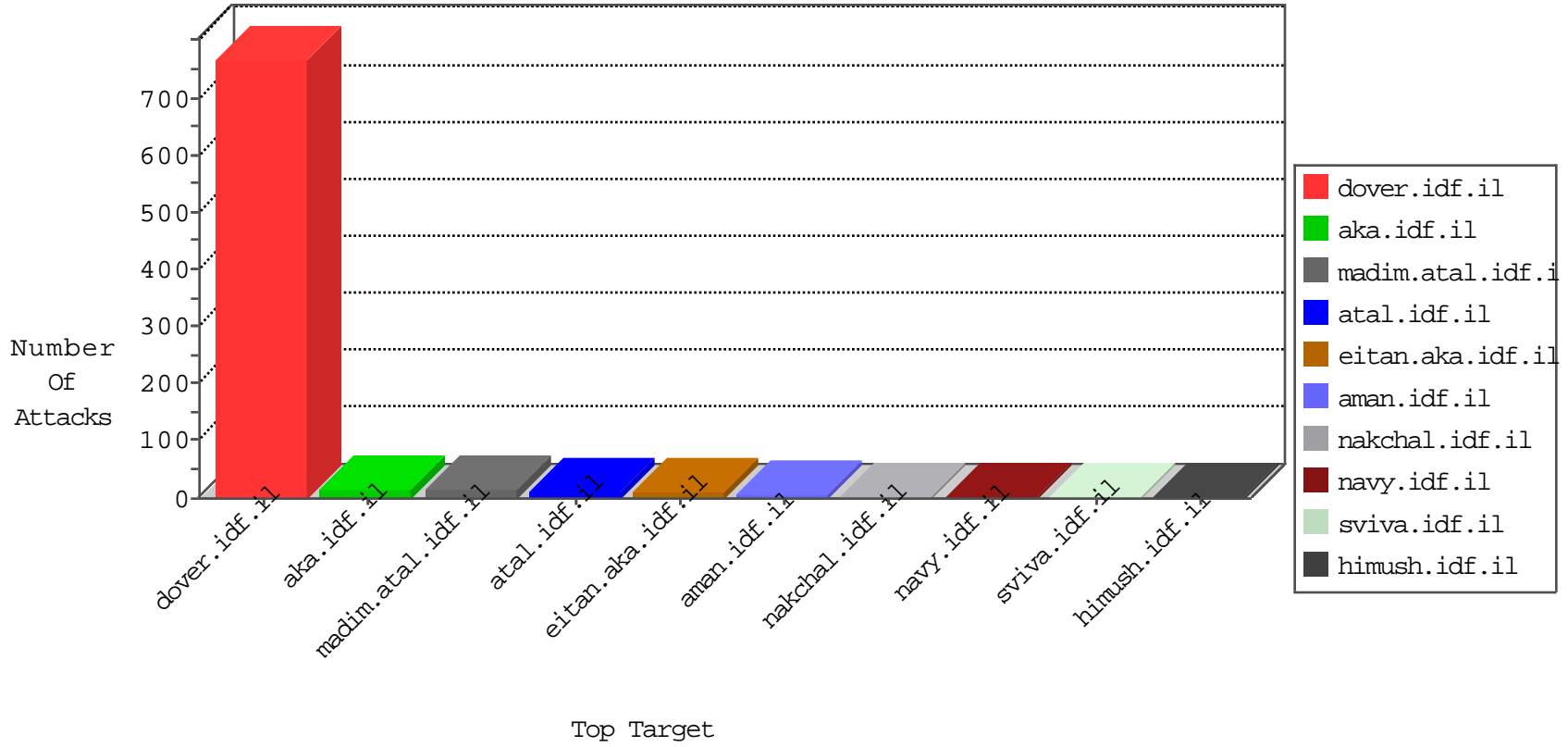


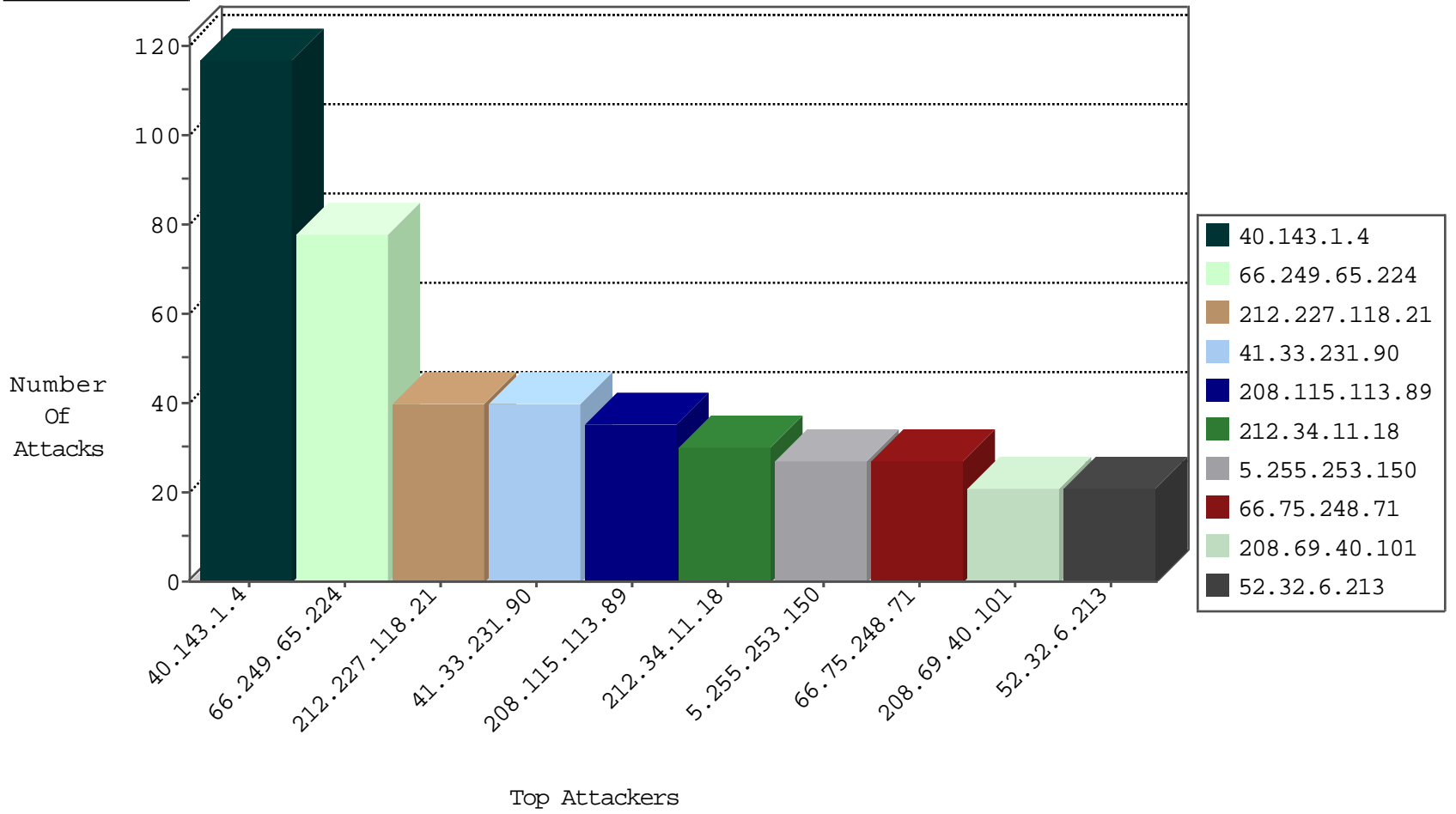
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
168.235.201.117	United States	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	3
168.235.201.117	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
104.192.0.226	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
176.123.29.54	Moldova, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
204.42.253.132	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
91.208.115.34	Ukraine	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

11-21-2015-05:04:00 to 11-21-2015-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## 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
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
184.172.196.106	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
184.172.196.106	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
222.186.56.32	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.22.182.65	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.34.142	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.142	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.151.55.35	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
184.172.196.106	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
184.172.196.106	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
184.172.196.106	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
184.172.196.106	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.32	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
184.172.196.106	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.142	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.142	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.142	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.97.60.174	147.237.76.34	India	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.5.101.82	147.237.8.27	Honduras	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
184.172.196.106	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
184.172.196.106	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.227.118.21	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
212.34.11.18	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.75.248.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
52.32.6.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
40.143.1.4	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
129.184.84.40	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.255.253.158	Russian Federation	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
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.143.1.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.67.130.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.178	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
157.55.39.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.155.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
17.142.152.85	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
76.28.145.220	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.255.253.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.111.190.231	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.178	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
157.55.39.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
17.142.152.81	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
141.8.142.11	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.143.1.4	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.143.1.4	Block	80
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	31
40.143.1.4	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	10
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	4
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	4
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.111.190.231	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.111.190.231	Block	1
66.249.67.129	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
141.212.122.160	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
107.150.43.206	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/givati/	Block	1
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	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/forms.aspx	Block	1
204.195.139.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/forums/asp/	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
114.108.214.74	Philippines	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
89.138.169.199	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 89.138.169.199 (sigalgs DoS Attack)	None	1
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/11275.jpg	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
74.82.47.3	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
207.46.13.158	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
114.108.214.74	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
89.138.169.199	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.34.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
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	1
79.179.37.110	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
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	1
207.46.13.158	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.158	Block	1
129.184.84.40	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/news/jenin.stm)	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/artillery	Block	1
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	1
203.133.170.94	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
40.143.1.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/piwik.php	Block	1
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	1
84.111.190.231	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1