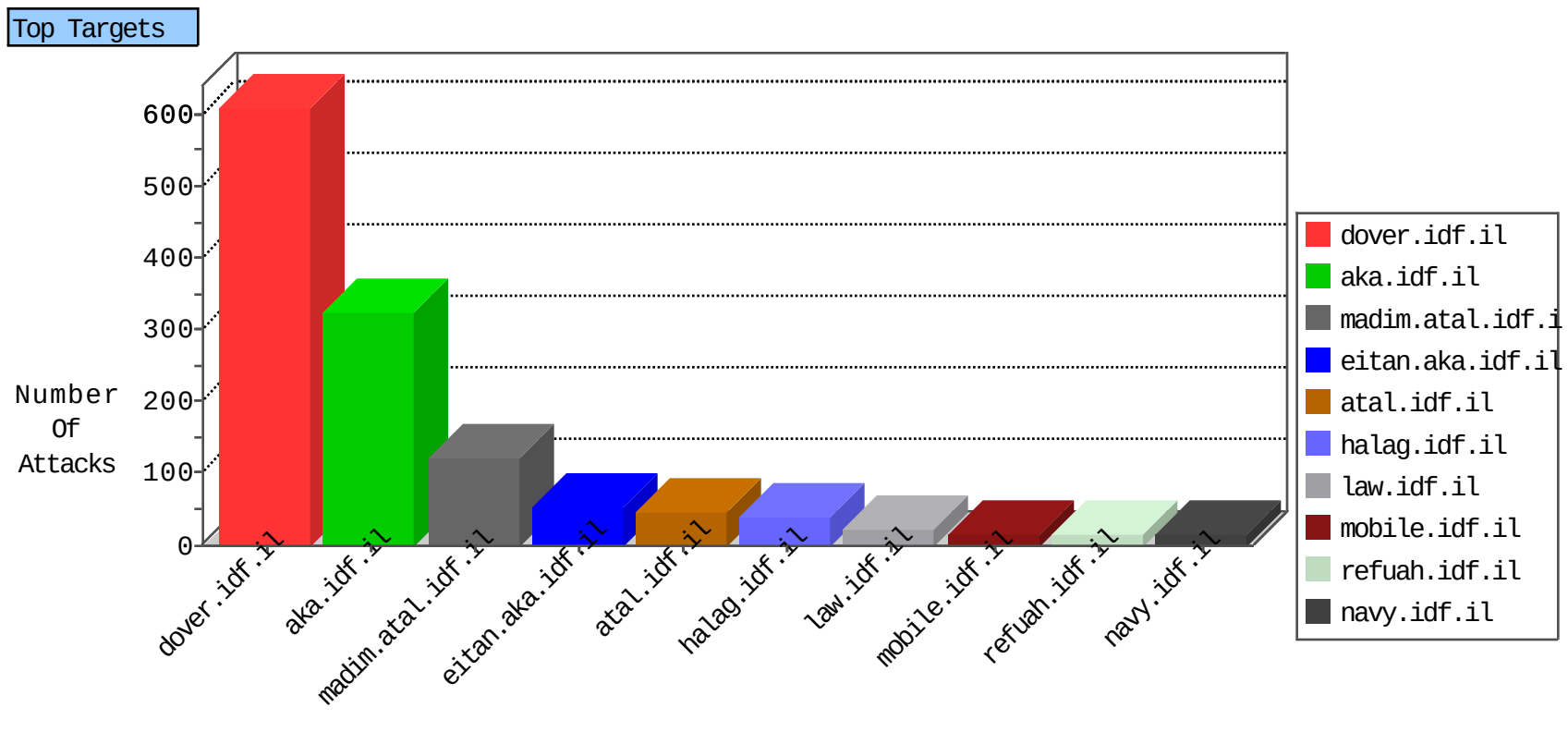
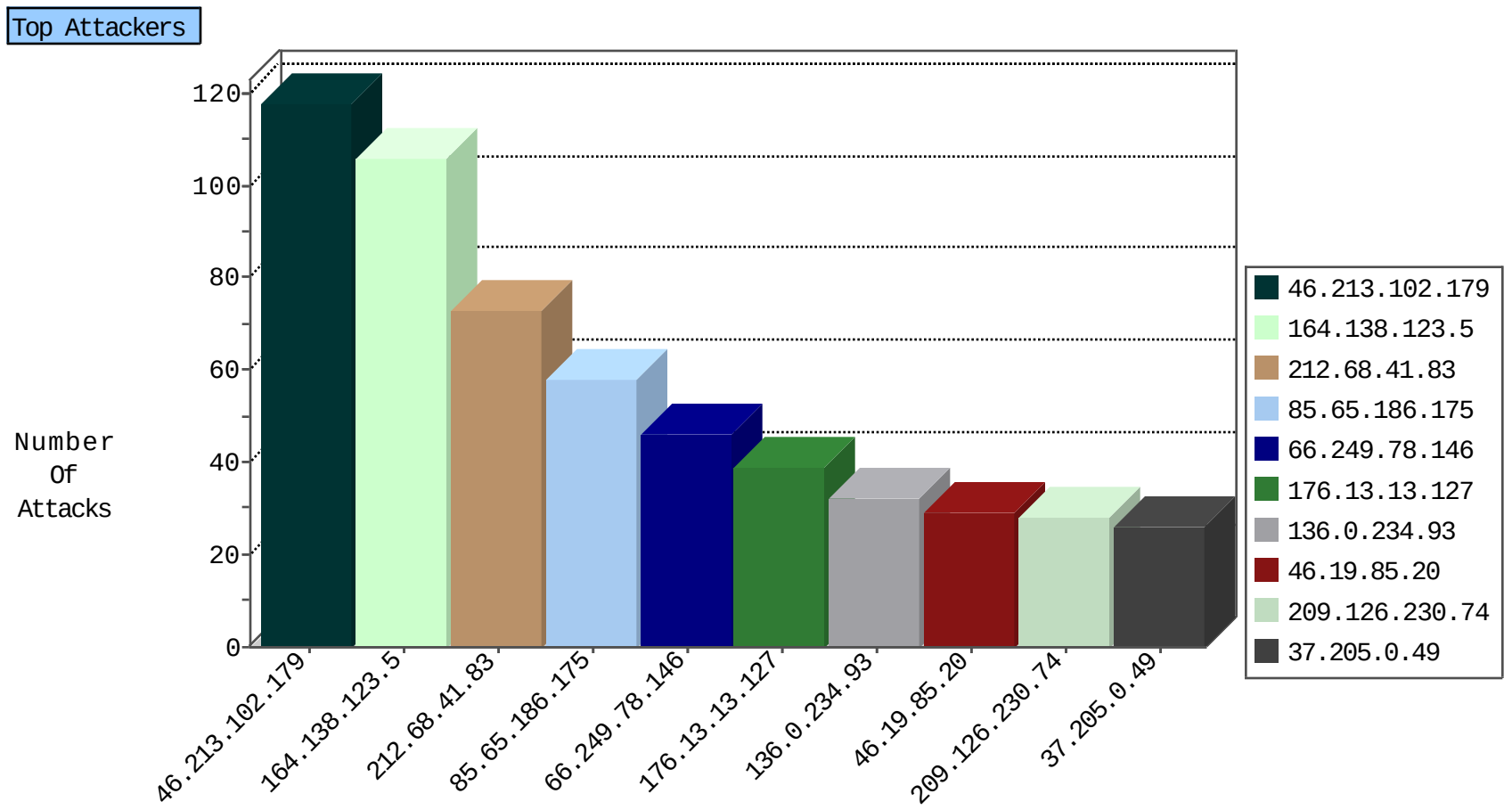
04-25-2016-22:04:09 to 04-25-2016-23:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-25-2016-22:04:09 to 04-25-2016-23:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
45.63.20.231	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.161	China	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.74	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

