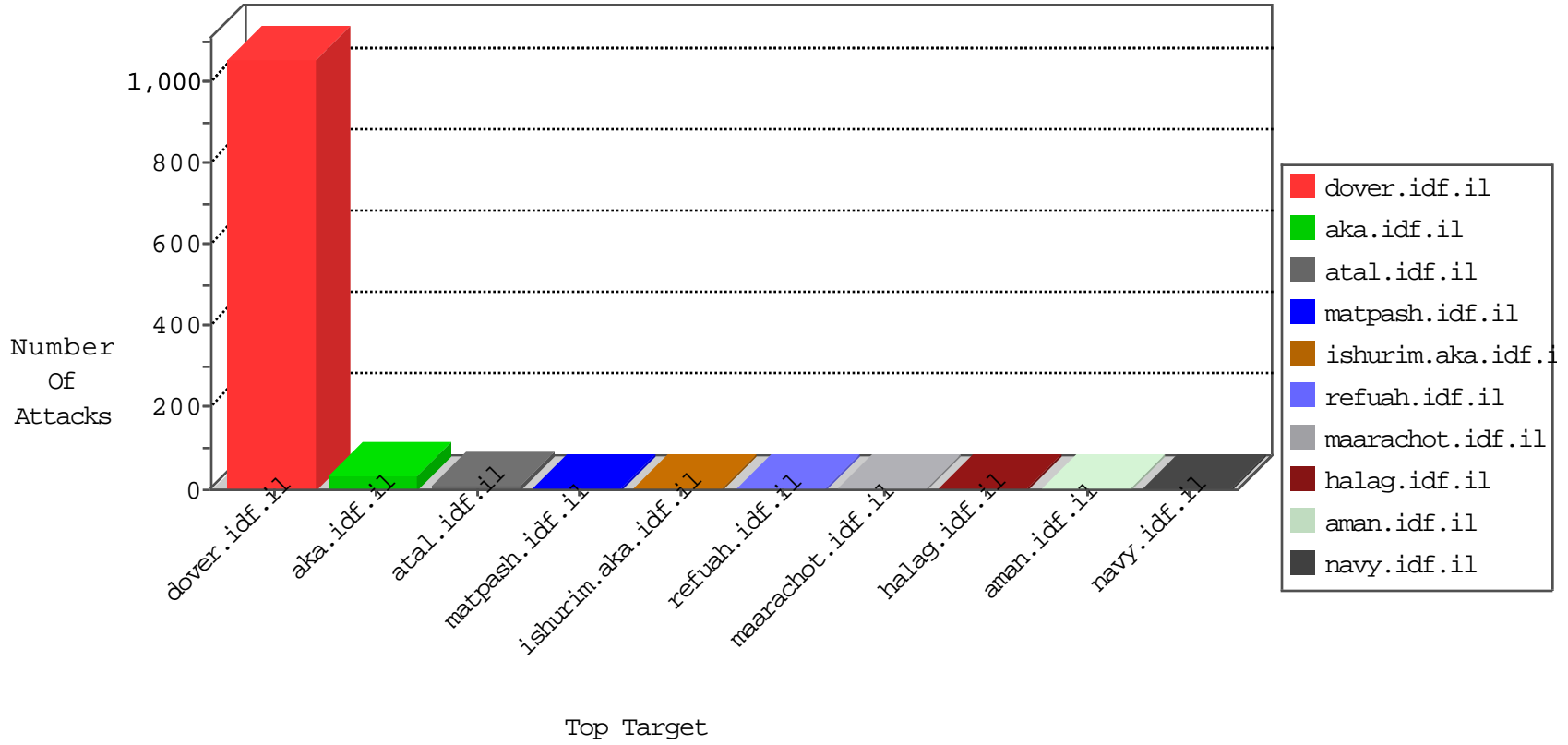


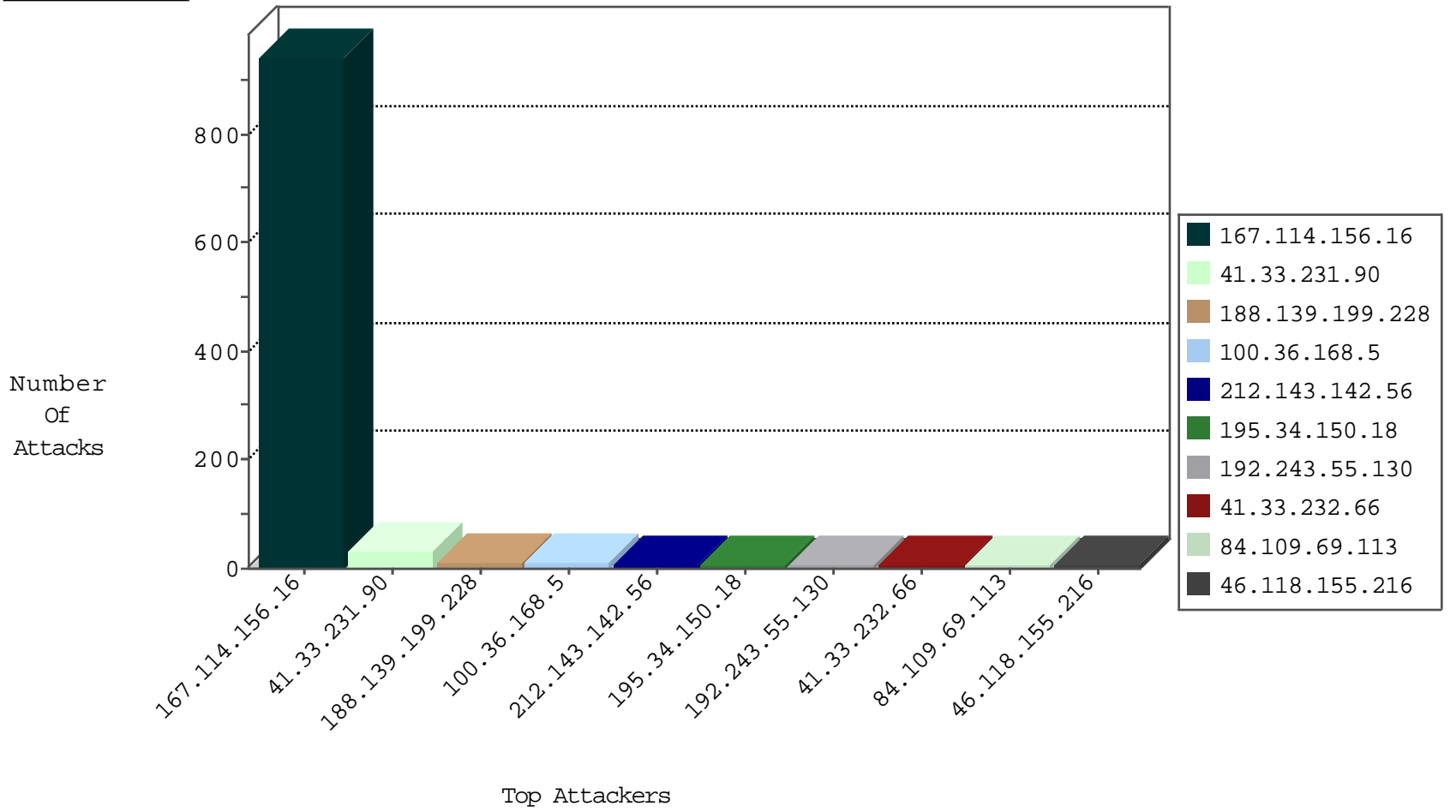
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3149
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	985
23.95.248.111	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
23.95.248.111	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
65.181.113.88	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

01-10-2016-03:04:05 to 01-10-2016-04:04:05

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
175.9.89.121	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.203	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.77.178	Kazakstan	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.196	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.57	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.90.21	147.237.77.179	France	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
177.231.140.62	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.203	147.237.76.147	Netherlands	chimuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.90.21	147.237.77.234	France	halag.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
100.36.168.5	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
188.139.199.228	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
188.139.199.228	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.69.113	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.228.185.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
184.105.247.220	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.32	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.236.214.244		147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.131.190.12	United States	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
94.102.48.195	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.143.107.155	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.67	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
104.236.26.153		147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.131.15.191	United States	147.237.0.19	madim.atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.86.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.236.214.244		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.131.190.12	United States	147.237.72.167	ishurim.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
95.90.186.146	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.83	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.236.52.43		147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.131.105.125	United States	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
213.151.46.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
69.122.148.186	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.236.15.109		147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
95.91.226.136	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
79.181.223.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.83	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.55.151.205		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.236.77.10		147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.131.105.199	United States	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
