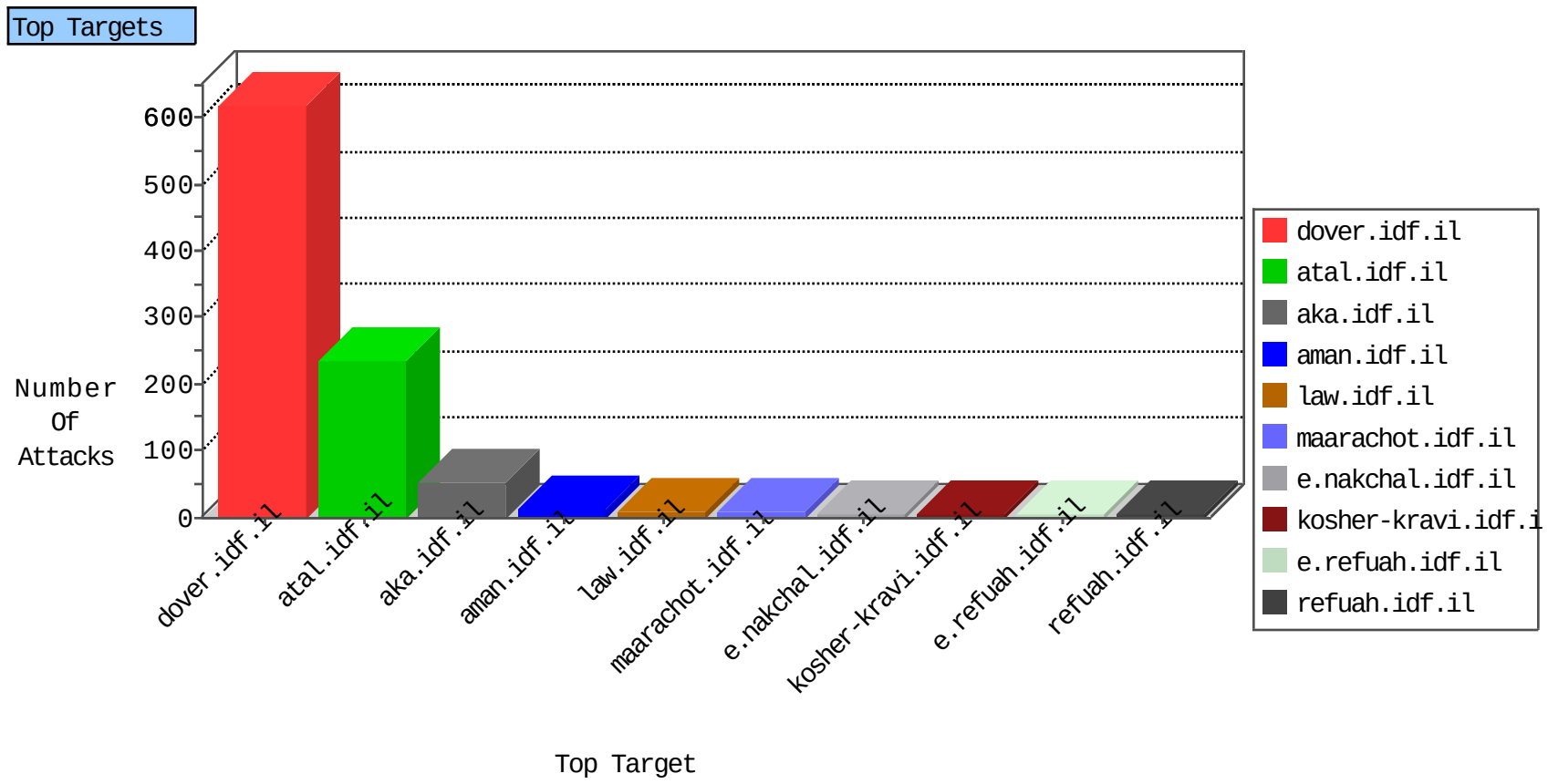
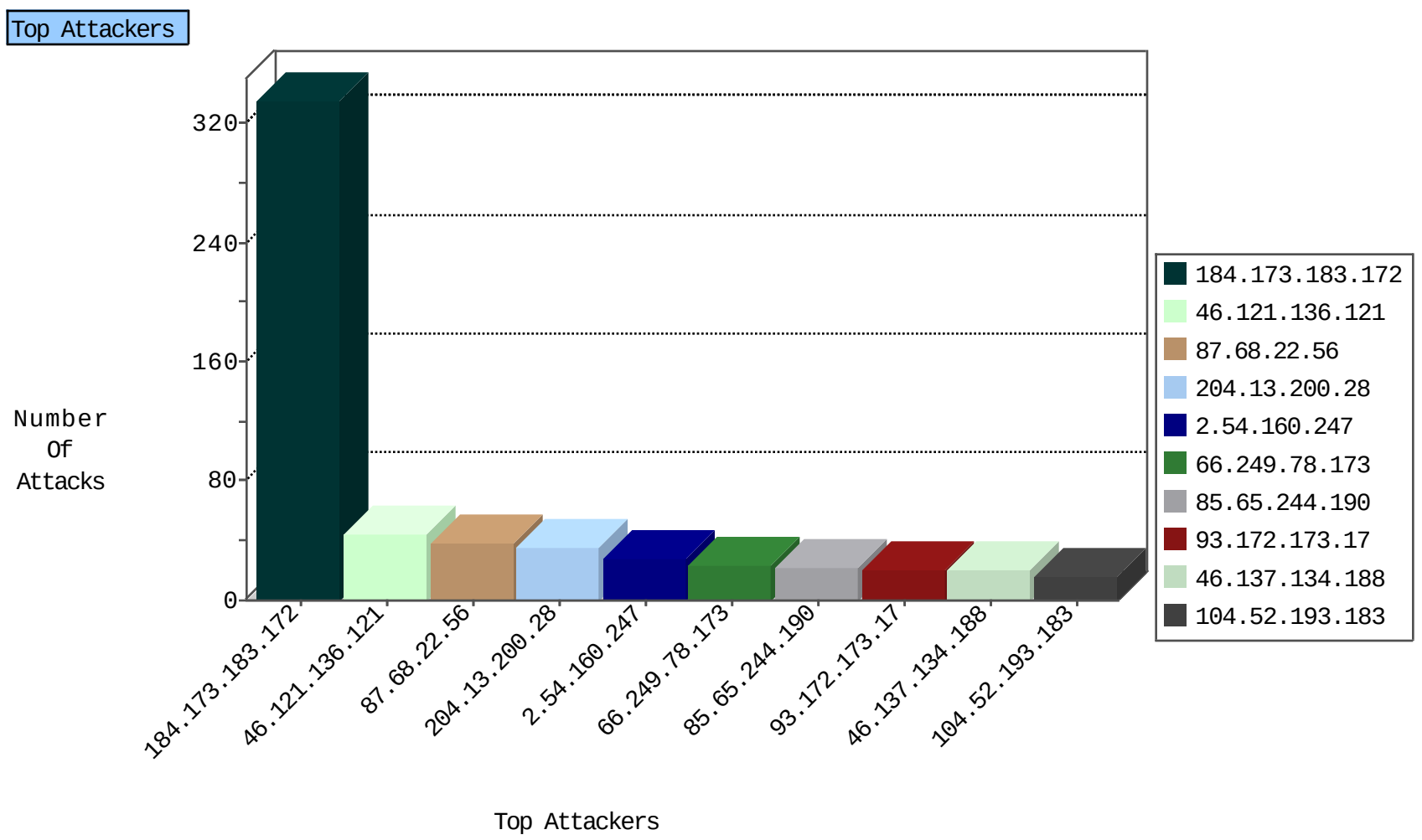
04-20-2015-05:03:09 to 04-20-2015-06:03:09

