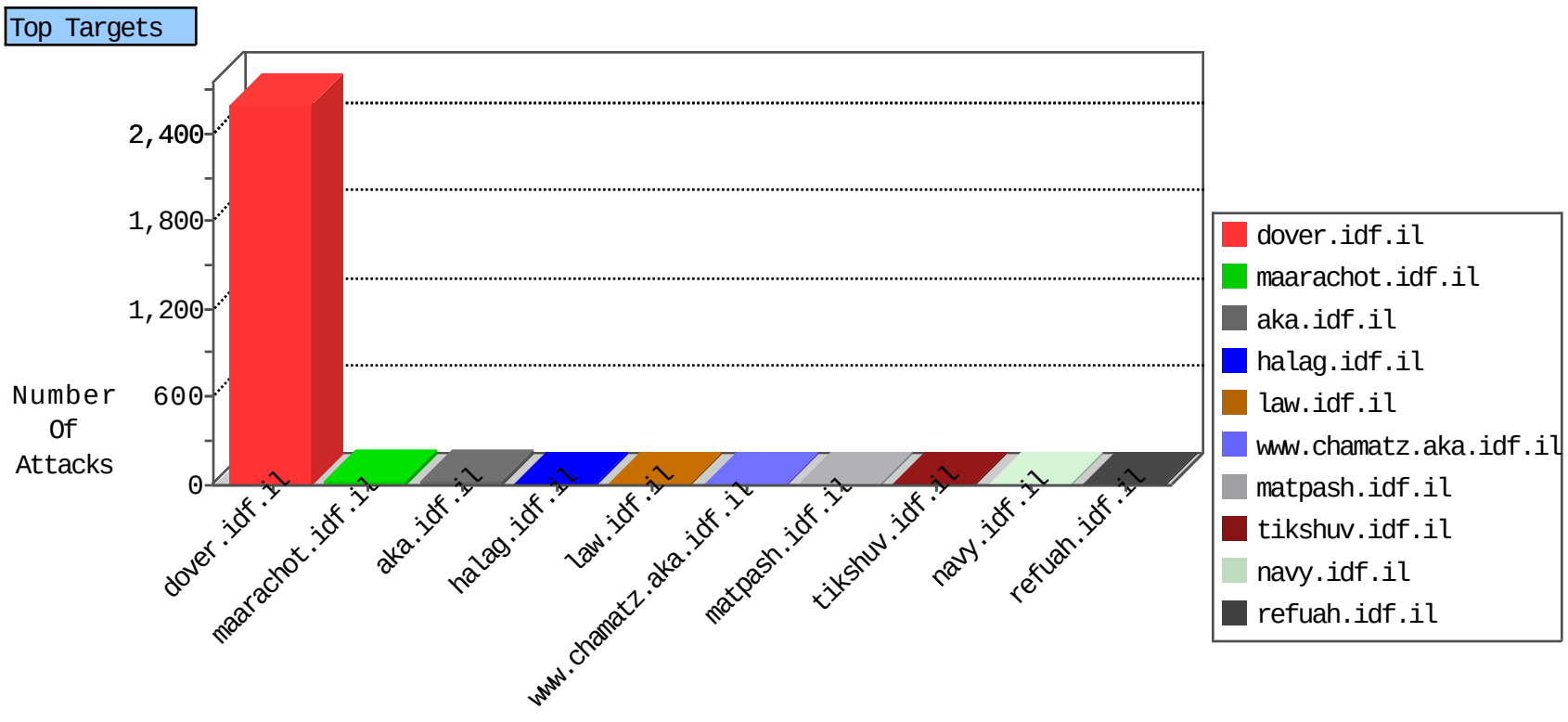
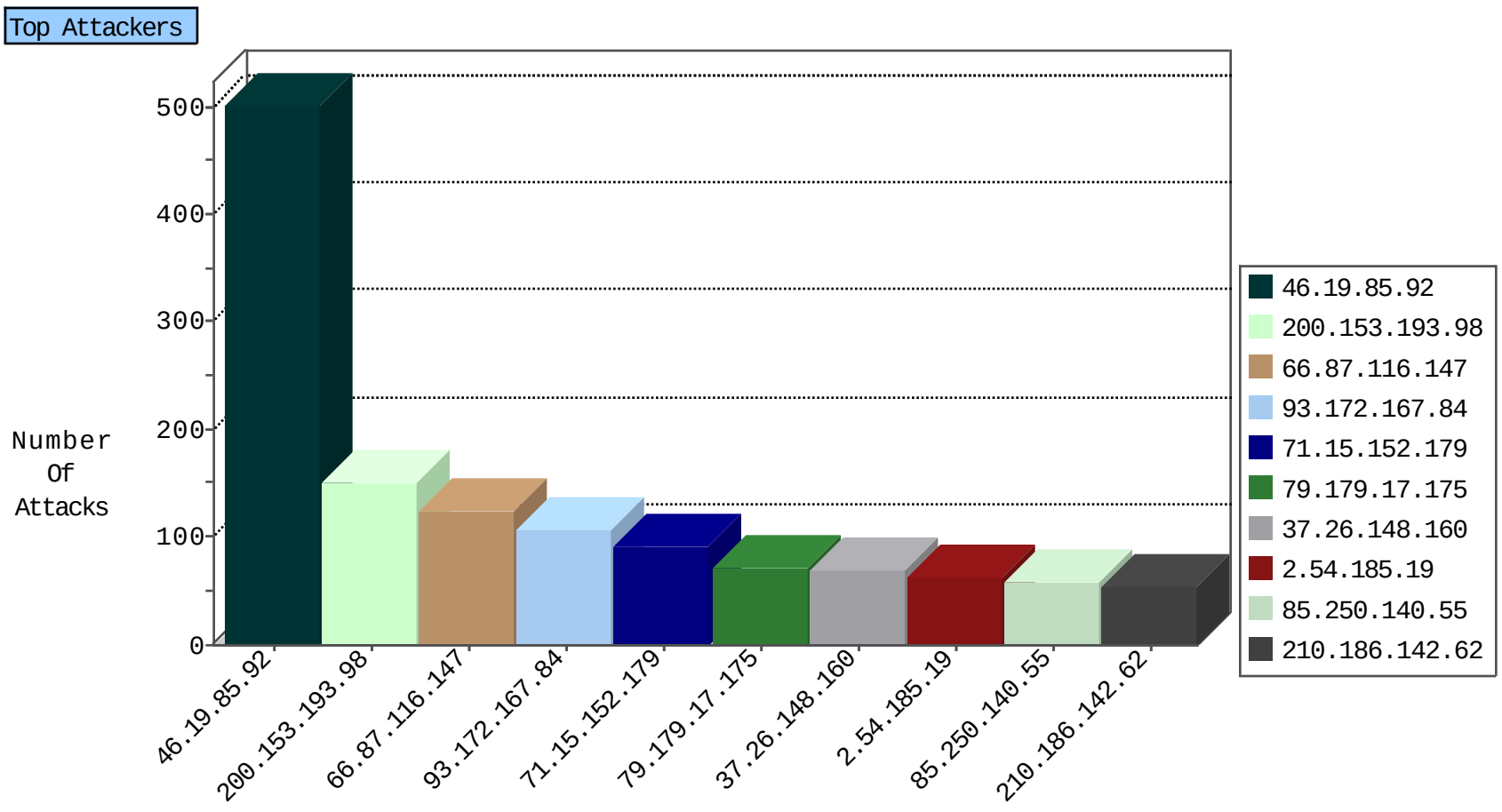
04-19-2015-06:03:06 to 04-19-2015-07:03:06

