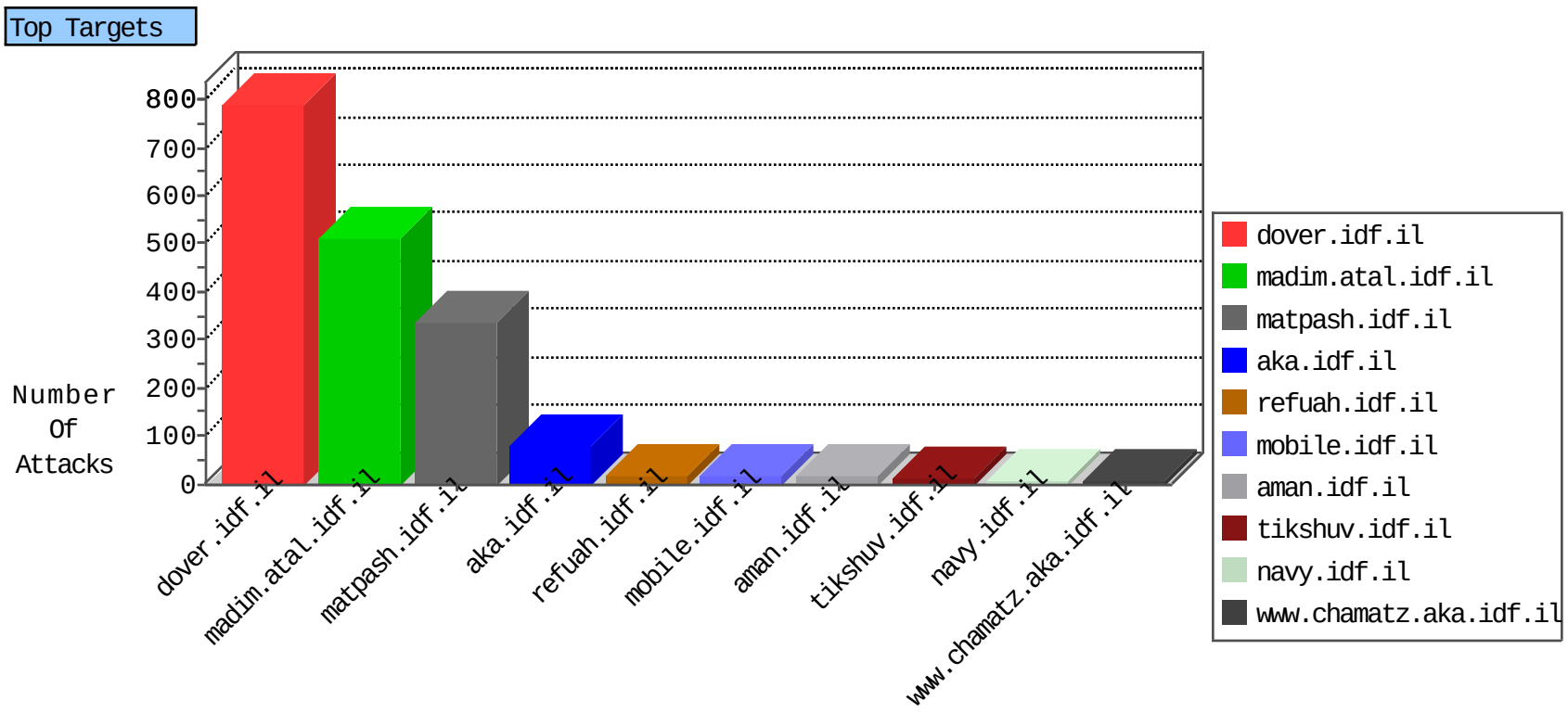
05-09-2015-17:03:07 to 05-09-2015-18:03:07

