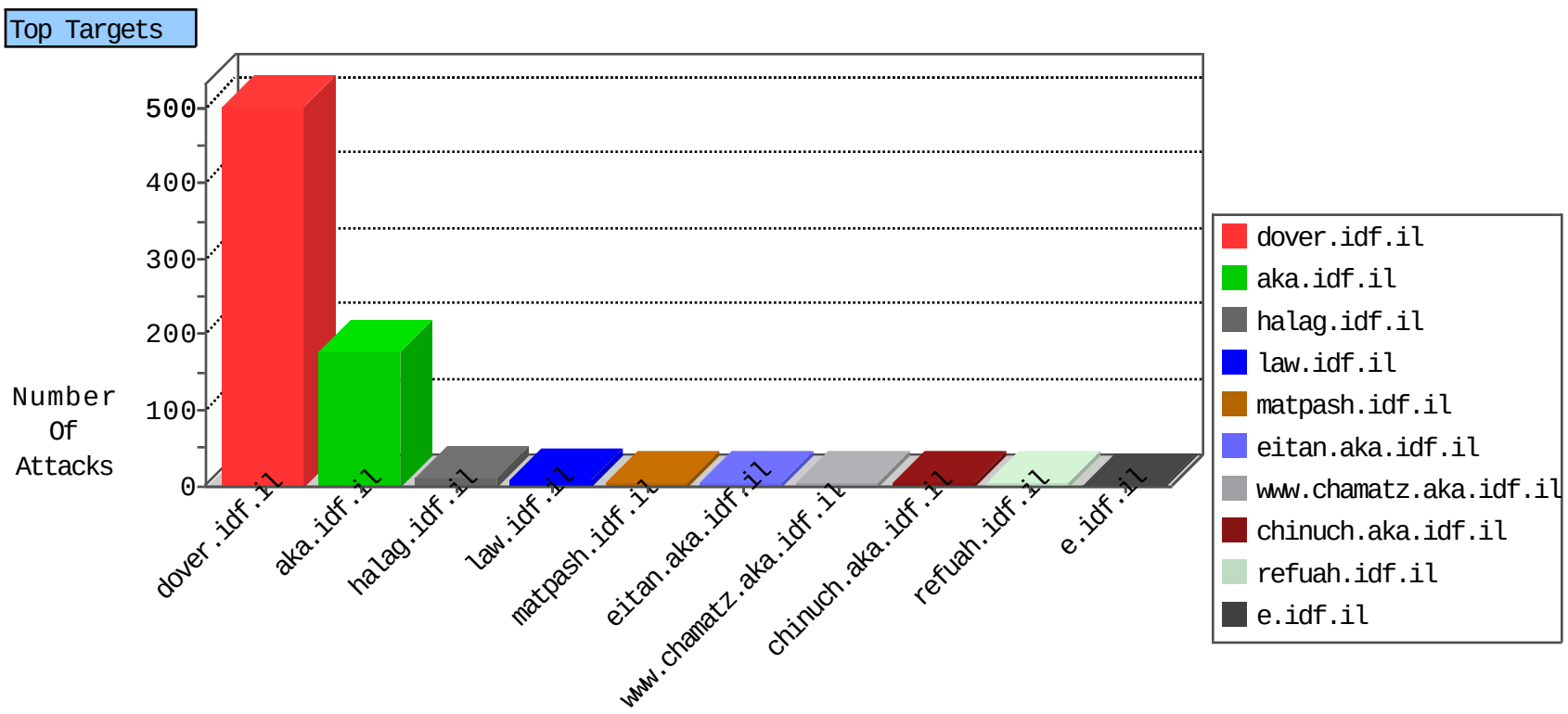
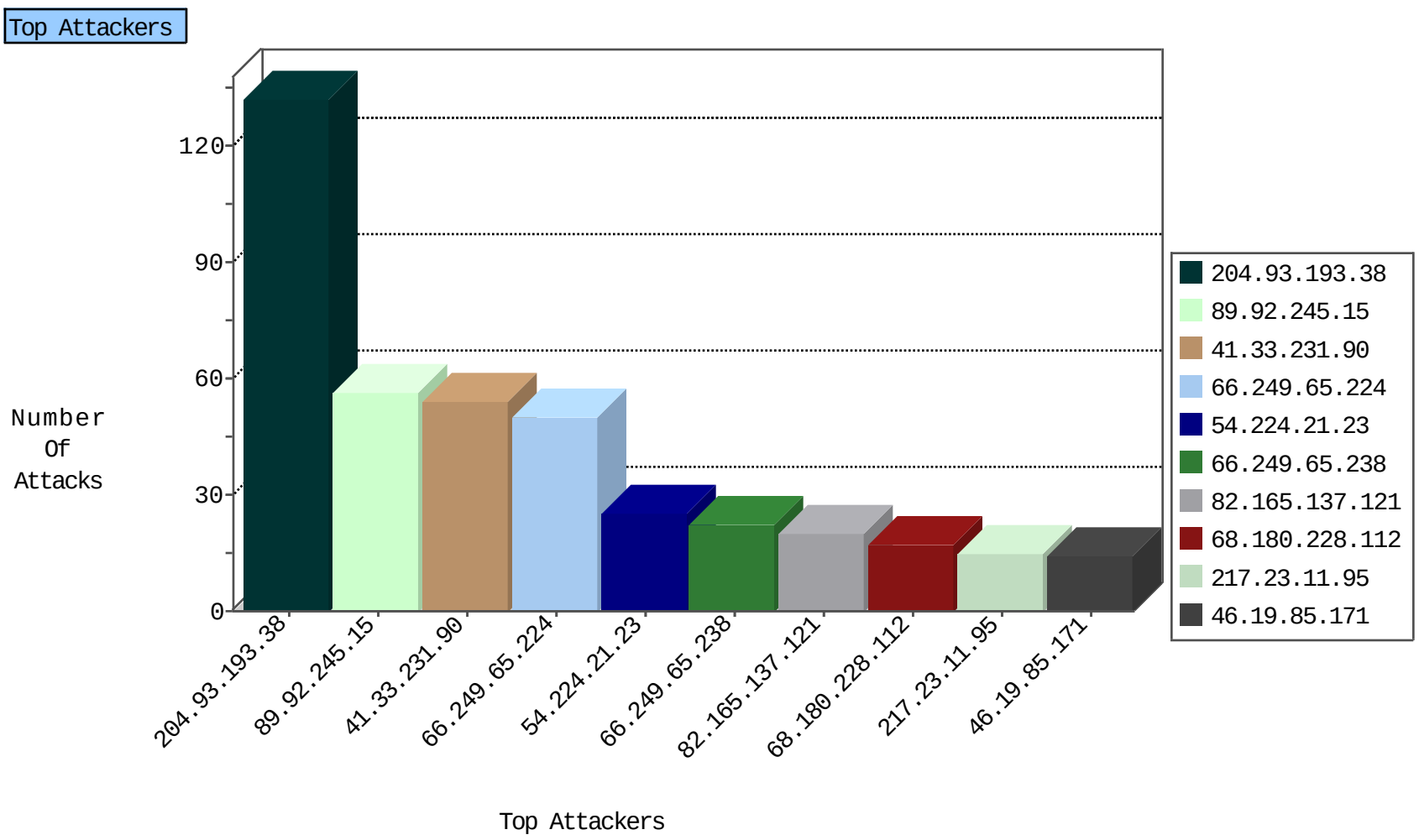
11-21-2015-02:04:02 to 11-21-2015-03:04:02

