20.25.247	POST /
[process 1]	217.149.11.231	10.20.25.247	POST /
[process 1]	141.101.117.200	10.20.25.247	POST / POST /
[process 1]	186.202.149.17	10.20.25.247	POST /
[process 1]	46.30.212.230	10.20.25.247	POST /
[process 1]	67.223.102.173	10.20.25.247	POST /
[process 1]	50.28.58.0	10.20.25.247	none
[process 1]	118.144.82.146	10.20.25.247	POST /
[process 1]	205.251.133.202	10.20.25.247	POST /
[process 1]	202.47.95.44	10.20.25.247	POST / POST /private/sandbox_status.php
[process 1]	60.43.132.135	10.20.25.247	POST

			/
[process 1]	211.13.204.89	10.20.25.247	POST /
[process 1]	119.245.143.88	10.20.25.247	POST /
[process 1]	173.194.41.120	10.20.25.247	POST /
[process 1]	178.124.130.199	10.20.25.247	POST /
[process 1]	210.150.6.88	10.20.25.247	POST /
[process 1]	65.98.59.242	10.20.25.247	POST /
[process 1]	37.187.20.229	10.20.25.247	POST /
[process 1]	74.125.229.178	10.20.25.247	GET /
[process 1]	208.113.187.143	10.20.25.247	POST /
[process 1]	210.169.184.168	10.20.25.247	POST /
[process 1]	204.93.213.45	10.20.25.247	POST /
[process 1]	108.162.202.140	10.20.25.247	POST /
[process 1]	108.162.203.235	10.20.25.247	POST /
[process 1]	194.50.126.226	10.20.25.247	POST / POST / POST /private/sandbox_status.php
[process 1]	108.162.200.55	10.20.25.247	POST /
[process 1]	64.111.24.104	10.20.25.247	POST /
[process 1]	213.186.33.19	10.20.25.247	POST /
[process 1]	66.232.99.164	10.20.25.247	POST /
[process 1]	67.227.252.139	10.20.25.247	POST /
[process 1]	112.175.11.240	10.20.25.247	POST /
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	108.175.148.57	10.20.25.247	POST /
[process 1]	209.50.251.101	10.20.25.247	POST /
[process 1]	74.124.214.210	10.20.25.247	GET

			/
[process 1]	108.162.196.53	10.20.25.247	POST
			/
[process 1]	219.118.206.4	10.20.25.247	POST
			/
[process 1]	78.47.37.140	10.20.25.247	POST
			/
[process 1]	46.105.107.214	10.20.25.247	POST
			/
[process 1]	198.154.229.165	10.20.25.247	POST
			/
[process 1]	141.101.117.223	10.20.25.247	POST
			/
[process 1]	141.101.116.74	10.20.25.247	POST
			/
[process 1]	121.83.133.146	10.20.25.247	POST
			/
[process 1]	168.144.109.12	10.20.25.247	none
[process 1]	209.105.227.150	10.20.25.247	POST
			/
[process 1]	199.204.137.151	10.20.25.247	POST
			/
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	218.150.78.243	10.20.25.247	POST
			/
[process 1]	182.50.130.117	10.20.25.247	POST
			/
[process 1]	157.7.184.19	10.20.25.247	POST
			/
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	157.7.184.19	10.20.25.247	GET
			/
[process 1]	69.198.129.78	10.20.25.247	none
[process 1]	211.13.204.89	10.20.25.247	POST
			/
[process 1]	213.208.149.2	10.20.25.247	none
[process 1]	108.162.200.50	10.20.25.247	POST
			/
[process 1]	46.249.205.175	10.20.25.247	POST
			/
[process 1]	216.70.113.196	10.20.25.247	POST
			/
[process 1]	173.231.139.57	10.20.25.247	POST
			/
[process 1]	67.223.102.97	10.20.25.247	POST
			/
[process 1]	85.159.56.120	10.20.25.247	POST
			/
[process 1]	202.47.95.44	10.20.25.247	POST
			/
[process 1]	122.219.254.148	10.20.25.247	none

