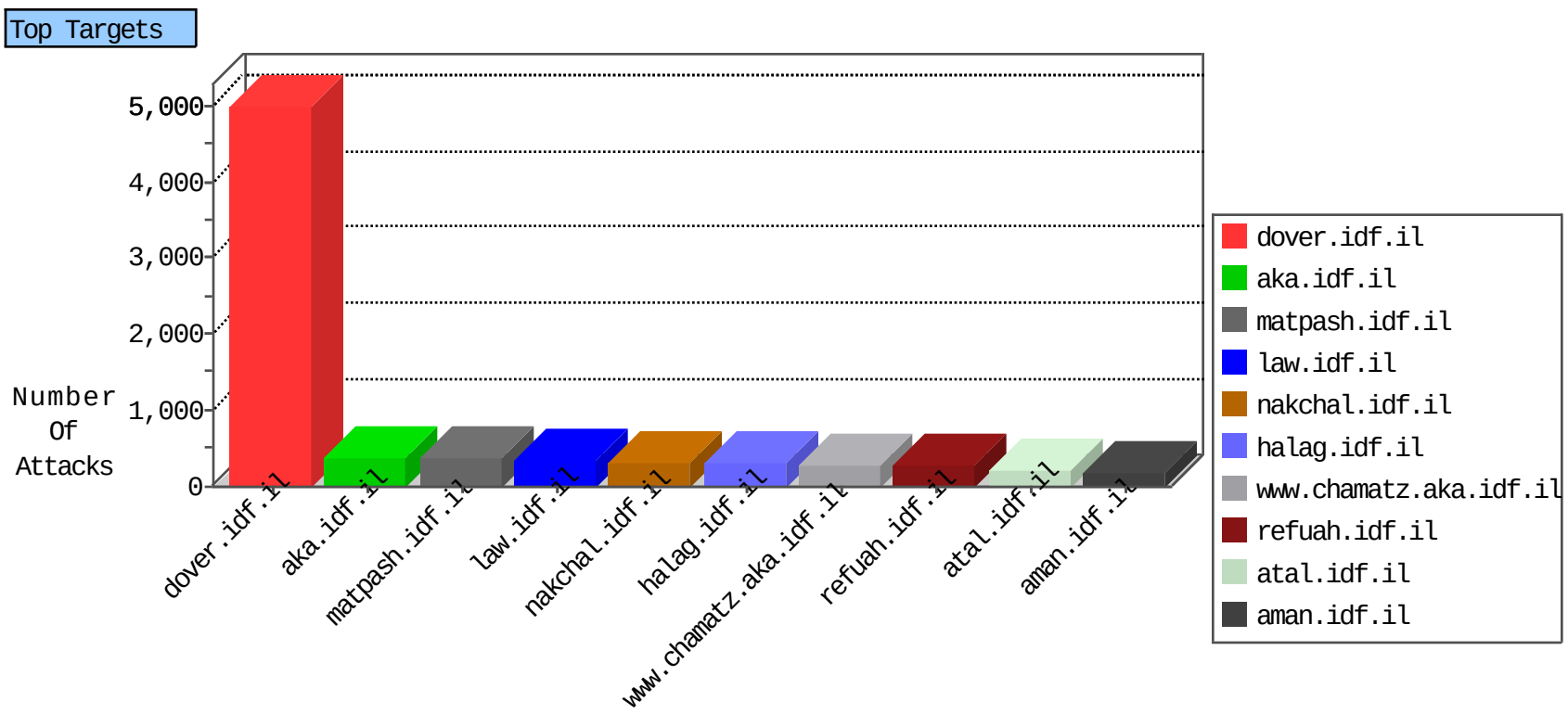
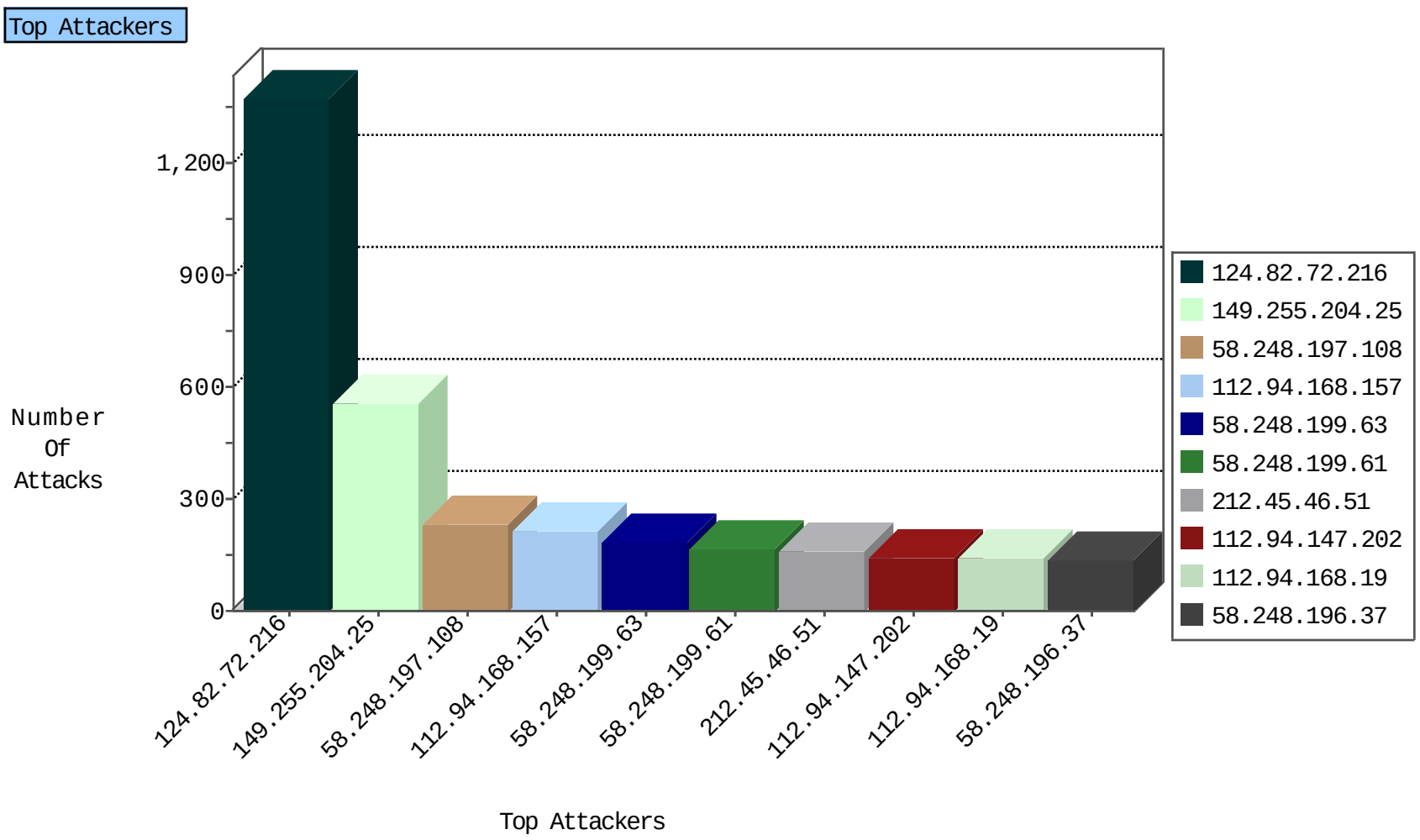
10-25-2015-18:04:06 to 10-25-2015-19:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-18:04:06 to 10-25-2015-19:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.255.204.25	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14426
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	292
149.88.242.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	38
2.52.187.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
46.121.209.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
185.120.126.65		147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
62.0.53.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
79.176.178.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
62.219.151.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
67.82.250.63	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
176.228.34.21	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
94.230.86.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
81.218.208.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.179.27.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
94.230.86.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.86.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
185.32.179.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.178.197.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.64.128.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
5.29.177.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.13.20.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.103.206.117	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.147.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.219.151.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.121.79.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.178.197.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
176.13.0.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.64.182.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.102.8.157	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.15.8.46	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	5
185.7.120.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.46.37.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.190.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
89.138.216.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.12.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.126.165.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
95.86.118.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.116.149.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.183.28.52	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.65.135.21	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
77.127.67.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.179.138.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.162.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
201.37.161.221	Brazil	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.228.34.21	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
79.176.129.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
85.250.56.255	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.149.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.176.174.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
82.80.135.16	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-25-2015-18:04:06 to 10-25-2015-19:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.41.125.22	Ireland	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1

10-25-2015-18:04:06 to 10-25-2015-19:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
58.248.197.74	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.162.116.221	147.237.77.170	Sweden	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
205.203.135.1	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.79.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.32.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.156.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.247.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
