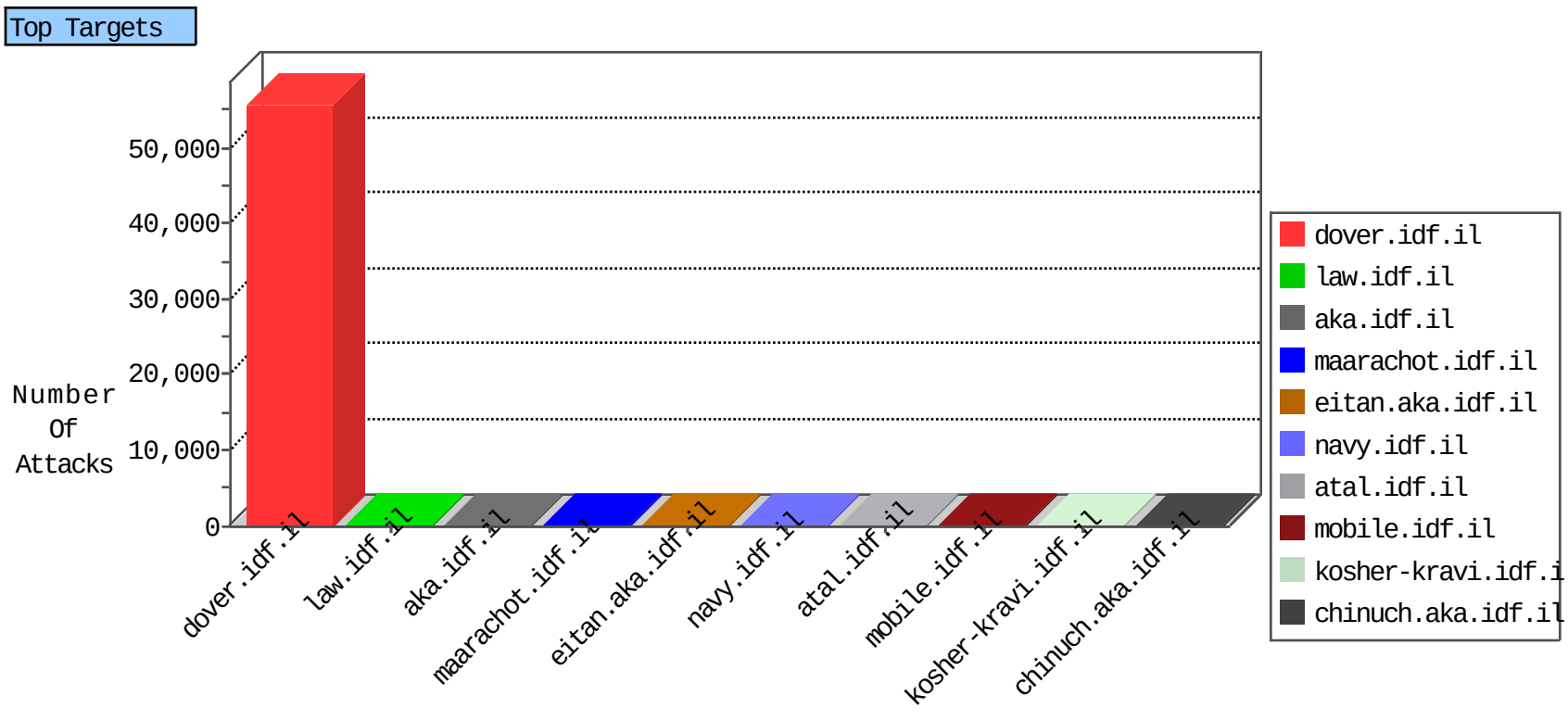
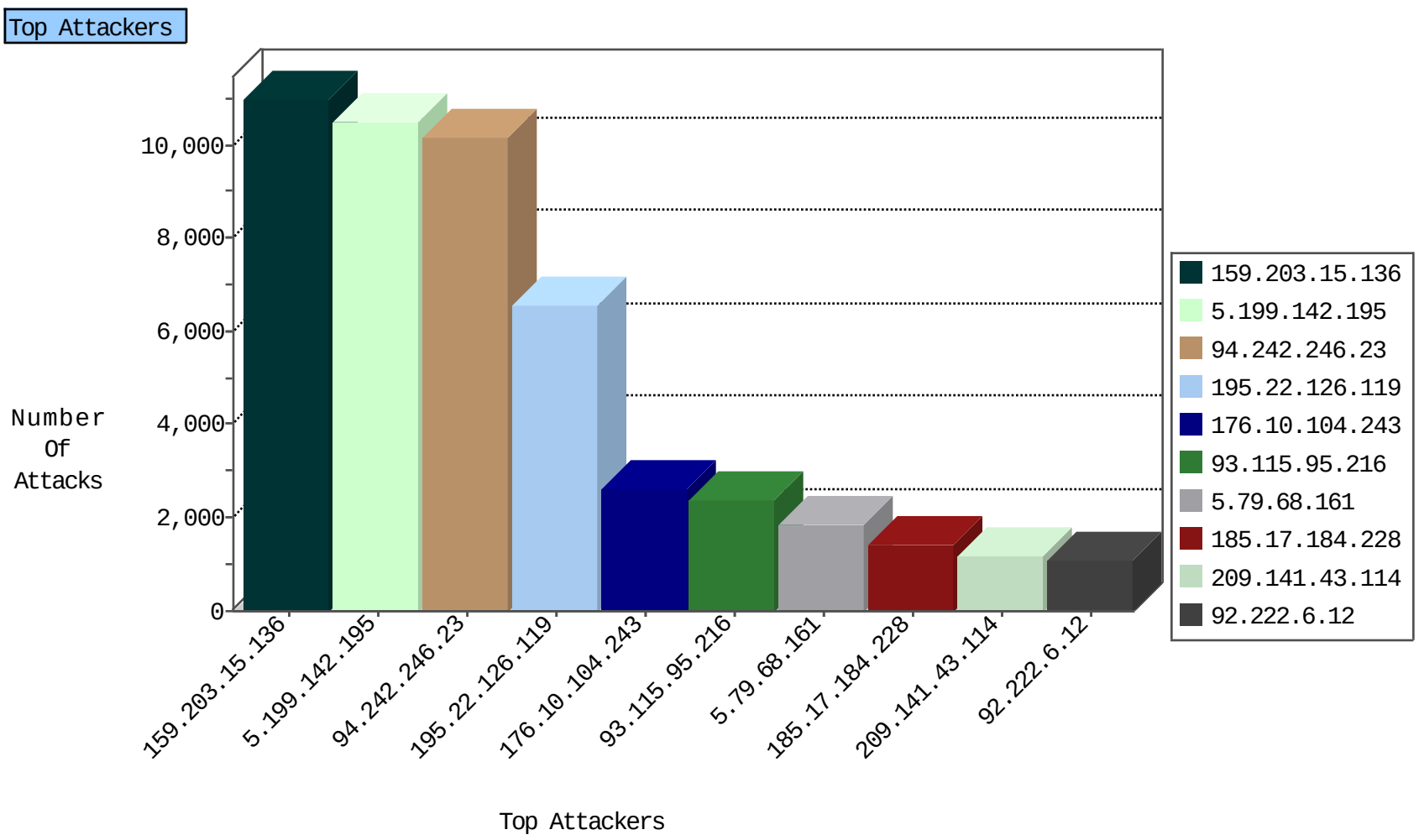
04-23-2016-07:04:05 to 04-23-2016-08:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-23-2016-07:04:05 to 04-23-2016-08:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	14286
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6347
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3909
0.0.0.0		147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	3342
67.225.75.74	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3171
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3093
192.241.232.57	United States	147.237.77.216	dover.idf.il	DOS-WEB-HULK-improved	forward	1307
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	1176
159.203.15.136	Canada	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	962
66.249.78.60	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	863
159.203.15.136	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	667
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	464
199.127.226.150	United States	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	292
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	232
92.222.6.12	Germany	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	130
79.17.87.4	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	87
159.203.15.136	Canada	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	dest-reset	65
79.98.107.90	Bulgaria	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	49
109.163.234.8	Romania	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	40
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	31
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	19
195.154.56.44	France	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
5.199.142.195	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
92.222.6.12	Germany	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
5.199.142.195	Germany	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
92.222.6.12	Germany	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
5.199.142.195	Germany	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
185.17.184.228	Netherlands	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
89.46.102.242	Romania	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.29.8.132	Sweden	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
195.22.126.119	Poland	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
89.46.102.242	Romania	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.103.252.98	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
94.155.49.47	Bulgaria	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
185.103.252.98	Russian Federation	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

04-23-2016-07:04:05 to 04-23-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-07:04:05 to 04-23-2016-08:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.115.95.216	147.237.77.216	Anonymous Proxy	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	14
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.138.25.228	147.237.0.15	France	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
188.138.25.228	147.237.0.15	France	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5800-5820	2
66.249.78.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
