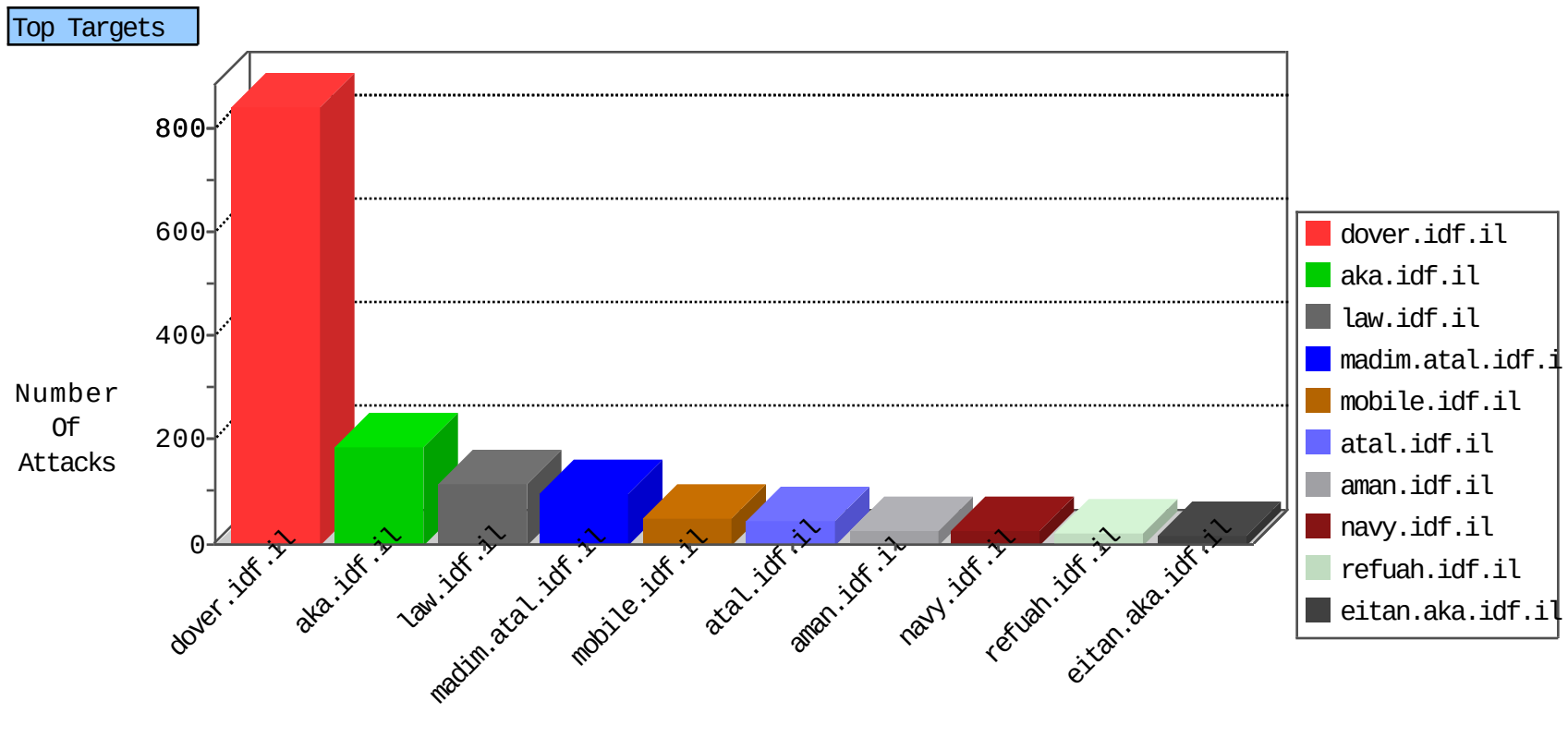
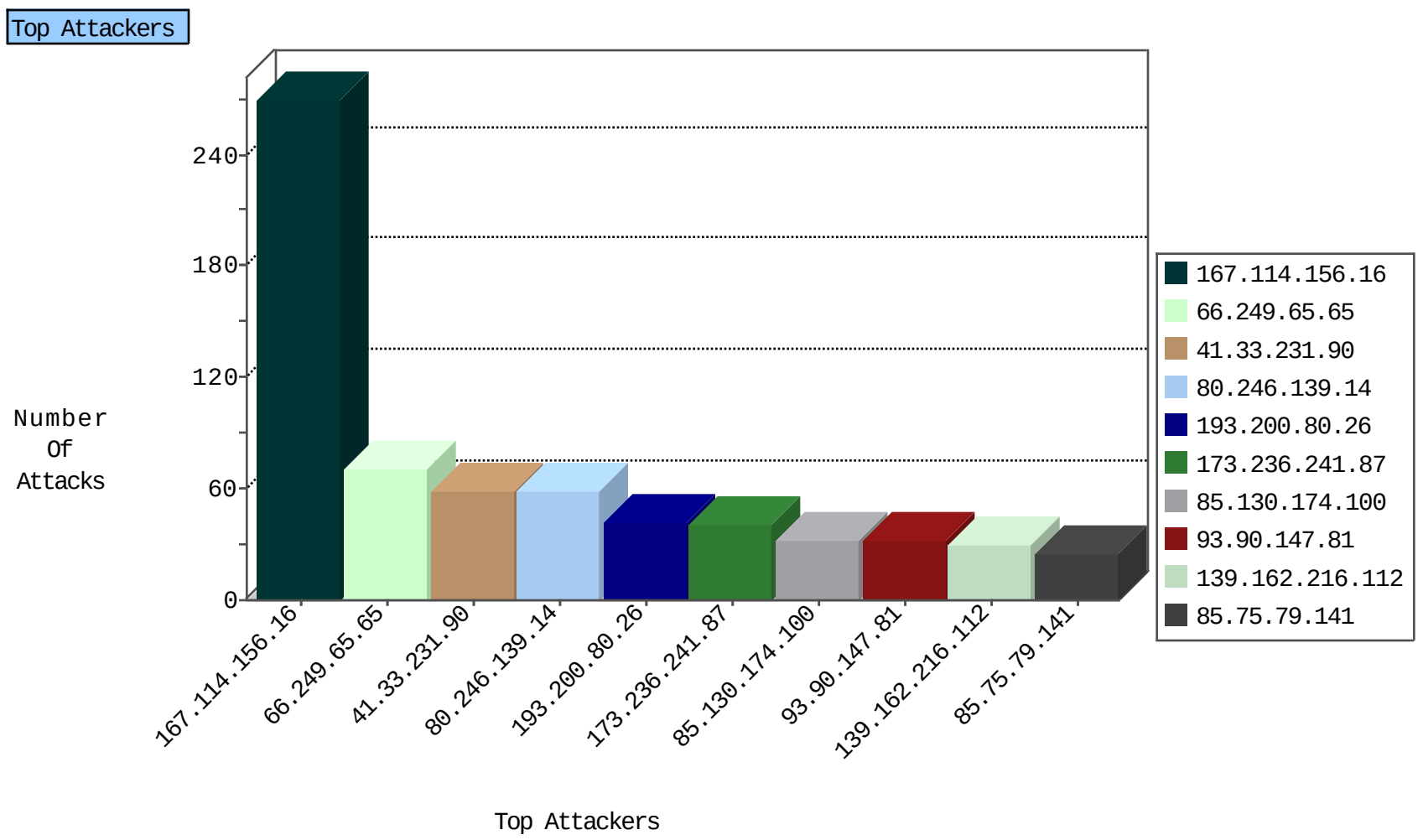
04-22-2016-10:04:08 to 04-22-2016-11:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-22-2016-10:04:08 to 04-22-2016-11:04:08