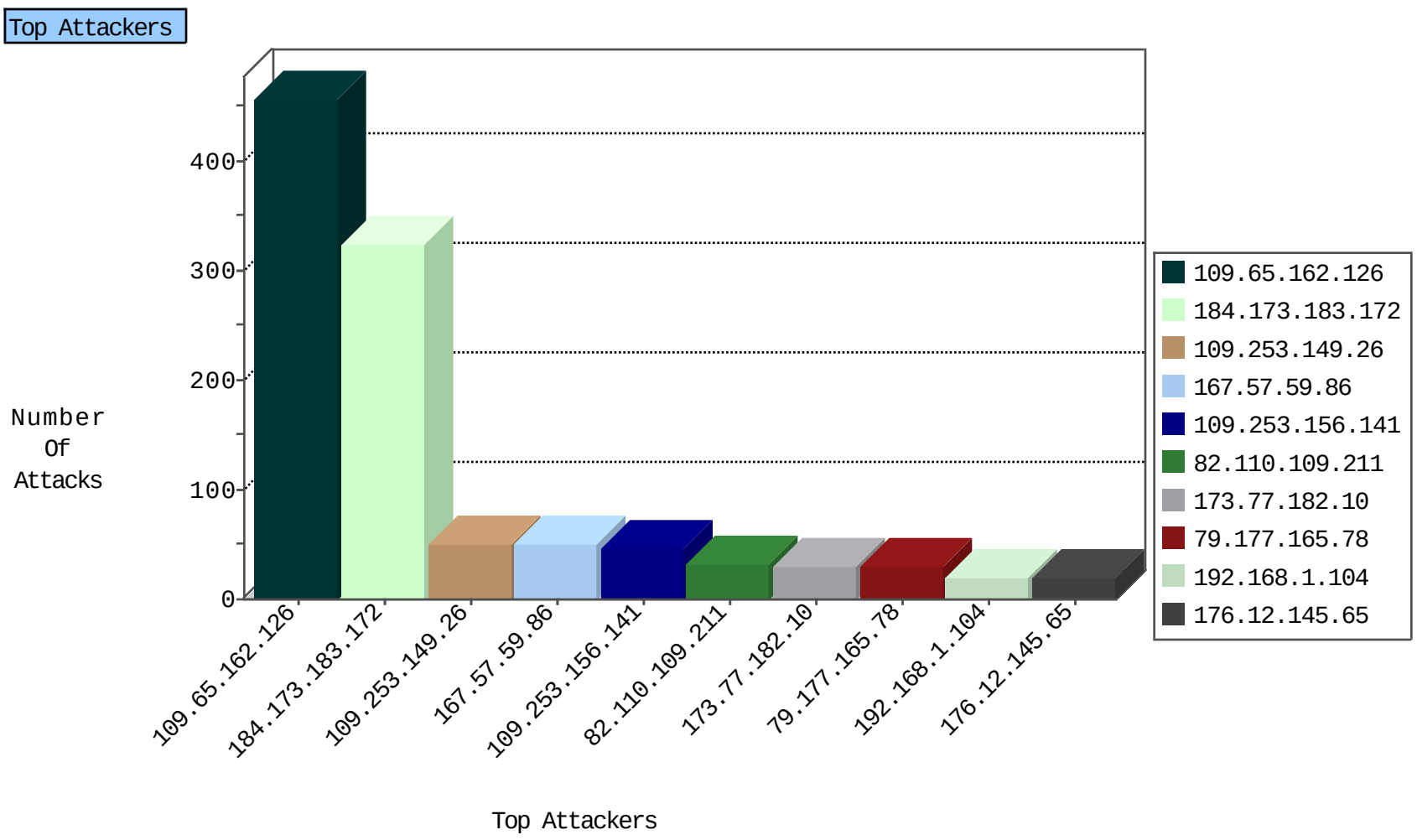
IDF Under Attack
05-09-2015-17:03:07

Top Targets



Top Target

Top Attackers



Top Attackers

05-09-2015-17:03:07 to 05-09-2015-18:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
80.178.13.60	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
46.18.19.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
220.181.108.96	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	72
192.168.1.104		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
66.249.67.190	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
192.168.1.104		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
79.180.120.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
82.102.141.252	Israel	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	3
149.78.93.123	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
167.57.59.86		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
124.232.142.220	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
61.238.58.9	Hong Kong	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
5.241.77.83	Sweden	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

05-09-2015-17:03:07 to 05-09-2015-18:03:07

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	324
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
46.120.114.48	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.176.170.49	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
31.210.180.15	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.34	yohalan.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
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.34	tikshuv.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	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
84.108.209.173	Israel	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	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.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	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.45	e.eitan.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
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-17:03:07 to 05-09-2015-18:03:07

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
66.249.73.201	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
178.19.107.114	Poland	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
107.170.4.120	United States	147.237.0.16	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.160.224.130	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.130	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.89.137.3	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.101.186.200	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
178.19.107.114	Poland	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
149.174.106.53	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.238.134.92	Poland	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.89.137.3	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.200	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1

05-09-2015-17:03:07 to 05-09-2015-18:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
167.57.59.86		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
109.253.156.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
173.77.182.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
79.177.165.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
82.110.109.211	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
176.12.145.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
79.181.160.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.183.52.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
24.189.169.67	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
76.109.55.86	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
89.138.231.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
79.179.54.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
109.64.113.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
2.54.30.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.67.64	United States	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
109.65.154.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
82.110.109.213	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.109.194.216	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
149.78.93.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.43.96.69	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.228.65.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.183.155.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
77.125.14.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
82.110.109.209	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
132.72.49.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
82.110.109.210	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
82.110.109.215	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.210.180.15	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
82.110.109.211	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
213.57.164.72	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.121.202.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.117.138.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.102.254.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.121.140.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.65.62.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.67	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
93.191.182.238	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
92.161.89.45	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
68.54.119.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.65.162.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	457
109.253.149.26	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.149.26	Block	48
94.153.9.66	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	6
178.137.19.143	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//901-11442-en/	Block	3
203.133.170.144	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.170.144	Block	3
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.149.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.30.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.161	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.64.209	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
109.67.13.84	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
104.131.193.97		147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on //	Block	1
79.178.205.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
107.170.72.219	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on //	Block	1
85.65.131.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
66.249.64.214	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
109.186.150.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
104.131.193.97		147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
80.246.133.173	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 80.246.133.173	Block	1
188.138.17.205	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
46.19.86.102	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//894-he/nakhal.aspx	Block	1
107.170.72.219	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on //	Block	1
203.133.171.29	Korea, Republic of	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
93.172.30.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.64.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
107.170.4.120	United States	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on //	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0708-1.stm	Block	1
83.244.36.98	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
46.117.197.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.64.43.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
157.55.39.223	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx	Block	1
109.253.149.26	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.67.78	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71866-he/maarachot.aspx	Block	1
107.170.4.120	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on //	Block	1
195.82.63.197	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.111.5.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1