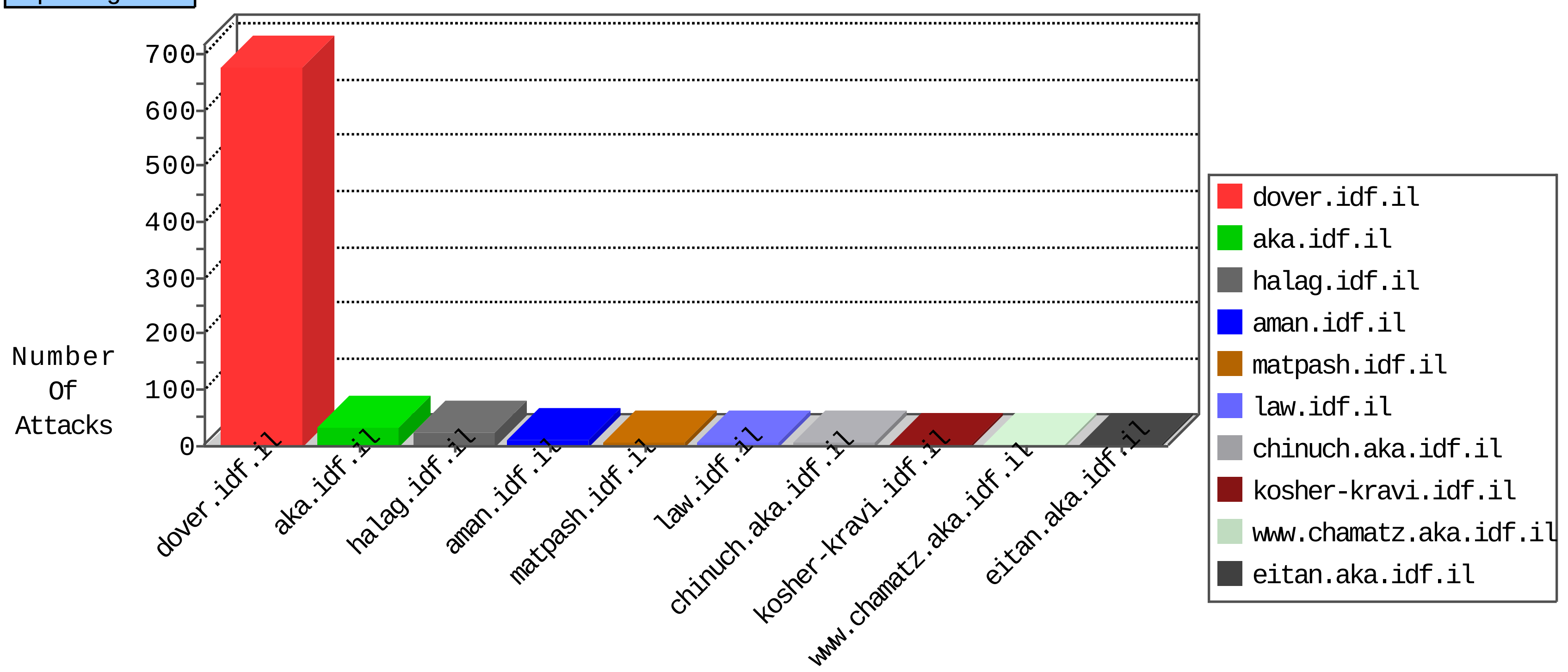
04-30-2015-05:03:04 to 04-30-2015-06:03:04