86.169.17.34	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.174.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.37.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.162.116.221	147.237.77.235	Sweden	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.162.116.221	147.237.77.61	Sweden	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
188.120.148.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.158.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.44.137.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.43.200.179	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.30.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.63.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.186.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.148.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-25-2015-18:04:06 to 10-25-2015-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.255.204.25	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	551
212.45.46.51	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	161
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
99.226.181.87	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
46.117.67.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
2.54.49.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
74.101.220.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
74.66.68.6	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
83.81.95.0	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
82.166.20.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
100.100.33.111		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	42
176.13.20.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
73.4.70.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
100.100.110.138		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	37
5.22.131.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.26.147.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
2.54.12.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
124.82.72.216	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.54.162.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.132.221.176	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
100.100.2.255		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
212.179.42.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
176.13.4.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
2.103.206.117	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
79.178.102.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
100.100.118.178		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.86.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
46.121.209.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.13.22.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
149.88.242.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.120.160.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
100.100.112.18		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	17
189.148.191.56	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
177.185.92.74	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.179.27.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.116.194.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.47.41.184	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.180.184.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.116.190.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.64.102.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

10-25-2015-18:04:06 to 10-25-2015-19:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
124.82.72.216	Malaysia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	1341
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	84
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
79.181.8.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	42
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.aspx	Block	42