IDF Under Attack
04-19-2015-06:03:06





04-19-2015-06:03:06 to 04-19-2015-07:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	199
82.102.141.248	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
68.198.118.220	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.246.36.210	Sweden	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

04-19-2015-06:03:06 to 04-19-2015-07:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	8
193.108.195.249	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.148	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
95.139.206.189	Russian Federation	147.237.72.166	aka.idf.il	3617: HTTP: Paros Proxy HTTP Request	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.207	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.61	e.cogat.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
85.25.103.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
41.36.132.192	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1

04-19-2015-06:03:06 to 04-19-2015-07:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	10
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	United States	147.237.76.177	ncore.idf.il	ET DROP Dshield Block Listed Source	1
61.240.144.64	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
188.136.199.244	Iran, Islamic Republic of	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
58.20.54.249	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
101.226.2.99	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
81.200.91.2	Russian Federation	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
101.226.2.99	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
58.20.54.249	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1

04-19-2015-06:03:06 to 04-19-2015-07:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	502
200.153.193.98	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	152
66.87.116.147	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	125
93.172.167.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
71.15.152.179	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	92
79.179.17.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
37.26.148.160	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	70
2.54.185.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
85.250.140.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
62.0.102.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
46.121.244.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
46.19.85.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
109.253.137.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
210.186.142.62	Malaysia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
210.186.142.205	Malaysia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
99.238.35.157	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
68.28.123.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
82.102.141.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
68.198.118.220	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
2.54.39.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
176.12.147.169	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
74.6.254.113	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
2.52.19.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
73.9.29.27	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
64.233.173.151	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
46.19.86.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
62.90.210.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
210.186.142.62	Malaysia	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
109.253.156.103	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.138.100	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
213.151.43.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
62.0.75.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
176.12.136.219	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
46.19.85.36	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	14
93.173.190.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
212.179.23.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
85.65.71.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
64.233.173.161	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.141.44	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
101.57.172.101	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
186.202.153.185	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 186.202.153.185	Block	4
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	3
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
95.173.171.224	Turkey	147.237.77.170	maarachot.idf.il	Illegal HTTP Version	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
207.46.13.22	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/asp/wars.asp	Block	1
176.12.145.151	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
82.102.136.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
188.165.15.27	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.27	Block	1
104.128.144.130		147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
66.249.64.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
183.54.49.234	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 183.54.49.234	Block	1
85.250.86.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
188.165.15.27	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/1226.stm	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
66.249.78.222	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/contactus/contactus.aspx	Block	1
66.249.64.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
2.52.174.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
183.54.49.234	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
87.69.248.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
62.210.136.217	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
193.232.184.141	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
158.222.10.33		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
69.12.66.217	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
5.58.44.153	Ukraine	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
183.207.228.38	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//english/news/grapheat.stm	Block	1
95.58.108.173	Kazakstan	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.mag.idf.il/163-4544-en/patzar.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.16	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
158.222.10.42		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/grapheat.stm	Block	1
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	1
66.249.67.41	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170//	Block	1