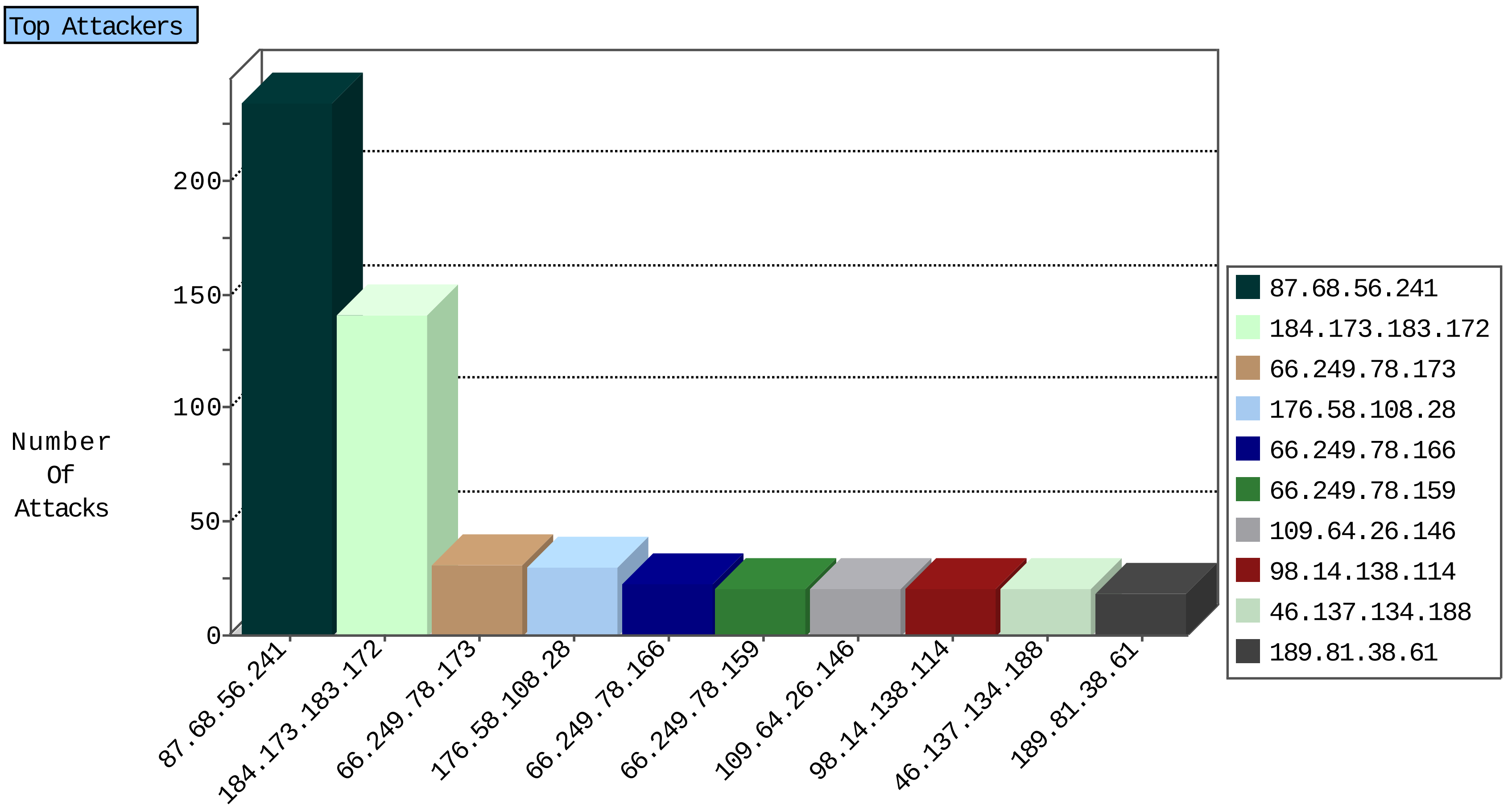
IDF Under Attack
04-30-2015-05:03:04

Top Targets



Top Target

Top Attackers



Top Attackers

04-30-2015-05:03:04 to 04-30-2015-06:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.82	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	761
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
146.185.239.100	Russian Federation	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-30-2015-05:03:04 to 04-30-2015-06:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	141
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
71.6.135.131	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.53	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
108.170.46.170	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.246.115.237	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.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
115.87.162.208	Thailand	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.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
85.25.103.50	Germany	147.237.76.38	e.e.meitav.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
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
161.253.17.2	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1

04-30-2015-05:03:04 to 04-30-2015-06:03:04

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
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
107.6.130.113	United States	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.188.250	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
173.208.188.250	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
111.203.22.56	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
173.208.188.250	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
111.203.22.57	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1

04-30-2015-05:03:04 to 04-30-2015-06:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
87.68.56.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	233
176.58.108.28	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.64.26.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
189.81.38.61	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
66.249.78.51	United States	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.78.37	United States	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.64.76	Israel	147.237.77.216	dover.idf.i	SAM rule	drop	drop	7
207.46.13.92	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
164.215.110.4	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
98.14.138.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
149.88.181.26	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
98.14.138.114	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	5
98.14.138.114	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
66.249.78.44	United States	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
98.14.138.114	United States	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	4
186.80.205.47	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
207.46.13.27	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
62.210.75.104	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
184.160.234.112	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
176.12.142.87	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.64.44	United States	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
173.209.211.244	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
67.243.8.13	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
157.55.39.10	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
84.108.191.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
188.165.15.195	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
87.68.56.241	Israel	147.237.77.216	dover.idf.i	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	2
74.6.254.113	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
109.67.20.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.79.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
192.241.245.200	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
46.19.85.56	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	1
76.4.246.217	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
66.249.88.232	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
207.46.13.27	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.200.12.61	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1465-he/refuah.aspx	Block	1
189.245.48.23	Mexico	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
157.55.39.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/feed/	Block	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
176.10.104.227	Switzerland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-en/	Block	1
46.116.81.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	1
66.249.78.215	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/997-he/atal.aspx	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.66.121.237	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info07.stm	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
180.76.4.58	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	1
66.249.79.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
157.55.39.176	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ie-index05.stm	Block	1
184.105.139.67	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-18773-en/dover.aspx	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/&sa=u&ei=zqsutjfxmn-fopdm-pkb&ved=0cauqfjaa&usg=afqjcnf2apehywz9apusaqdzaz5_jkfq7g	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
157.55.39.237	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
103.50.88.31		147.237.77.216	dover.idf.il	Unauthorized HTTP Method	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
66.249.67.84	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
184.105.139.68	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
157.55.39.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-13102-en/dover.aspx forcerecrawl: 0	Block	1
69.30.240.46	United States	147.237.77.19	law-forum.idf.il	Illegal HTTP Version	Block	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
176.10.104.227	Switzerland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 176.10.104.227	Block	1