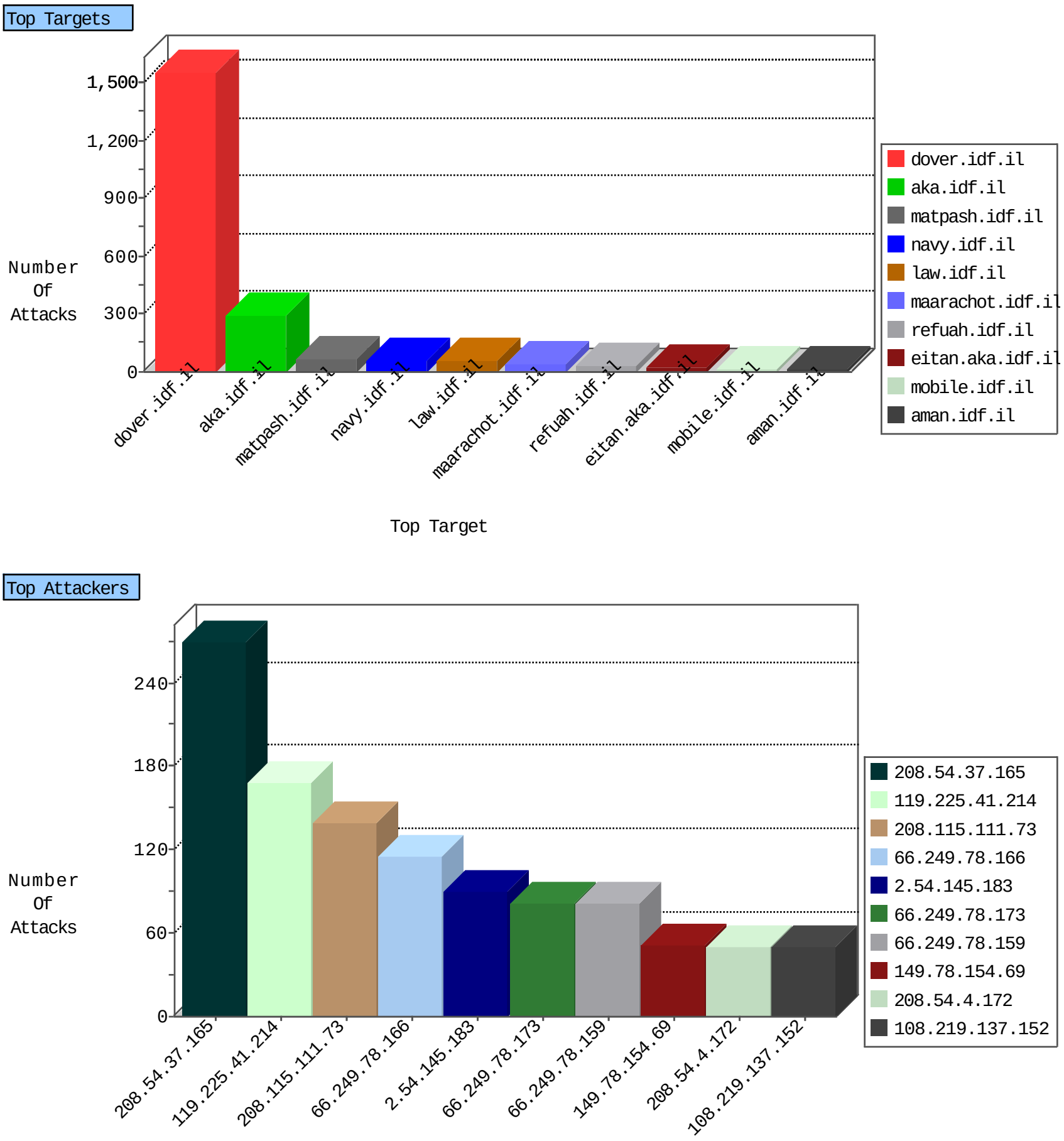
10-29-2015-03:04:01 to 10-29-2015-04:04:01

IDF Under Attack Daily Report



10-29-2015-03:04:01 to 10-29-2015-04:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4599
66.249.69.77	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2793
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	641
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	318
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	282
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	53
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
10.0.0.17		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
181.55.195.8	Colombia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.166.188.68	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

10-29-2015-03:04:01 to 10-29-2015-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.213.82	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.169.85	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

10-29-2015-03:04:01 to 10-29-2015-04:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.67.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
69.64.46.86	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
69.64.46.86	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
1.235.195.234	147.237.77.233	Korea, Republic of	atal.idf.il	ET SCAN NMAP -sS window 2048	1
218.89.137.3	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
216.197.239.142	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
211.241.180.35	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
78.185.199.42	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
69.64.46.86	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
1.235.195.234	147.237.77.233	Korea, Republic of	atal.idf.il	ET SCAN NMAP -sS window 3072	1
1.235.195.234	147.237.77.233	Korea, Republic of	atal.idf.il	ET SCAN NMAP -f -sS	1
218.89.137.3	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
211.241.180.35	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1

10-29-2015-03:04:01 to 10-29-2015-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.54.37.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	270
119.225.41.214	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	168
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
2.54.145.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	82
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	74
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
108.219.137.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
208.54.4.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
176.12.137.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
5.102.227.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
109.64.144.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.79.79	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.79.232.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.79.77	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.4.255.71	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
135.23.129.247	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.142.159.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.181.108.212	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
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
181.55.195.8	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.161	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
216.197.239.142	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
152.236.199.9	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.117.97.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
180.76.15.20	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.45	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
157.55.39.130	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
66.249.67.34	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.67.34	Block	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/17436.jpg	Block	15
85.173.67.215	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	15
66.249.75.116	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/112540.pdf	Block	15
162.253.180.218	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 162.253.180.218 (Open Mode)	None	15
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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/4/71084.doc	Block	15
207.46.13.53	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	15
85.173.67.215	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	15
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16789-he/dover.aspx	Block	15
66.249.67.202	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/3/423.pdf319	Block	15
184.105.139.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	15
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	15
66.249.69.35	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.71	Block	15
207.46.13.187	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/news/news.asp	Block	15
141.212.122.128	United States	147.237.76.86	navy.idf.il	Malformed URL proxytest.zmap.io:80	Block	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12188-he/dover.aspx	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/shared/usercontrols/headerupper/	Block	15
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/1528.png	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/1158-he/chinuch.aspx	Block	15
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	15
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/sitemap.asp	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20313-he/dover.aspx	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1158-he/chinuch.aspx	Block	15
193.252.118.176	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	15
85.173.67.215	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-en/cogat.aspx	Block	15
66.249.75.46	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/programmer.asp	Block	15