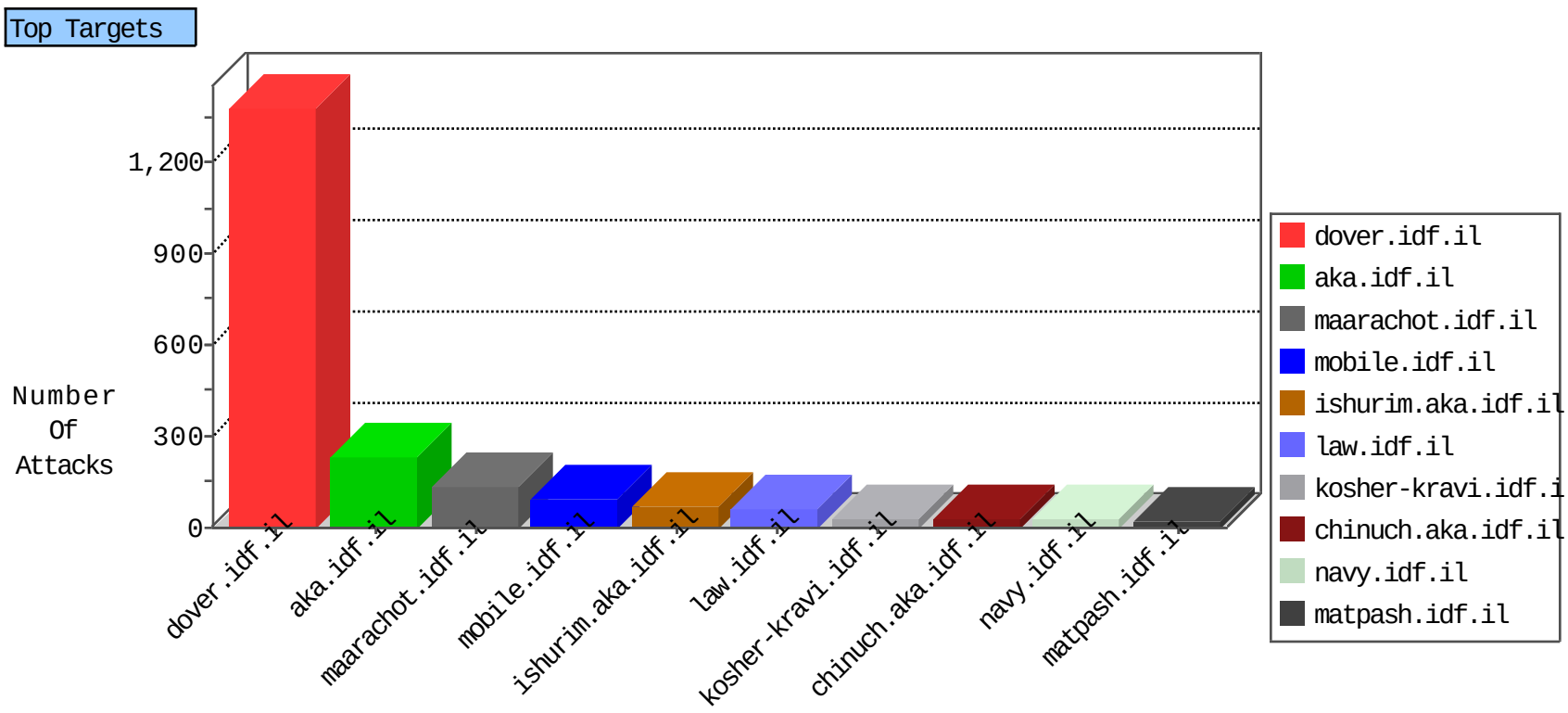
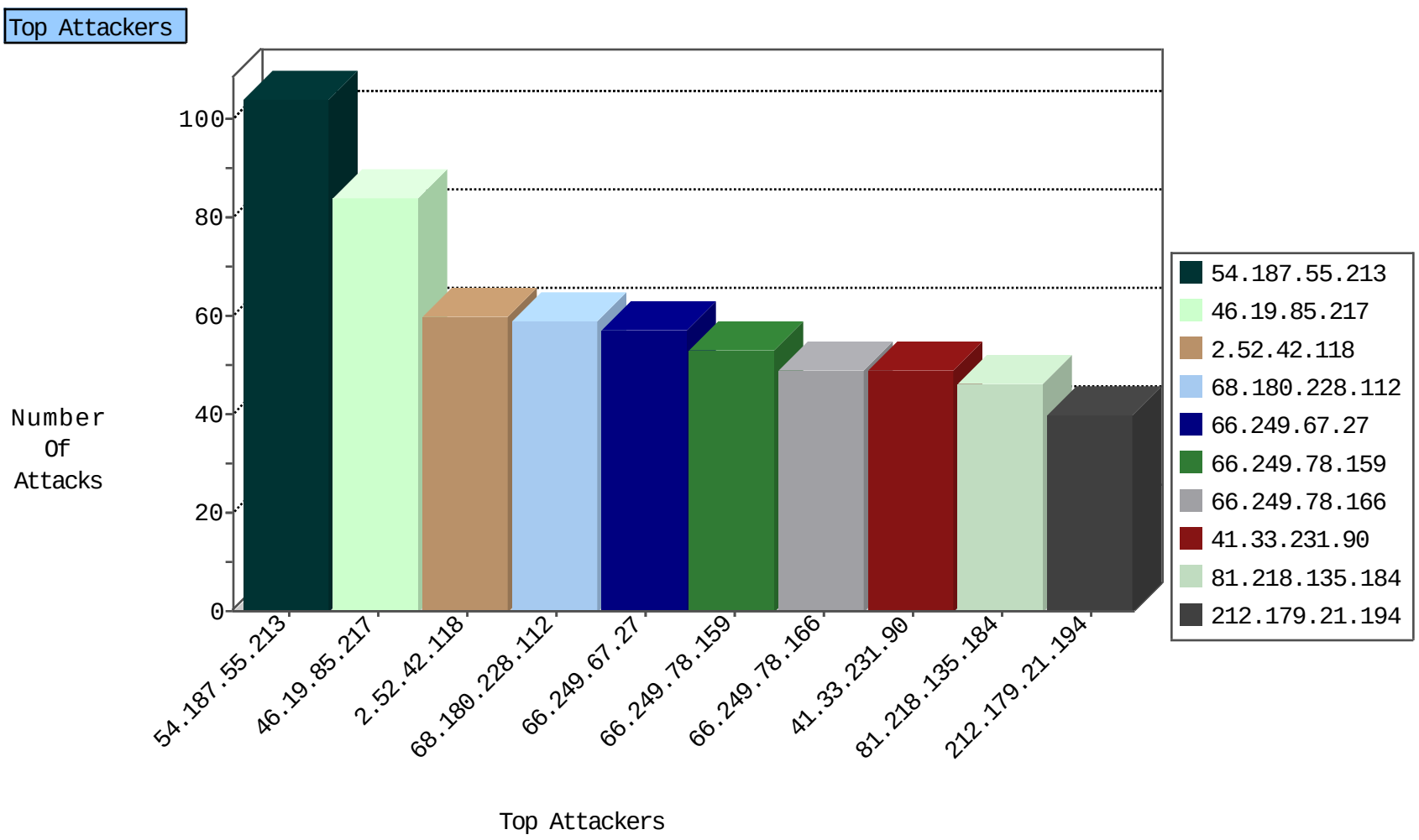
11-01-2015-06:04:01 to 11-01-2015-07:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-01-2015-06:04:01 to 11-01-2015-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	13333
176.13.23.58	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2582
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	707
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	409
71.191.192.50	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	50
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	42
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
79.181.188.231	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
24.44.104.30	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
209.44.148.203	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
79.180.153.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.78.198.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.178.104.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.67.42.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
185.32.179.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.12.151.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
104.14.54.172	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
201.81.172.28	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.86.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
176.13.23.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
176.13.23.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.146.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.142.68.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.139.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.137.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
80.246.137.192	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
68.152.51.14	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
2.54.164.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