58.248.199.63	China	147.237.76.31	nakchal.idf.il	Distributed Illegal HTTP Version	Block	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	28
58.248.199.61	China	147.237.76.31	nakchal.idf.il	Distributed Illegal Byte Code Character in Method	Block	28
94.153.10.149	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 94.153.10.149	Block	28
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
68.197.38.81	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 68.197.38.81	Block	28
58.248.199.61	China	147.237.76.31	nakchal.idf.il	Distributed NULL Character in Method	Block	24
58.248.196.37	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#0]][[#0]]S[[#1]][[#0]][[#0]]O[[#3]][[#0]]?GÃ–Ã·Â°,Ã®ÃªÂ²`~Ã³[[#0]]Ã½Â,{Â¹Ã•Â–Ã^wÂ›Ã¦Ã„Ã›<=Ã› oÃ¯[[#16]]n[[#0]][[#0]]([[#0]][[#22]][[#0]][[#19]][[#0]] in URL	Block	14
58.248.199.63	China	147.237.77.74	law.idf.il	Distributed NULL Character in Header Name	Block	14
112.94.149.158	China	147.237.76.200	eitan.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	14
218.107.22.202	China	147.237.77.176	matpash.idf.il	Distributed NULL Character in Method	Block	14
58.248.197.108	China	147.237.77.226	www.chamatz.aka.idf.il	Distributed NULL Character in Method	Block	14
109.67.68.148	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
112.94.173.29	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	14
84.109.39.134	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
112.94.168.157	China	147.237.77.234	halag.idf.il	Distributed Illegal Byte Code Character in Method	Block	14
46.120.202.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
58.248.199.61	China	147.237.77.235	sviva.idf.il	Distributed Unauthorized URL Access on /	Block	14
112.94.147.202	China	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in Method	Block	14
218.107.21.236	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	14
58.248.197.82	China	147.237.77.19	law-forum.idf.il	Distributed Illegal Byte Code Character in Method	Block	14
66.249.93.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
112.94.168.19	China	147.237.77.233	atal.idf.il	NULL Character in Method	Block	14
58.248.199.61	China	147.237.76.31	nakchal.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	14
112.94.146.144	China	147.237.77.176	matpash.idf.il	Distributed NULL Character in Method	Block	14
112.94.185.194	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	14
58.248.198.111	China	147.237.76.42	refuah.idf.il	Distributed Illegal HTTP Version	Block	14
112.94.145.0	China	147.237.76.200	eitan.aka.idf.il	Distributed NULL Character in Method	Block	14
112.94.174.82	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	14
58.248.197.74	China	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in Method	Block	14
64.41.200.101	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unsupported Legacy SSL Version	None	14
112.94.150.57	China	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on /	Block	14
112.94.148.215	China	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /nice ports,/trinity.txt.bak	Block	14
85.65.11.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
112.94.168.157	China	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Header Name	Block	14
58.248.196.37	China	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	14
58.248.199.63	China	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	14
5.29.165.3	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
112.94.147.202	China	147.237.76.200	eitan.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	14
207.46.13.35	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/general/eitan.aspx	Block	14
58.248.197.108	China	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on /	Block	14
68.197.38.81	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/	Block	14
112.94.168.157	China	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in Method	Block	14
58.248.197.74	China	147.237.77.235	sviva.idf.il	Distributed Unauthorized URL Access on /	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14

10-25-2015-18:04:06 to 10-25-2015-19:04:06