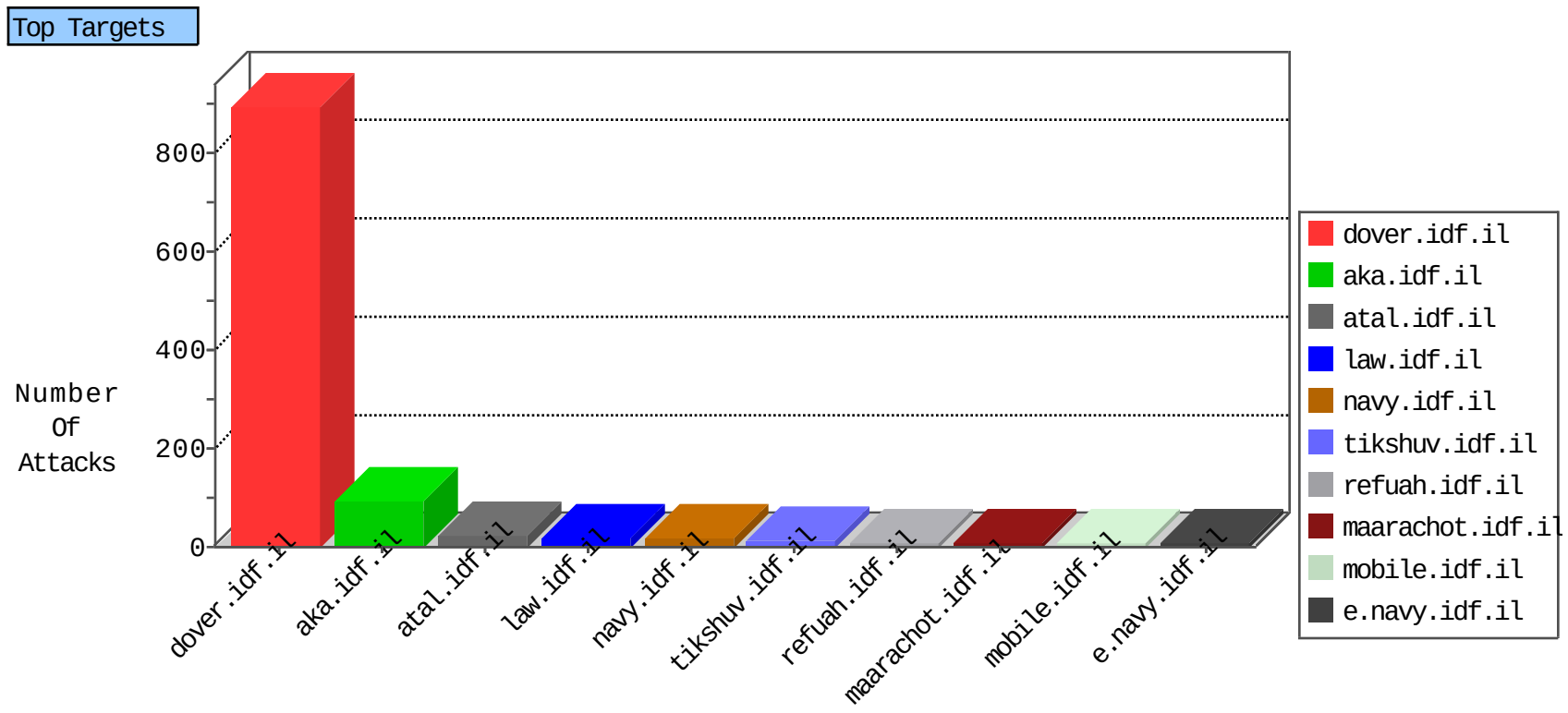
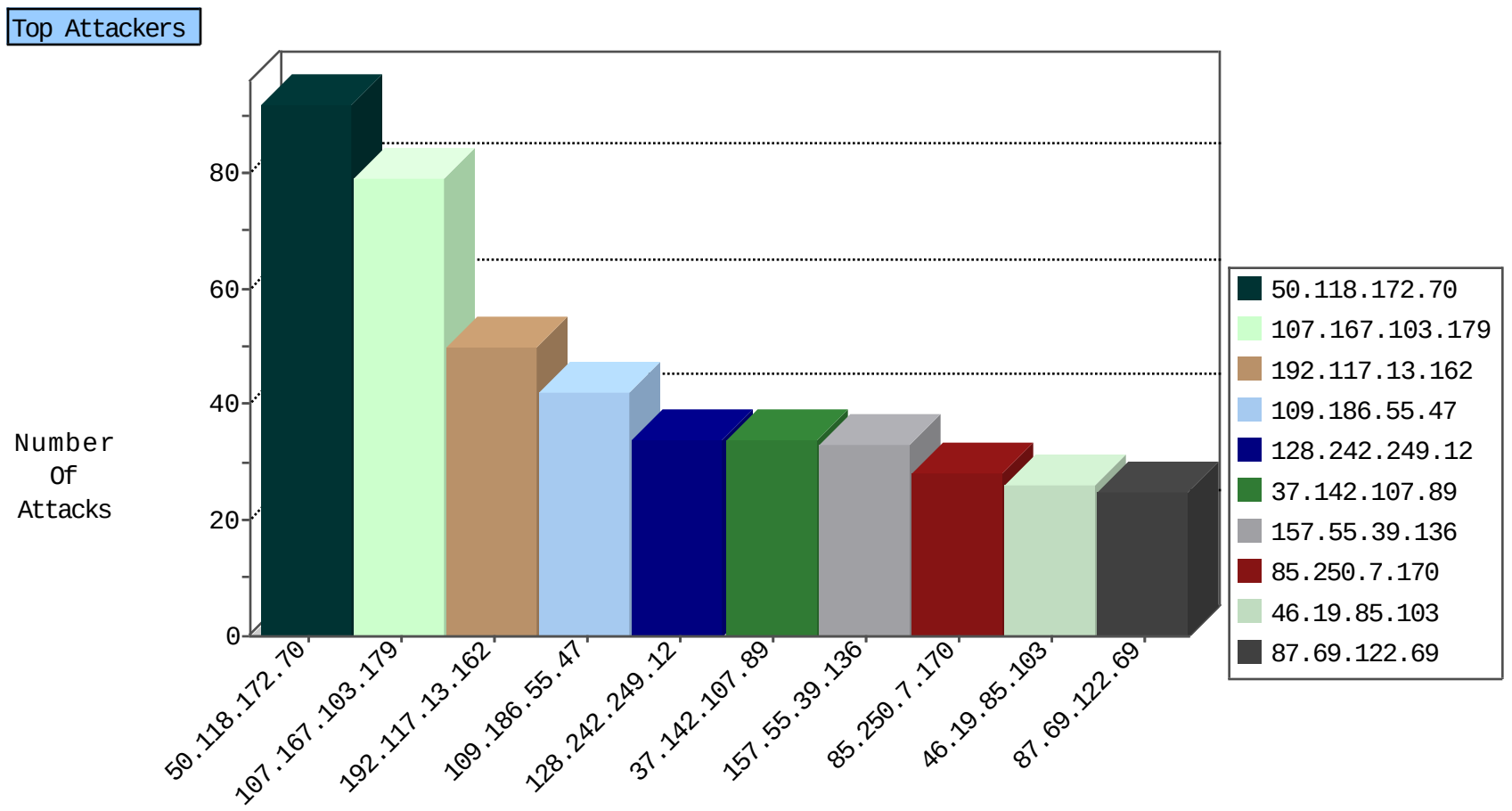
05-09-2015-13:03:04 to 05-09-2015-14:03:04