11-01-2015-06:04:01 to 11-01-2015-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.108.86	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
62.210.97.48	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

11-01-2015-06:04:01 to 11-01-2015-07:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
221.7.213.44	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.119.55.249	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
209.119.55.249	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	147.237.0.33	Seychelles	idf.il	ET SCAN NMAP -sS window 1024	1
111.93.198.54	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
41.140.253.9	147.237.77.170	Morocco	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
41.140.253.9	147.237.77.170	Morocco	maarachot.idf.il	ET SCAN NMAP -f -sS	1
209.119.55.249	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
209.119.55.249	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
111.93.198.54	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -f -sS	1
62.219.83.119	147.237.0.200	Israel	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
41.140.253.9	147.237.77.170	Morocco	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1

11-01-2015-06:04:01 to 11-01-2015-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
81.218.135.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.19.85.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.19.85.217	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
201.81.172.28	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
46.117.116.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.240.254.146		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.151	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.12.160.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.42.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
62.210.113.143	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
73.134.115.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.165.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.83.158	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
1.127.48.206	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.181.117.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.168.187.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
80.246.130.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.179.31.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.67.38.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
209.44.148.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.120.182.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.106.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.151	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.220	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.140.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.153.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
71.191.192.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.146.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.42.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
54.187.55.213	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.187.55.213	Block	30
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	30
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	30
54.187.55.213	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15
96.44.189.100	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	15
82.80.196.44	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	15
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18858-he/dover.aspx	Block	15
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17374.jpg	Block	15
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/70902.pdf	Block	15
87.68.255.132	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
155.94.171.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	15
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	15
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	15
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	15
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
41.254.8.12	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	15
93.173.252.255	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	15
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	15
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	15
54.187.55.213	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	15
84.177.23.204	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15
217.132.52.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	15
150.70.173.6	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/45026dotjpg	Block	15
46.19.86.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
95.165.106.128	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15
68.180.230.240	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/112922.pdf×ž× ×″×™×′×•×ª	Block	15
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/718-he/patzar.aspx	Block	15
176.103.48.58	Ukraine	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	15
148.240.174.247	Mexico	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15
66.249.67.20	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/112436.pdf	Block	15
84.201.138.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	15
150.70.173.6	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71926-he/maarachot.aspx	Block	15
46.166.190.135	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15
95.220.148.136	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	15
66.249.75.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	15
188.244.39.126	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15
148.240.174.247	Mexico	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	15
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	15
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	15