114.35.1.36	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.192.0.19	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
104.171.122.176	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 3072	1
197.231.221.211	147.237.77.216	Liberia	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
185.17.184.228	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
112.124.10.141	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.19	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
202.170.80.40	147.237.76.177	Mongolia	ncore.idf.il	ET SCAN Potential SSH Scan	1
5.199.142.195	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
195.81.248.101	147.237.0.15	United Kingdom	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
195.22.126.119	147.237.77.216	Poland	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1

04-23-2016-07:04:05 to 04-23-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
159.203.15.136	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10611
5.199.142.195	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10406
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10095
195.22.126.119	Poland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6487
176.10.104.243	Switzerland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	2256
5.79.68.161	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1857
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1814
185.17.184.228	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1353
209.141.43.114	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1165
77.247.181.162	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1040
92.222.6.12	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	944
185.29.8.132	Sweden	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	839
94.155.49.47	Bulgaria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	839
198.134.125.78	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	559
85.25.103.119	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	538
199.127.226.150	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	248
82.102.251.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	227
79.98.107.90	Bulgaria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	216
197.231.221.211	Liberia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	125
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
109.163.234.8	Romania	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	99
64.62.219.156	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	99
185.17.184.228	Netherlands	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	61
185.29.8.132	Sweden	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	53
212.47.238.193	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
139.162.216.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
52.29.223.39	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
93.115.95.201	Anonymous Proxy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
78.249.30.40	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
67.225.75.74	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
69.30.234.186	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
197.231.221.211	Liberia	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
100.13.30.121	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
68.180.231.43	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