[process 1]	92.61.39.244	10.20.25.247	POST /
[process 1]	89.161.181.123	10.20.25.247	POST /
[process 1]	49.50.249.80	10.20.25.247	POST /
[process 1]	116.251.205.115	10.20.25.247	POST /
[process 1]	49.50.249.80	10.20.25.247	GET /404.html
[process 1]	124.146.222.27	10.20.25.247	POST /
[process 1]	79.98.23.30	10.20.25.247	POST /
[process 1]	85.159.56.120	10.20.25.247	GET /index.asp
[process 1]	127.0.0.1	0.0.0.0	none
[process 1]	188.93.212.32	10.20.25.247	POST /
[process 1]	95.110.192.171	10.20.25.247	POST /
[process 1]	208.87.35.103	10.20.25.247	POST /
[process 1]	91.121.66.183	10.20.25.247	POST /
[process 1]	69.163.135.152	10.20.25.247	POST /
[process 1]	213.186.33.17	10.20.25.247	POST /
[process 1]	10.0.0.1	10.20.25.247	none
[process 1]	69.0.211.58	10.20.25.247	POST /
[process 1]	116.251.204.207	10.20.25.247	POST /
[process 1]	198.1.90.242	10.20.25.247	POST /
[process 1]	209.208.32.245	10.20.25.247	POST /
[process 1]	209.208.32.245	10.20.25.247	GET /
[process 1]	209.222.7.227	10.20.25.247	POST /
[process 1]	209.222.7.227	10.20.25.247	GET /
[process 1]	192.168.0.1	10.20.25.247	none
[process 1]	199.19.85.86	10.20.25.247	POST /
[process 1]	108.162.203.164	10.20.25.247	POST /
[process 1]	10.0.0.1	10.20.25.247	none
[process 1]	198.252.69.69	10.20.25.247	POST

			/
[process 1]	93.186.180.72	10.20.25.247	POST
			/
[process 1]	199.83.129.93	10.20.25.247	POST
			/
[process 1]	12.158.190.246	10.20.25.247	POST
			/
[process 1]	60.43.132.135	10.20.25.247	POST
			/
[process 1]	122.55.79.88	10.20.25.247	none
[process 1]	75.119.209.232	10.20.25.247	POST
			/
[process 1]	103.28.249.103	10.20.25.247	POST
			/
[process 1]	50.62.115.1	10.20.25.247	POST
			/
[process 1]	199.83.131.103	10.20.25.247	GET
			/
[process 1]	50.62.115.1	10.20.25.247	GET
			/
[process 1]	74.124.195.5	10.20.25.247	POST
			/
[process 1]	184.168.233.1	10.20.25.247	POST
			/
[process 1]	199.91.125.75	10.20.25.247	POST
			/
[process 1]	199.83.129.93	10.20.25.247	POST
			/
[process 1]	5.9.122.172	10.20.25.247	POST
			/
[process 1]	69.198.129.78	10.20.25.247	none
[process 1]	5.9.122.172	10.20.25.247	GET
			/
[process 1]	216.245.218.146	10.20.25.247	POST
			/
[process 1]	217.199.187.58	10.20.25.247	POST
			/
[process 1]	66.147.244.241	10.20.25.247	POST
			/
[process 1]	66.241.192.192	10.20.25.247	POST
			/
[process 1]	216.8.179.23	10.20.25.247	POST
			/
[process 1]	46.20.228.113	10.20.25.247	POST
			/
[process 1]	184.106.119.164	10.20.25.247	POST
			/
[process 1]	196.209.216.192	10.20.25.247	none
[process 1]	91.216.141.46	10.20.25.247	POST
			/
[process 1]	198.252.69.69	10.20.25.247	POST

