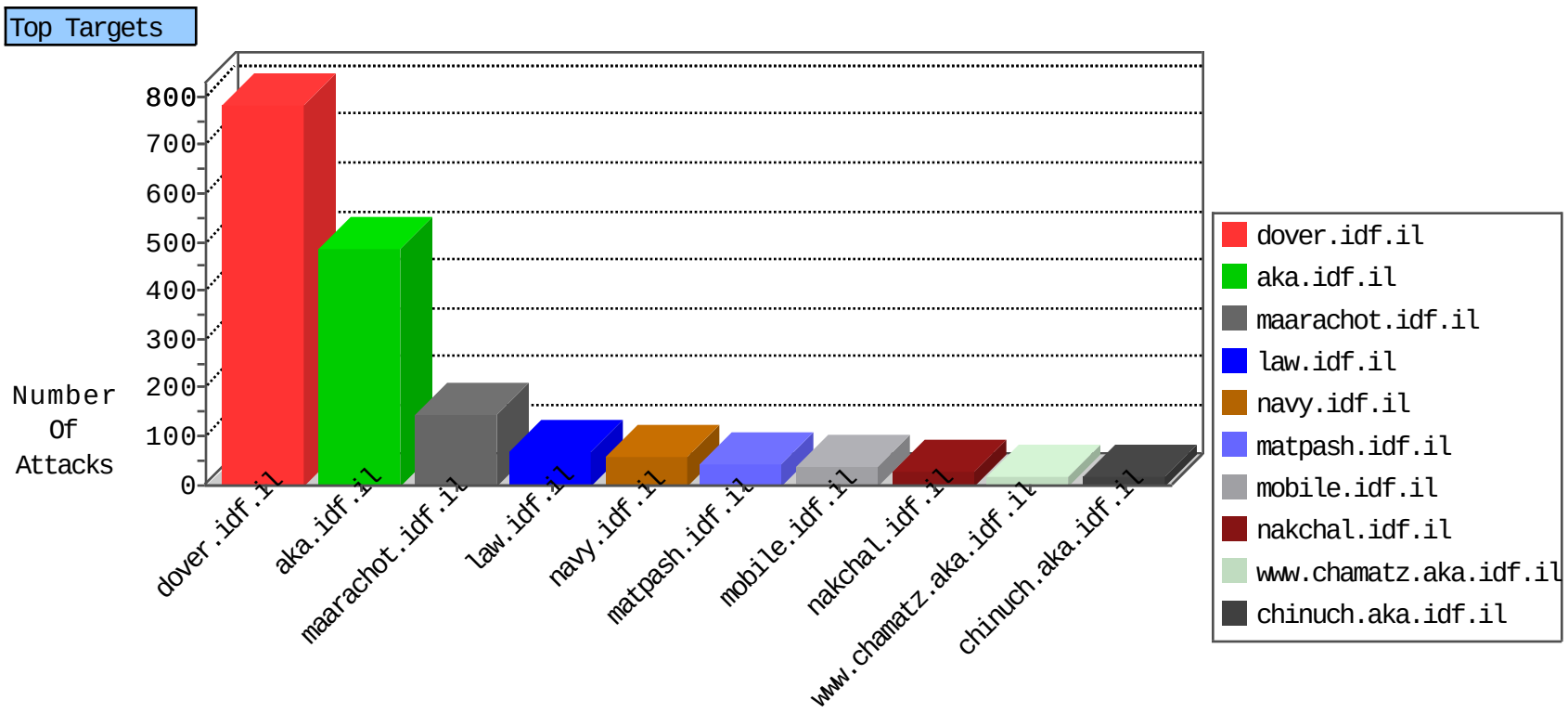
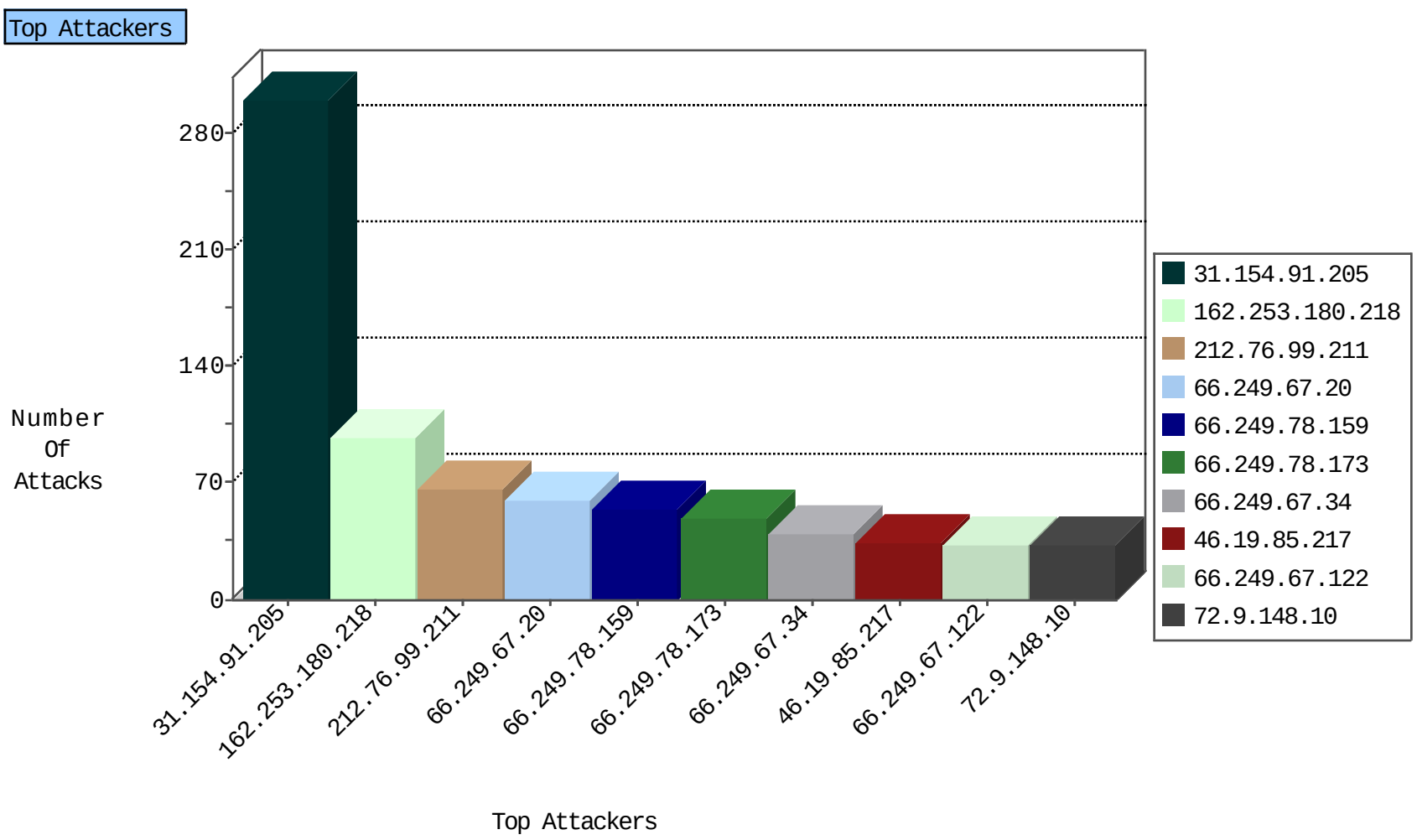
10-29-2015-02:04:08 to 10-29-2015-03:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-29-2015-02:04:08 to 10-29-2015-03:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	33348
66.249.69.85	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	12289
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8952
51.254.143.241	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6301
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1018
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	863
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	442
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	27
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
212.76.99.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
72.83.21.149	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.66.125.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
222.186.34.73	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
2.54.18.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2
176.13.20.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.136.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.15.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
149.88.206.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