207.46.13.192	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	23
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
195.154.56.44	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
136.243.5.203	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
136.243.5.87	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
40.77.167.52	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	310
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	71
5.199.142.195	Germany	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	59
94.155.49.47	Bulgaria	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	54
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 197.231.221.211	Block	54
195.22.126.119	Poland	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	52
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	38
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	35
185.17.184.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	18
5.199.142.195	Germany	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	18
94.155.49.47	Bulgaria	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	14
5.199.142.195	Germany	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	10
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Query String from 197.231.221.211	Block	9
195.22.126.119	Poland	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	9
5.199.142.195	Germany	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	8
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Parameter Value from 197.231.221.211	Block	8
94.155.49.47	Bulgaria	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	7
94.155.49.47	Bulgaria	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	7
195.22.126.119	Poland	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	6
185.17.184.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	4
195.22.126.119	Poland	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	4
185.17.184.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	4
104.236.60.186	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 104.236.60.186	Block	3
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Parameter Name from 197.231.221.211	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.248.160.136	Netherlands	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 89.248.160.136	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
104.236.60.186	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/kapatz/default.aspx	Block	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
89.248.160.136	Netherlands	147.237.77.176	matpash.idf.il	Illegal HTTP Version	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
165.234.191.224	United States	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9688-he/refuah.aspx	Block	1
89.248.160.136	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version	Block	1
93.173.249.118	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	1
80.246.133.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/statistics/chrono3.stm</i>	Block	1
93.173.249.118	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/	Block	1
89.248.160.136	Netherlands	147.237.0.15	kosher-kravi.idf.il	Illegal HTTP Version	Block	1
64.62.219.156	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
199.30.25.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-23-2016-07:04:05 to 04-23-2016-08:04:05