			/
[process 1]	182.50.130.117	10.20.25.247	POST
			/
[process 1]	122.55.79.88	10.20.25.247	none
[process 1]	208.97.174.44	10.20.25.247	POST
			/
[process 1]	66.33.213.228	10.20.25.247	none
[process 1]	108.162.197.90	10.20.25.247	GET
			/
[process 1]	108.162.197.115	10.20.25.247	POST
			/
[process 1]	119.145.168.16	10.20.25.247	none

Network Traffic		
	Remote IP	**Local IP**
Connection #1	10.20.25.255	10.20.25.247
Connection #2	10.20.25.248	10.20.25.247
Connection #3	10.20.25.255	10.20.25.247
Connection #4	10.20.25.248	10.20.25.247

DNS Requests	
Request	**Result**
smtp.live.com	65.55.96.11
marcusgrimes.co.uk	109.74.242.160
wkhk.net	203.189.104.242
eleterno.com	184.168.233.1
berkshirebusiness.org	64.99.80.30
agrarno.ru	178.63.17.213
iaiglobal.or.id	49.50.8.93
bocr.cz	217.198.115.41
eyggroup.com	85.233.160.22
tollefsondesign.com	192.168.0.1
tutuji-saitama.com	157.7.160.37
avisay.com	127.0.0.1
cksglobal.net	46.249.205.175
geothermusa.com	50.62.125.1
appelfarm.org	108.162.206.115
	108.162.205.115
upsilon89.com	151.236.48.69
ans-service.com	67.227.252.139
macgregor.co.kr	112.175.11.240
chocolatecovers.com	141.101.123.98
	190.93.242.98
	190.93.241.98
	190.93.243.98
	190.93.240.98
www.eygwindows.co.uk	173.0.131.15
stop-ddos.me	195.22.26.253
	195.22.26.231
	195.22.26.254
	195.22.26.252
kamaruka.vic.edu.au	112.140.176.61
www.wkhk.net	203.189.104.242
sortedorganizing.com	74.220.199.6
stecom.nl	193.23.143.117
photoclubs.com	209.50.251.101
xing-group.com	59.106.165.171
urantiaproject.com	69.94.124.47
digpro.se	89.221.250.12
brijindia.com	67.18.185.98
arckepesajandek.hu	127.0.0.1
mail57.us2.mcsv.net	173.231.139.57
vitalur.by	178.124.130.199
sigmametalsinc.com	208.113.149.173
ompgp.co.jp	204.227.165.46
freepatentauction.com	213.186.33.4
westhillsstl.org	108.162.196.220
	108.162.197.220
bapasitaramsevatrust.org	68.67.76.41
www.sigmaaero.com	208.113.225.142
trinity-works.com	219.94.206.70

al-mawared.com	209.50.248.224
heliomare.nl	85.158.207.109
csmbc.org	129.121.224.188
www.patentauction.com	213.186.33.4
acicinvestor.ca	207.150.203.36
gablemarine.com	141.101.125.46
	141.101.126.46
victoria.com.pl	89.161.158.128
msasys.com	216.70.112.211
jeansmate.co.jp	211.1.230.105
steelpennygames.com	54.227.239.237
coketh.com	59.106.13.131
fabianonline.de	88.198.7.211
agence-des-druides.com	213.186.33.3
c21edu.com	66.155.9.238
	66.155.11.238
	76.74.254.123
	76.74.254.120
	192.0.81.250
	192.0.80.250
toddpipe.com	173.247.243.173
taykon.com	141.101.116.127
	141.101.117.127
robertmcintyre.com.au	199.73.58.66
nataliecurtiss.com	192.168.100.1
churchclothes.com	97.74.42.79
re-wakefield.co.uk	141.101.117.86
	141.101.116.86
atr-technologies.com	141.101.117.118
	141.101.116.118
www.atr-technologies.com	141.101.116.118
	141.101.117.118
bethisraelcenter.org	204.213.246.4
shbrazil.com	50.23.134.43
istanbultarim.com.tr	31.7.35.112
www.traderush.com	199.83.129.93
hpp-services.com	69.27.112.3
audio-direkt.net	127.0.0.1
coe.pku.edu.cn	162.105.5.245
www.photoclubs.com	209.50.251.101
www.hpp-services.com	69.27.112.3
stormwildlifeart.com	70.86.7.138
link-list-uk.com	91.109.14.224
easyformations.net	88.208.216.219
eygwindows.co.uk	173.0.131.15
rovoneli.com	144.76.86.115
skaner.com.pl	109.234.111.40
genmar.gen.tr	127.0.0.1
thedonaldsongroup.com	64.120.153.69
unitedearthgroup.com	213.171.195.105
golfpark-moossee.ch	149.126.72.165