IDF Under Attack
05-09-2015-13:03:04

Top Targets



Top Attackers



05-09-2015-13:03:04 to 05-09-2015-14:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.159	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3270
85.64.94.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
138.134.102.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
37.142.105.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
49.251.45.177	Japan	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
218.200.188.213	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

05-09-2015-13:03:04 to 05-09-2015-14:03:04

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	32
84.228.47.216	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	147.237.72.14	dover.idf.il(old)	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
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
5.28.168.158	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.172.144.206	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.i	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.201	e.atal.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
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.250	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
82.205.72.118	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.234	halag.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
46.121.140.81	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
193.164.216.238	Netherlands	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
84.108.127.223	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
62.45.47.18	Netherlands	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	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-13:03:04 to 05-09-2015-14:03:04

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
46.121.81.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.105.184	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.25	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.226.60.77	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.178.181.15	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.126	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.160.224.130	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.200.188.213	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.200.188.213	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.200.188.213	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
121.46.0.125	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
92.47.29.12	Kazakstan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.165	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.67	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.200.188.213	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.200.188.213	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.34	tikshuv.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
218.200.188.213	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
121.46.0.125	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
218.200.188.213	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1

05-09-2015-13:03:04 to 05-09-2015-14:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
50.118.172.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	92
107.167.103.179	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	79
192.117.13.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
109.186.55.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
37.142.107.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
85.250.7.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
157.55.39.136	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
46.121.16.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	12
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	11
157.55.39.204	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
37.142.7.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
89.138.193.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.140.141.37	Russian Federation	147.237.77.74	law.idf.il	SAM rule	drop	drop	10
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
46.19.85.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
89.139.171.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.85.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
94.230.86.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
199.30.24.40	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
5.102.254.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.121.81.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
93.172.23.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
185.32.177.6	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
185.32.177.6	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
185.32.177.6	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	7
84.109.210.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.102.254.205	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
79.178.61.36	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
89.138.83.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
85.250.222.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
80.246.133.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
77.125.91.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.139	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.94.182.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.226.60.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.149	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
37.18.51.237	Russian Federation	147.237.77.121	e.navy.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	4
66.249.78.166	Israel	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
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
157.55.39.64	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.64	Block	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	6
157.55.39.81	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.81	Block	6
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
192.99.12.99	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	3
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
176.12.145.41	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
157.55.39.137	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
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
185.24.234.102	Ireland	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.73.239	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
37.26.148.145	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
85.250.7.170	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
212.143.152.28	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
173.252.113.112	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2	Block	1
155.133.18.153	Poland	147.237.77.216	dover.idf.il	Distributed eMail Hoarding	Block	1
2.54.21.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
157.55.39.64	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/main/main.asp	Block	1
109.186.189.79	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
217.132.74.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
173.252.113.116	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	1
5.9.156.11	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.9.156.11	Block	1
79.177.117.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giuse	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18590-he/dover.aspx	Block	1
199.180.114.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17436-en/dover.aspx/trackback/	Block	1
46.120.128.140	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
119.134.251.140	China	147.237.77.170	maarachot.idf.il	Admin Blocking	Block	1
66.249.64.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
5.9.156.11	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/shared/usercontrols/lobbyinfocenteritem/	Block	1
84.108.86.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.194.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl50.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
119.134.251.140	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
66.249.78.165	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
185.24.234.102	Ireland	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5866-he/patzar.aspx	Block	1
5.28.168.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.7	Block	1
85.64.247.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20200-he/idfgdover.aspx	Block	1

05-09-2015-13:03:04 to 05-09-2015-14:03:04