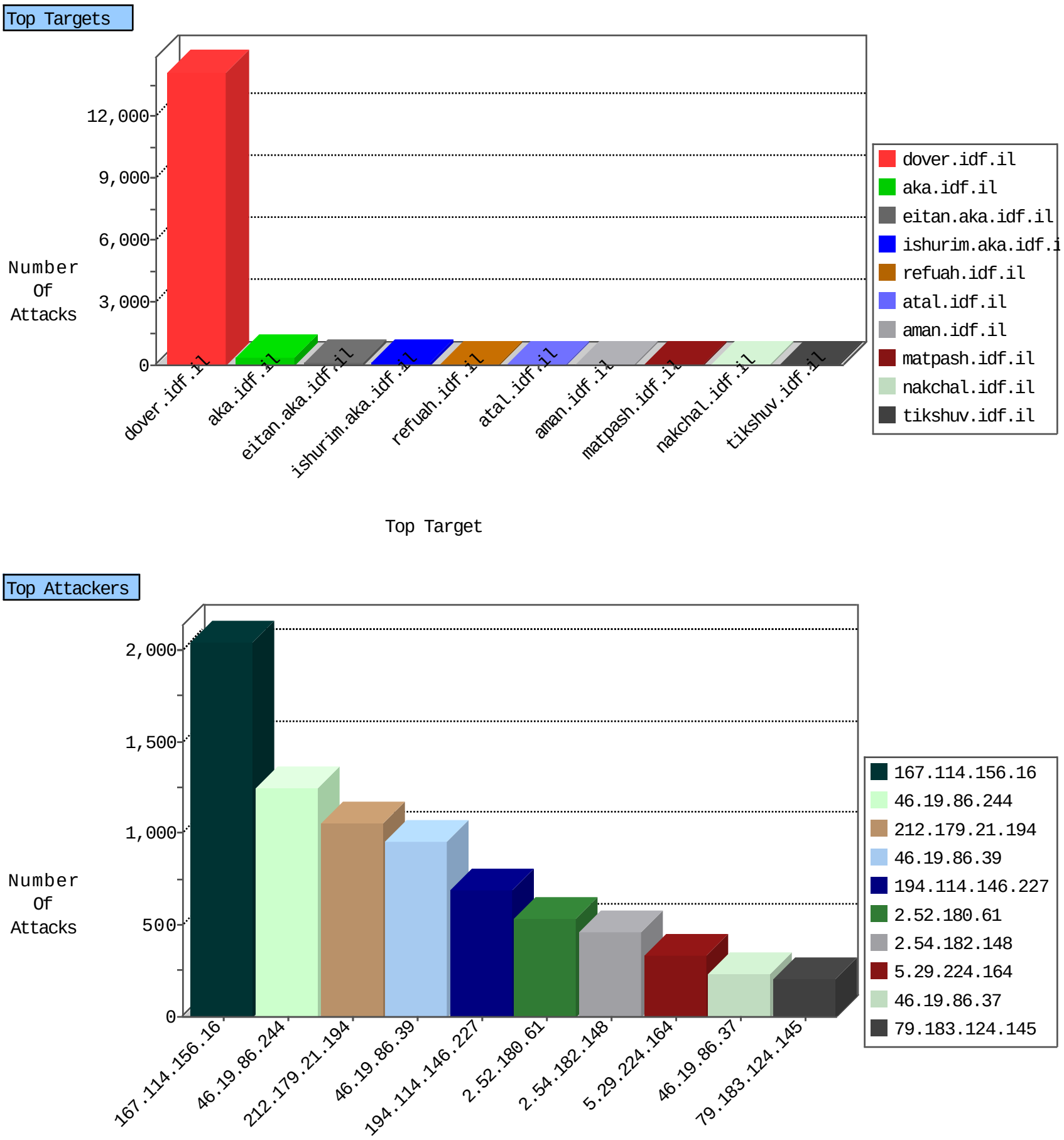
11-03-2015-10:04:00 to 11-03-2015-11:04:00

IDF Under Attack Daily Report



11-03-2015-10:04:00 to 11-03-2015-11:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	3160
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood full table	drop	1108
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	533
62.90.165.46	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	72
2.54.181.1	Israel	147.237.77.216	dover.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	69
46.19.85.184	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	35
79.178.119.11	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	30
2.54.142.246	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	25
87.69.222.124	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	25
2.54.23.87	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	25
46.120.140.241	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	25
37.142.148.89	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	25
37.26.148.147	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	23
37.142.64.136	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	23
2.54.6.56	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	23
46.19.86.180	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	21
212.143.3.44	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	21
185.120.126.55		147.237.77.216	dover.idf.i	SYN Flood full table	drop	20
89.139.184.97	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	20
176.106.46.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	20
95.35.151.97	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	20
2.54.146.158	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	19
2.54.162.101	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	18
89.138.228.218	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	16
176.12.148.151	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	15
192.114.91.244	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	14
212.179.21.194	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	12
46.121.102.134	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
109.160.143.218	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
79.183.124.145	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
82.80.17.163	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
5.29.160.138	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
79.181.114.93	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
87.69.189.161	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
46.19.86.90	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
46.19.85.163	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
46.19.86.167	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	9
2.54.148.68	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
77.126.12.20	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
46.117.94.150	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
84.94.39.148	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
82.166.88.93	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
194.90.169.2	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
176.12.137.114	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
46.19.86.87	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
80.246.136.37	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
134.191.232.68	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
37.26.147.221	Israel	147.237.77.216	dover.idf.i	SYN Flood delete reset	drop	6
82.213.0.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
37.26.147.221	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6