	199.83.130.50
acsmedioambiente.com	50.97.221.19
padstow.com	62.233.107.131
rueggeberg.com	81.209.182.37
tss.org	107.22.254.167
cath4choice.org	76.12.228.8
hostphd.com.br	199.48.164.108
christybarry.com	66.49.139.143
safetyconnection.ca	209.222.48.210
nuritech.com	210.183.236.111
tvndra.net	91.216.141.46
wsipowerontheweb.com	108.162.199.18
	108.162.198.18
fruitspot.co.za	41.203.18.186
d-j-b.net	210.172.144.247
szostka.com	127.0.0.1
childscope.com	173.203.121.238
e-shuukyaku.com	211.13.204.89
woodlandhillwinery.com	198.252.69.69
denville.ca	204.11.237.35
theautospas.com	70.32.102.108
www.childscope.com	173.203.121.238
dormfantasies.com	184.94.149.35
pbna.com	93.186.180.72
hinnenwiese.de	127.1.0.2
4pipp.com	141.101.117.69
	141.101.116.69
teasing-video.com	99.192.154.182
adultlivechat.us	74.119.145.130
buzzkillmedia.com	173.201.140.128
glmghotels.com	141.101.116.108
	141.101.117.108
urayasu.net	NONE
ryumachi-jp.com	180.222.185.78
trenpalau.com	217.149.11.231
urayasu.net.local	NONE
guberman.com.br	186.202.149.17
racknstackwarehouse.com.au	141.101.117.200
	141.101.116.200
colourprint.nl	46.30.212.230
capitalcitytuxedo.com	67.223.102.173
unslp.edu.bo	50.28.58.0
realtechre.com	205.251.133.202
niray.com.cn	118.144.82.146
thesergery.com	202.47.95.44
kagu-hokuren.com	60.43.132.135
yamamoto-sr.com	211.13.204.89
kurecci.or.jp	119.245.143.88
merceorti.com	173.194.41.120
	80.93.92.146
tessera.co.jp	210.150.6.88

tavdi.com	65.98.59.242
iktus.fr	37.187.20.229
www.google.com	74.125.229.178
	74.125.229.180
	74.125.229.177
	74.125.229.176
	74.125.229.179
arquiteturadigital.com	208.113.187.143
sun-ele.co.jp	210.169.184.168
graintrain.coop	204.93.213.45
screaminpeach.com	108.162.203.235
	108.162.204.235
goodvaluecenter.com	108.162.202.140
	108.162.201.140
ziuabarbatului.ro	194.50.126.226
pcpeds.com	108.162.200.55
	141.101.127.54
fleshercorp.com	64.111.24.104
paintball.be	213.186.33.19
churchsupplies.net	66.232.99.164
hoyuu.com	NONE
pixemia.com	127.0.0.1
hoyuu.com.local	NONE
midwestga.com	108.175.148.57
www.mibsga.com	74.124.214.210
totalearthcare.com.au	108.162.196.53
	108.162.197.53
asj.co.jp	219.118.206.4
le-mariage.com	46.105.107.214
lognetic.com	78.47.37.140
paulrenna.com	198.154.229.165
sdlp.ie	141.101.117.223
cbsprinting.com.au	141.101.116.74
	141.101.117.74
egao.net	121.83.133.146
starmedia.ca	168.144.109.12
ginalimo.com	209.105.227.150
malagacorp.com	199.204.137.151
penavision.co.in	127.0.0.1
ezmedi.com	218.150.78.243
sspackaginggroup.com	182.50.130.117
saios.net	157.7.184.19
www.saios.net	157.7.184.19
meridies.org	127.0.0.1
acmepacificrepairs.com	69.198.129.78
osouji-school.com	211.13.204.89
eomc.net	213.208.149.2
stepnet.de	108.162.200.50
	141.101.127.49
phototype.com	216.70.113.196
courtney.ca	67.223.102.97