10-29-2015-02:04:08 to 10-29-2015-03:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-29-2015-02:04:08 to 10-29-2015-03:04:08

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
66.249.67.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
162.248.10.134	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
123.18.206.13	147.237.77.178	Vietnam	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
69.64.46.86	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
162.248.10.134	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
162.248.10.134	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.194	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
69.64.46.86	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.162.116.98	147.237.77.19	Sweden	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1

10-29-2015-02:04:08 to 10-29-2015-03:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
162.253.180.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
212.76.99.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
46.19.85.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
100.100.69.191		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
141.0.8.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
62.210.113.143	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
66.249.79.77	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.66.3.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.151.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.18.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.30	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.39	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.220.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.167.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.15.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.167.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.171.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.66.125.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
128.232.110.28	United Kingdom	147.237.76.201	e.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.108.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.88.206.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
72.83.21.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
95.108.132.175	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.85.98.210	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.142.150.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.6	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.91.205	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 31.154.91.205	Block	285
91.90.191.135	Poland	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	Block	30
66.249.67.20	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.67.20	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
79.182.13.72	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/home.asp	Block	15
31.154.91.205	Israel	147.237.72.166	aka.idf.il	Too Many 404: Response Code per Session	Block	15
66.249.69.35	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	15
58.8.148.3	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	15
174.129.237.157	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20581-he/dover.aspx	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.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/6/size220x0/17436.jpg	Block	15
66.249.67.34	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/108889.pdf	Block	15
66.249.69.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/19122010hodshy.aspx	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71633-he/maarachot.aspx	Block	15
66.249.64.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.153	Block	15
176.13.0.135	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
207.46.13.47	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
141.212.122.128	United States	147.237.0.19	madim.atal.idf.il	Malformed URL proxytest.zmap.io:80	Block	15
31.193.51.17	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.75.23	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	15
180.76.15.16	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	15
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/106321.pdf	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
54.160.209.189	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14886-en/dover.aspx.	Block	15
66.249.75.44	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/shared/usercontrols/headerupper/	Block	15
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	15
66.249.67.20	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	15
180.76.15.32	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	15
77.125.84.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/	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
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/military-police	Block	15
58.8.148.3	Thailand	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	15
162.253.180.218	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	15
66.249.75.83	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	15
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/602-6394-he/patzar.aspx	Block	15
185.32.179.39	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.34	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.67.34	Block	15