11-03-2015-10:04:00 to 11-03-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.116.167	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
2.54.54.177	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-03-2015-10:04:00 to 11-03-2015-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.108.75.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.190.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.182.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.102.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
91.144.30.96	147.237.77.216	Syrian Arab Republic	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.156.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.190.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.224	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
210.61.150.154	147.237.8.50	Taiwan	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1
185.32.179.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-03-2015-10:04:00 to 11-03-2015-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1248
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1040
46.19.86.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	955
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	689
2.52.180.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	539
2.54.182.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	465
5.29.224.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	333
46.19.86.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	230
79.183.124.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	185
2.54.151.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	175
109.67.50.81	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
176.16.209.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
46.19.86.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
37.26.146.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
46.19.85.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
37.142.64.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
193.106.206.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
212.143.84.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
91.144.30.96	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
84.109.166.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
2.54.178.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
101.177.22.167	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
178.193.108.150	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
46.19.86.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
149.78.184.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
176.106.46.249	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
2.54.162.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
2.54.177.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.26.149.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.26.148.147	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	36
37.26.148.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
93.78.98.176	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.52.61.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.54.130.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
2.54.38.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
168.63.200.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
82.213.0.210	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
176.12.143.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.12.145.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.52.183.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.78.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
84.94.152.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.86.63	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
2.54.24.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25

11-03-2015-10:04:00 to 11-03-2015-11:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.129.216	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.129.216	Block	5
192.117.175.226	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	4
84.229.35.245	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
192.117.49.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
149.88.129.216	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
80.246.136.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
81.218.203.20	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
149.88.232.199	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	2
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name }Â•ÃŠÂº@n]GÃ©Âµ[[#25]]Â^Ã¾ÂŸÂ-[[#25]]J$[[#1]]Â–'Ã¨-Ã–Âƒ`ÂºPÂ‡Â´Â‡Â»eÂ›3I7Ã^7JÂ¬[[#1]]8Ã‹Â” [[#21]]Ã•Ã¨ÃŒ.Â£Ã^ÃªÂ½~Ã¿Ã¶?Ã›Ã?Ã‰2Ã®Ã€ DV$Ã¶Â-[[#3]]Â?[[#8]][[#22]]oÂª[[#8]]ÃªÃºÂ½Ã«UÃŽCezÂš	Block	1
2.54.19.218	Israel	147.237.72.166	aka.idf.il	Too Many 403: Response Code per Session	Block	1
192.117.49.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.117.49.171	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 5.29.247.168	Block	1
66.249.83.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
141.212.121.208	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
14.139.244.243	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
2.54.40.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=e8e73185a4e34167.1436095445.4.1446540517.1446540517. ;	Block	1
149.88.129.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
85.64.49.39	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/113267.pdf	Block	1
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 5.29.247.168	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
212.150.59.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
176.13.12.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wepdwullte5odk5nji2ntmpzbyczg9kfgjmd2qwagidd2qwbaihdw8wah4hvmlzawjszwhkzaild2qwbaibd2qwagibdxychgrocmvmbqxkzwzhdwx0lmfzchhkagupzbycagepfgiebxn0ewxlbqt3awr0ado5ntbwebyeagepfgiecwlubmvyahrtbauz16nxknec15xxqidxldeq16nxlder15xxqmqcag8wah8cbqt3awr0ado5ntbwegqyaquex19db250cm9sc1jlcxvpcmvqb3n0qmfja0tlev9ffgmffmn0bdawjgn0bdawjhjivghpc1npdguffmn0bdawjgn0bdawjhjiqwxsu2l0zxmffmn0bdawjgn0bdawjhjiqwxsu2l0zxm8eh5yubarwrcttqtsdbjv4srbosmtntap+hah2uc8vg==	Block	1
149.88.94.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.110.200	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 1	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.54.52.41	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.65.34	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2423.jpg	Block	1
109.65.10.15	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 5.29.247.168	Block	1
74.82.47.2	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
176.13.20.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
149.88.106.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
5.29.247.168	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Header Line from 5.29.247.168	Block	1

11-03-2015-10:04:00 to 11-03-2015-11:04:00