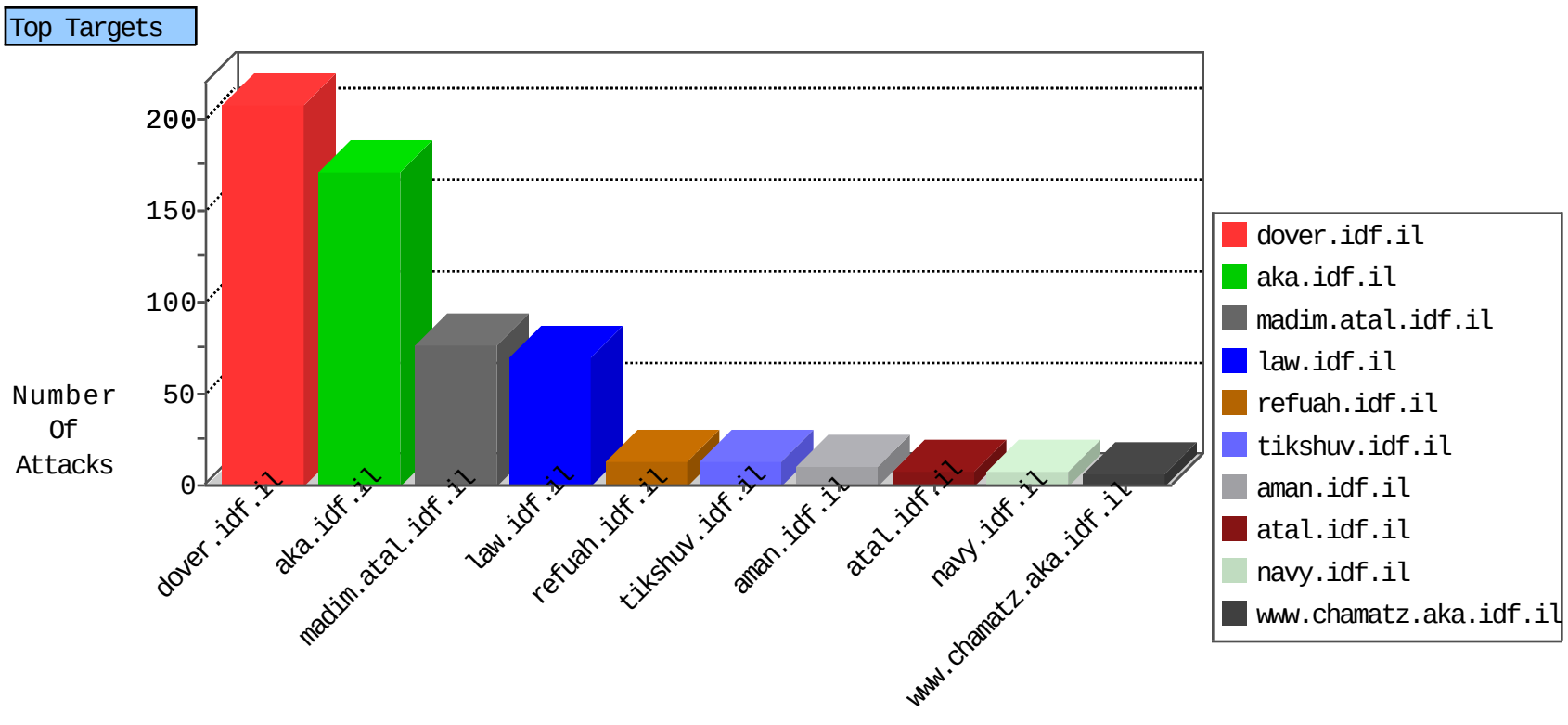
04-01-2015-07:03:03 to 04-01-2015-08:03:03