216.218.206.92	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
91.143.235.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.185.82.88	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.26	United States	147.237.0.33	idf.il	drop		drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.236.16.11		147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
184.105.247.200	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.55.193.110		147.237.0.17	m.my-kosher-kravi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.236.106.95		147.237.0.34	tikshuv.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	5
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	3
2.54.9.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
212.76.96.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
109.201.152.21	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
104.236.77.10		147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
104.131.105.199	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.75	Block	1
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/926-he/atal.aspx	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/glyus/general.aspx?catid=59269&docid=75172	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/masaiyot11012011.aspx	Block	1
104.236.16.11		147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.109.69.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1158-he/dover.aspx	Block	1
166.170.5.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
104.236.106.95		147.237.0.34	tikshuv.idf.il	Unauthorized Method HEAD for 147.237.0.34/	Block	1
104.131.181.197	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/925-he/atal.aspx	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
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2308.jpg	Block	1
40.77.167.3	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/js/js_messages.jsp	Block	1
104.236.26.153		147.237.76.86	navy.idf.il	Unauthorized Method HEAD for 147.237.76.86/	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
104.131.15.125	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1039-he/dover.aspx	Block	1
173.252.74.106	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.236.214.244		147.237.76.30	himush.idf.il	Unauthorized Method HEAD for 147.237.76.30/	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
104.131.190.12	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
212.47.227.72	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/	Block	1
109.163.234.8	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3468.gif	Block	1
45.55.151.205		147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
104.236.26.153		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
104.131.15.191	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.69.46	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1745	Block	1
104.236.214.244		147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.166.186.206	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1