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	TCP handshake violation, first packet not syn	drop	13837
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7291
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4426
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
79.178.229.60	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
5.102.195.129	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
209.133.214.215	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
162.252.86.87	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
104.156.63.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

04-22-2016-10:04:08 to 04-22-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.90.147.81	Sweden	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
195.234.228.90	Germany	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.8.145.99	Israel	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
193.200.80.26	United Kingdom	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
195.234.228.90	Germany	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
158.85.253.245	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
209.15.196.171	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
193.200.80.26	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
64.87.23.55	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.90.147.81	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-22-2016-10:04:08 to 04-22-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.200.80.26	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	30
93.90.147.81	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	20
213.8.145.99	147.237.77.74	Israel	law.idf.il	SQL Injection - Select From	6
209.15.196.171	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
187.245.10.131	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.65.167	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
58.218.211.11	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
187.245.10.131	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.76.201	Ukraine	e.atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.82.78.38	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.211.11	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

04-22-2016-10:04:08 to 04-22-2016-11:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
173.236.241.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
85.75.79.141	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
76.174.87.209	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
89.163.148.58	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.14.243.74	Palestinian Territory, Occupied	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	22
80.40.134.104	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.179	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.234.177.180	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.97.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.67.251.142	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
89.187.219.146	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.179.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
125.238.132.185	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.167.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.130.174.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.156.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.192.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.27.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.164.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
105.44.109.234	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.174.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.202.178	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence		monitor	5
37.26.148.232	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.40.134.103	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.130.174.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-22-2016-10:04:08 to 04-22-2016-11:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.139.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
80.246.136.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
185.32.179.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	7
89.139.253.217	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 89.139.253.217	Block	6
185.32.179.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
65.55.213.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.119.127.129	Ukraine	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 46.119.127.129	Block	3
2.55.12.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.253.217	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
178.137.90.202	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	2
85.65.246.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.156.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.199.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.27.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.95	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
188.161.236.63	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
79.178.111.47	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.178.111.47 (Open Mode)	None	1
197.231.221.211	Liberia	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
79.178.111.47	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.119.127.129	Ukraine	147.237.76.147	chinuch.aka.idf.i	PHP Attempt	Block	1
185.13.47.166	Russian Federation	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 221 cookies	Block	1
87.71.48.246	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/patzar/news/	None	1
199.30.25.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
79.180.104.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
46.119.127.129	Ukraine	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
87.169.99.116	Germany	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/smalim/	Block	1
66.249.65.167	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.142.64.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
131.253.25.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-22-2016-10:04:08 to 04-22-2016-11:04:08