IDF Under Attack
04-20-2015-05:03:09

Top Targets



Top Attackers



04-20-2015-05:03:09 to 04-20-2015-06:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	207
204.13.200.28	United States	147.237.72.166	aka.idf.il	Frk_Under_Attack_Con_Https	drop	2
221.7.168.18	China	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
38.229.1.13	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
124.232.142.220	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
178.162.201.166	Germany	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
124.232.142.220	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

04-20-2015-05:03:09 to 04-20-2015-06:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	205
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	131
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1

04-20-2015-05:03:09 to 04-20-2015-06:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
180.76.6.16	China	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
58.20.54.249	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
177.148.168.71	Brazil	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
213.182.43.222	France	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
177.148.168.71	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.182.43.222	France	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
177.148.168.71	Brazil	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.184.217.221	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.49	Ukraine	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	India	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
201.231.105.189	Argentina	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
201.231.105.189	Argentina	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
177.148.168.71	Brazil	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
58.20.54.249	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
177.148.168.71	Brazil	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
213.182.43.222	France	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
177.148.168.71	Brazil	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.184.217.221	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
104.155.216.239		147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
208.184.217.221	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
202.71.25.29	India	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
201.231.105.189	Argentina	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	United States	147.237.76.177	ncore.idf.il	ET DROP Dshield Block Listed Source	1
61.240.144.65	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

04-20-2015-05:03:09 to 04-20-2015-06:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.121.136.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
204.13.200.28	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	33
87.68.22.56	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	29
2.54.160.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
85.65.244.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
93.172.173.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
104.52.193.183		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
5.102.204.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
140.228.147.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
219.113.243.170	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
119.73.253.4	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
118.46.152.52	Korea, Republic of	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
174.6.36.154	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
220.255.1.125	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
87.68.22.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
124.6.181.36	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
5.102.254.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
46.19.86.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
1.136.96.119	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
65.19.138.34	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.116.187.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.82.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
59.167.118.165	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
79.179.172.33	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
190.225.0.57	Argentina	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
119.73.170.114	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
2.52.182.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
220.255.1.43	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
84.109.215.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
76.187.51.207	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
220.255.1.149	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
77.75.77.11	Czech Republic	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
66.249.82.210	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
220.255.1.119	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
65.19.138.33	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
84.228.124.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
134.249.53.8	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
188.138.17.205	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
77.75.77.11	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyius	Block	1
207.46.13.143	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
136.243.36.88	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/	Block	1
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
195.159.233.44	Norway	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 195.159.233.44 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
82.80.59.150	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/contact/contact.asp	Block	1
155.94.254.143		147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
195.159.233.44	Norway	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
87.68.22.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1770-he/refuah.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×ž×™×œ×•×?×™ ×?/contact/	Block	1
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22089-	Block	1
101.30.232.217	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx/trackback/	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
74.82.47.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18063-he/dover.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/300900_riot.stm	Block	1