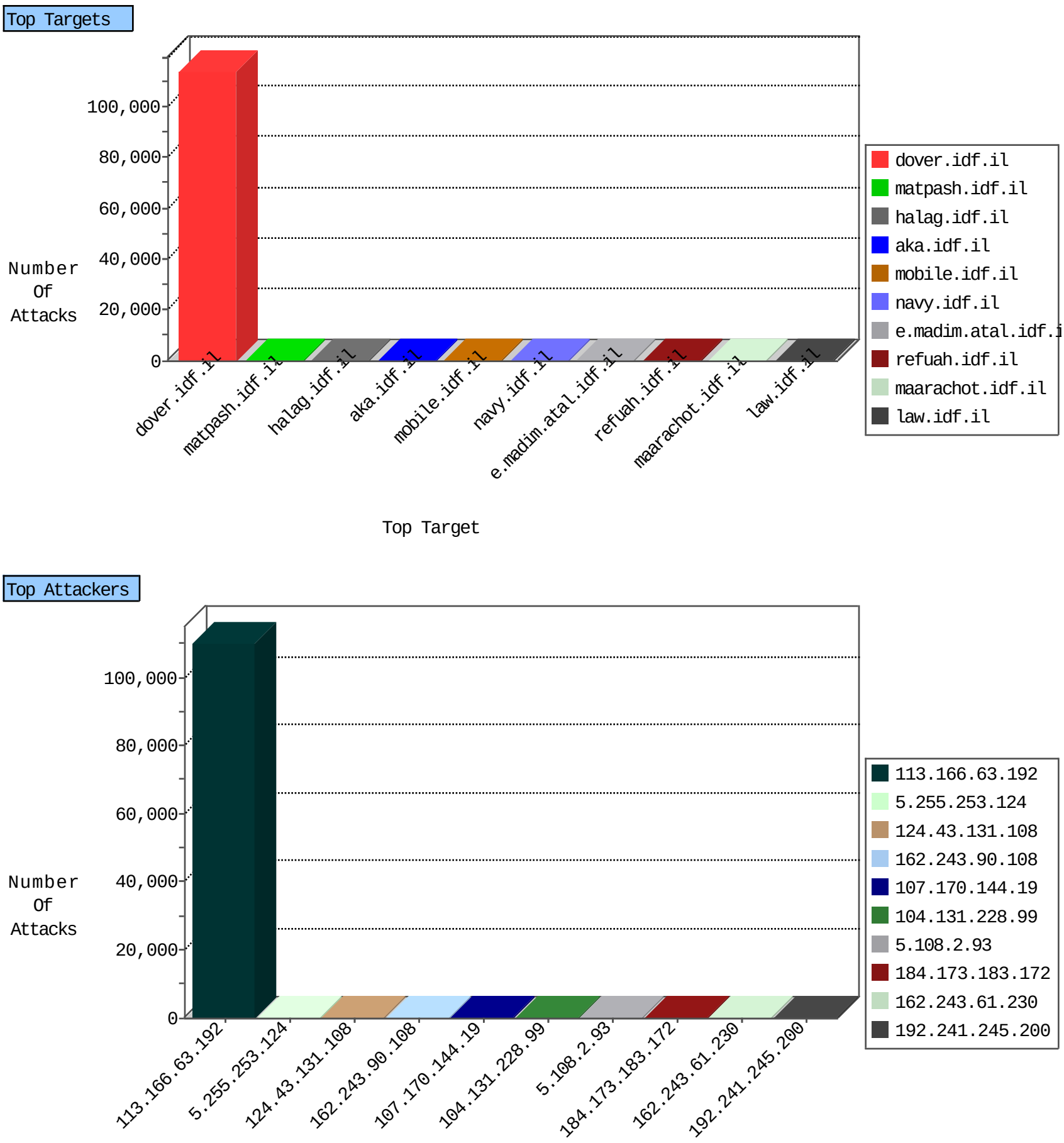
04-21-2015-02:12:16 to 04-21-2015-03:12:16

IDF Under Attack
04-21-2015-02:12:16



04-21-2015-02:12:16 to 04-21-2015-03:12:16

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.155	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2815
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	547
220.181.108.116	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	421
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	184
116.225.83.168	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
46.19.85.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-21-2015-02:12:16 to 04-21-2015-03:12:16

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	166
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	2
213.57.63.14	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.8.46	e.chinuch.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
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.217	e.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
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1

04-21-2015-02:12:16 to 04-21-2015-03:12:16

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
211.68.127.29	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
66.249.83.194	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
211.68.127.29	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.20	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
122.228.207.77	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
213.182.43.222	France	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.77	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.20	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
213.182.43.222	France	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
122.228.207.77	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1

04-21-2015-02:12:16 to 04-21-2015-03:12:16

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
113.166.63.192	Vietnam	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	110140
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	406
124.43.131.108	Sri Lanka	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	298
162.243.90.108	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	284
107.170.144.19	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	250
104.131.228.99		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	240
5.108.2.93	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	238
162.243.61.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	128
192.241.245.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	126
87.69.244.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	125
173.208.169.226	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	116
162.243.210.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	107
68.64.172.118	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	102
192.68.112.171	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
119.252.233.34	Papua New Guinea	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
162.230.61.94	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.67.104	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
95.144.186.103	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
91.61.79.33	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.83.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
24.60.206.193	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.85.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
78.250.152.29	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.85.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.67.112	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
213.149.104.52		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
75.80.164.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
50.138.196.152	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
24.17.204.144	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
157.55.39.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
85.130.138.149	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
184.153.54.171	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.108.4.28	Israel	147.237.77.243	mobile.idf.i	First packet isn't SYN	drop	drop	7
177.32.239.241	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.76.108.210	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
84.109.106.152	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
213.57.63.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	2
95.173.171.224	Turkey	147.237.72.156	aman.idf.il	Illegal HTTP Version	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/m/	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
157.55.39.252	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.65.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/august/15.stm	Block	1
66.249.64.57	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/ajax/setivgallerycontrol.aspx	Block	1
66.249.67.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
31.13.112.119	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/3	Block	1
94.153.8.126	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.64.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1