04-25-2016-22:04:09 to 04-25-2016-23:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.205.0.49	Turkey	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
37.205.0.49	Turkey	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
37.205.0.49	Turkey	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
41.251.194.218	Morocco	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	2
41.251.194.218	Morocco	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
37.205.0.49	Turkey	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

04-25-2016-22:04:09 to 04-25-2016-23:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.205.0.49	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	14
66.249.79.111	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
212.179.159.253	147.237.77.74	Israel	law.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
188.214.249.153	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	2
91.201.236.155	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
187.188.72.11	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
187.188.72.11	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
158.255.5.147	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
114.215.150.146	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.77.74	Latvia	law.idf.il	ET SCAN NMAP -sS window 1024	1
187.188.72.11	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
185.25.136.230	147.237.0.16	Italy	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.20.41.62	147.237.76.198	Singapore	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

04-25-2016-22:04:09 to 04-25-2016-23:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.68.41.83	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
46.213.102.179	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	59
46.213.102.179	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	59
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
85.65.186.175	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
136.0.234.93	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
176.13.13.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
85.130.184.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
185.120.126.18	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.65.186.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
84.94.46.94	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
92.194.120.165	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
157.55.39.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
200.222.27.193	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
196.141.255.210	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.153.170.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
199.58.86.206	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.75.79.141	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.130.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
130.76.96.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.214.11.209	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.28.159.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.115.83.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.239.222	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.180.98	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.13.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.60.146.143	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.115.83.5	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
190.207.230.128	Venezuela	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.179.194.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.194.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
186.93.110.62	Venezuela	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.20	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.138.123.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
5.28.159.81	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.119.112.23	Block	3
5.29.130.190	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	3
2.53.149.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.29.71.132	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.159	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	2
176.13.22.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
132.64.142.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docID in www.aka.idf.il/miluim/templates/inner.asp	None	1
217.78.50.204	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
84.108.18.212	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
209.126.230.74	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.208	Israel	147.237.76.42	refuah.idf.il	Malformed URL he-il,en-us;q=0.8	Block	1
151.80.31.175	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/540-he/patzar/aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/webresource.axd	Block	1
51.255.65.71	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
207.46.13.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17899-he/dover.aspx'½¿|'½¿|'½¿|''¦'•:	Block	1
85.65.186.175	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
209.126.230.74	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.208	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ccept-Language: in URL he-il,en-us	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.115.113.82	Block	1
95.35.51.221	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.15	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
209.126.230.74	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
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	1
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.41	Block	1
109.253.196.94	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
212.68.41.83	Turkey	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
2.53.43.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
82.196.42.196	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/smalim/scriptresource.axd	None	1
209.126.230.74	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.208	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1

04-25-2016-22:04:09 to 04-25-2016-23:04:09