IDF Under Attack Daily Report





11-21-2015-02:04:02 to 11-21-2015-03:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3587
204.93.154.211	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	17
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
115.231.222.40	China	147.237.76.200	eitan.aka.idf.i	JLM_Under_Attack_Con_Http	drop	2
176.123.29.54	Moldova, Republic of	147.237.76.200	eitan.aka.idf.i	Block_Ntp_All_Net	drop	1
176.123.29.54	Moldova, Republic of	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

11-21-2015-02:04:02 to 11-21-2015-03:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.193.38	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	24
204.93.193.38	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8

11-21-2015-02:04:02 to 11-21-2015-03:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
204.93.193.38	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	100
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.65.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
184.172.196.106	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
109.251.56.171	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.58.47.99	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.58.47.99	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
58.58.47.99	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
58.58.47.99	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
188.214.128.12	147.237.8.28	Romania	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
109.251.56.171	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
58.58.47.99	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
58.58.47.99	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.58.47.99	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
58.58.47.99	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
58.58.47.99	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
188.214.128.12	147.237.77.19	Romania	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1

11-21-2015-02:04:02 to 11-21-2015-03:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.92.245.15	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
82.165.137.121	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
217.23.11.95	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
220.255.97.4	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.82.78.104	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
52.68.136.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.120.160.157	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.168.76.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.34.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
66.249.65.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
116.14.50.100	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.49.224.248		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
173.252.79.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.176.127.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
204.93.154.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
220.255.97.158	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
173.252.79.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.121.116.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
82.166.119.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
66.249.67.122	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
190.234.105.140	Peru	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.16.156.124	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	2
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
173.252.90.229	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

11-21-2015-02:04:02 to 11-21-2015-03:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	9
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	4
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
176.12.137.13	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.54.165.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.178.21.180	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
2.54.41.243	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
150.70.173.42	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.67.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
107.150.43.203	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /	Block	1
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
91.229.77.64	Ukraine	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
2.54.42.220	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
107.150.55.53	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.75.94	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
194.150.168.79	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.67.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.166.186.208	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9694-he/refuah.aspx	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	1
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/	Block	1
5.175.0.137	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.78.137	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/undefined	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
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.178.21.180	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.21.180	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
150.70.173.42	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-21-2015-02:04:02 to 11-21-2015-03:04:02