servico-ind.com	85.159.56.120
mastergrp-spb.ru	NONE
mastergrp-spb.ru.local	NONE
aipi.co.nz	NONE
aipi.co.nz.local	NONE
konishi-hp.com	122.219.254.148
miltinio-teatras.lt	92.61.39.244
biurimex.pl	89.161.181.123
krafthaus.com	49.50.249.80
xuanxiao.com	116.251.205.115
www.krafthaus.com	49.50.249.80
djkentaro.com	124.146.222.27
nd-evenementiel.com	79.98.23.30
www.servico-ind.com	85.159.56.120
accel.lt	127.0.0.1
kvadratoff.ru	188.93.212.32
sztartufi.com	95.110.192.171
choice-select.com	208.87.35.103
e-storming.com	91.121.66.183
beechwoodmetalworks.com	69.163.135.152
doctsf.com	213.186.33.17
celebikalip.com.tr	10.0.0.1
nazcapictures.com	69.0.211.58
brookfarm.com.au	116.251.204.207
gamblingonlinemagazine.com	198.1.90.242
solutioncorp.com	209.208.32.245
www.solutioncorp.com	209.208.32.245
ixtractor.com	209.222.7.227
www.ixtractor.com	209.222.7.227
ibcd.com.br	192.168.0.1
area72aa.org	199.19.85.86
ctr4process.org	108.162.203.164
	108.162.204.164
mojacar-vacaciones.com	12.158.190.246
shakeyspizza.ph	122.55.79.88
debtrescueusa.com	NONE
fastarchofamerica.com	75.119.209.232
debtrescueusa.com.local	NONE
toutenmeuse.com	NONE
toutenmeuse.com.local	NONE
rodeoshow.com.au	103.28.249.103
	103.28.250.103
vanguardpkg.com	50.62.115.1
www.rodeoshow.com.au	199.83.131.103
www.vanguardpkg.com	50.62.115.1
violadagamba.com	74.124.195.5
icigrain.com	199.91.125.75
justconnect.co.za	5.9.122.172
www.justconnect.co.za	5.9.122.172
enzoyrodrigo.com.br	216.245.218.146
spiti.org	217.199.187.58

dbcomponents.com	66.147.244.241
bigtopmultimedia.com	66.241.192.192
sullyfrance.com	216.8.179.23
theprintinghouseltd.co.uk	46.20.228.113
wlf.louisiana.gov	184.106.119.164
hartmultimedia.com	196.209.216.192
graceweb.net	208.97.174.44
myfilecenter.com	66.33.213.228
www.graceweb.net	108.162.197.90
	108.162.196.90
figabara.com	108.162.197.115
	108.162.196.115
nanfangcw.com	119.145.168.16
nichedictionary.com	NONE
nichedictionary.com.local	NONE

Virus Total Results
No Results

ThreatTrack Security, Inc.
33 North Garden Avenue, Suite 1200, Clearwater, Florida, USA 33755
Telephone: (855) 443-4284 Intl: +1(813)367-9907
Email: Sales@ThreatTrack.com