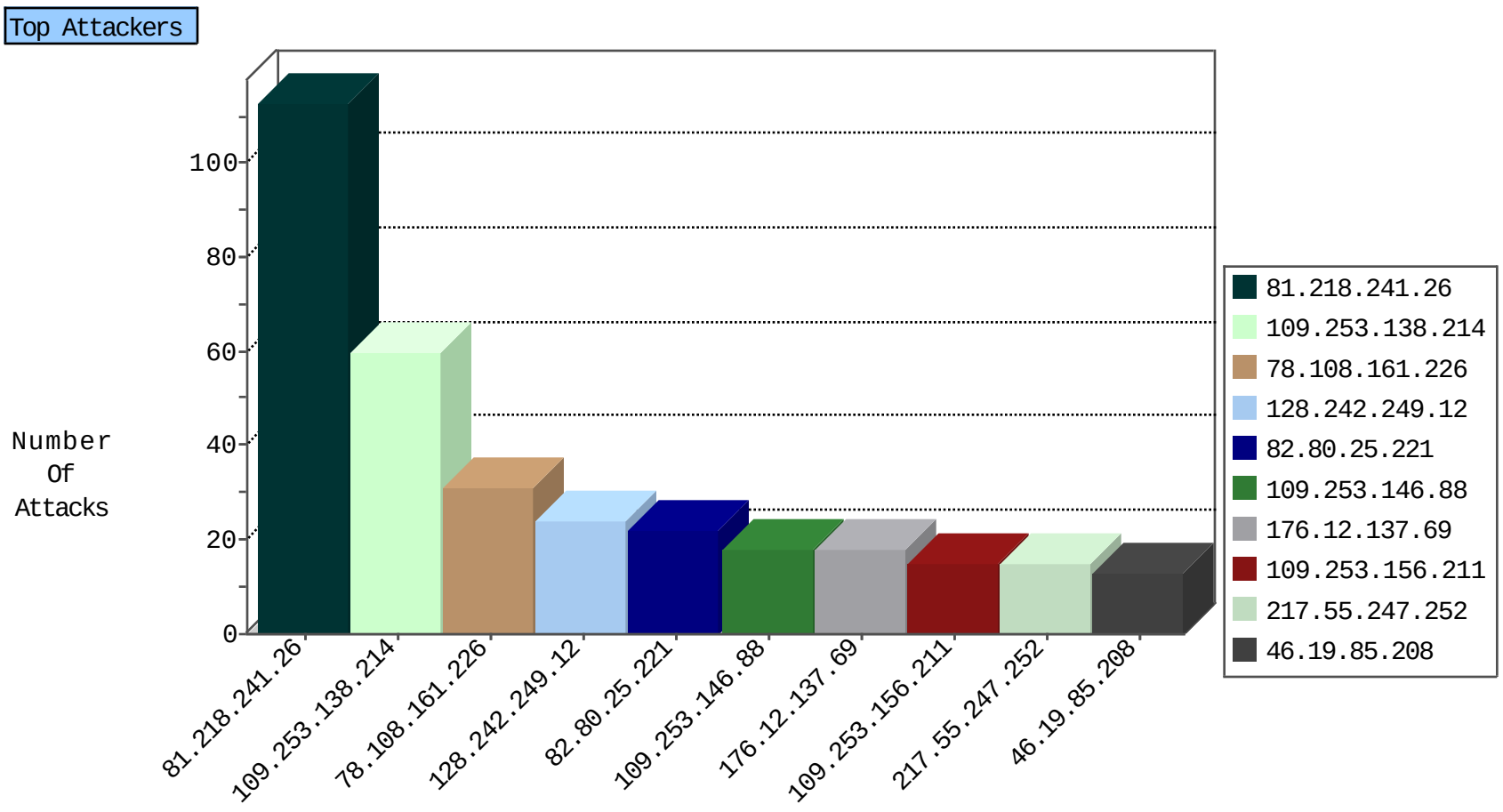
IDF Under Attack
04-01-2015-07:03:03

Top Targets



Top Target

Top Attackers



Top Attackers

04-01-2015-07:03:03 to 04-01-2015-08:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	715
95.172.79.156	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
95.172.79.180	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
89.248.172.57	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.57	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.57	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

04-01-2015-07:03:03 to 04-01-2015-08:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.67.121.85	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
37.26.147.239	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-01-2015-07:03:03 to 04-01-2015-08:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
91.227.71.250	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
192.118.11.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.152	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
221.179.89.90	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
208.124.237.146	Canada	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
5.196.147.122	Germany	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	United States	147.237.76.39	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
119.61.7.43	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
79.182.130.195	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.179.89.90	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
208.124.237.146	Canada	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
208.124.237.146	Canada	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
183.136.216.7	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1

04-01-2015-07:03:03 to 04-01-2015-08:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.12.137.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.146.88	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
217.55.247.252	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.253.135.141	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
81.218.241.26	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
78.108.161.226	Lebanon	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
176.12.149.128	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
173.2.24.83	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.129.150	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	5
78.108.161.226	Lebanon	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.27	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
78.108.161.226	Lebanon	147.237.77.234	halag.idf.il	First packet isn't SYN	drop	drop	4
176.12.144.158	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.253.146.231	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.186.228.25	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	4
98.254.185.23	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
31.186.228.65	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.32	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.61	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.57	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
78.108.161.226	Lebanon	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	3
84.108.236.193	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
31.186.228.86	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.60	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.93	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.88	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.28	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.66	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
31.186.228.24	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.89	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
207.241.237.101	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.62	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.29	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.95	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
84.108.30.220	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
31.186.228.58	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.63	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.30	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.96	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
78.108.161.226	Lebanon	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.138.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.138.214	Block	59
109.253.156.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
73.25.161.71	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
164.138.116.98	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 164.138.116.98	Block	3
80.246.130.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
176.12.143.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
84.108.213.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	2
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	2
180.76.6.59	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-ar/cogat.aspx	Block	1
54.225.104.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
54.83.95.68	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
109.253.159.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.17.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ie-index05.stm	Block	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/insignia/insignia.stm	Block	1
176.12.148.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
164.138.116.98	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 164.138.116.98	Block	1
54.215.43.237	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//navy/	Block	1
2.52.54.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl04.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.253.141.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
180.76.6.130	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-10153-ar/cogat.aspx	Block	1
81.57.102.243	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
61.135.190.71	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
176.12.143.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.148.136.55	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
113.194.129.33	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
91.200.12.28	Ukraine	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/haredim/maslulimlist.aspx	None	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
176.12.150.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/home.asp-link1	Block	1
164.138.116.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/6_s3_	Block	1
54.215.43.237	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/main.stm	Block	1
109.253.146.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
183.15.236.145	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ie-welcome.stm	Block	1
66.249.64.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.142	Block	1
176.12.144.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
113.194.129.33	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.194.129.33	Block	1
54.159.215.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
93.172.51.213	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$rbSearchSites in www.aka.idf.il/main/sachar/	None	1
213.57.142.118	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
176.12.137.187	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
54.221.198.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//hebrew/news/main.stm	Block	1
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.253.149.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
198.20.69.74	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
84.228.6.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __LASTFOCUS in www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	None	1
66.249.64.142	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
176.12.147.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-01-2015-07:03:03 to 04-01-2015-08:03:03