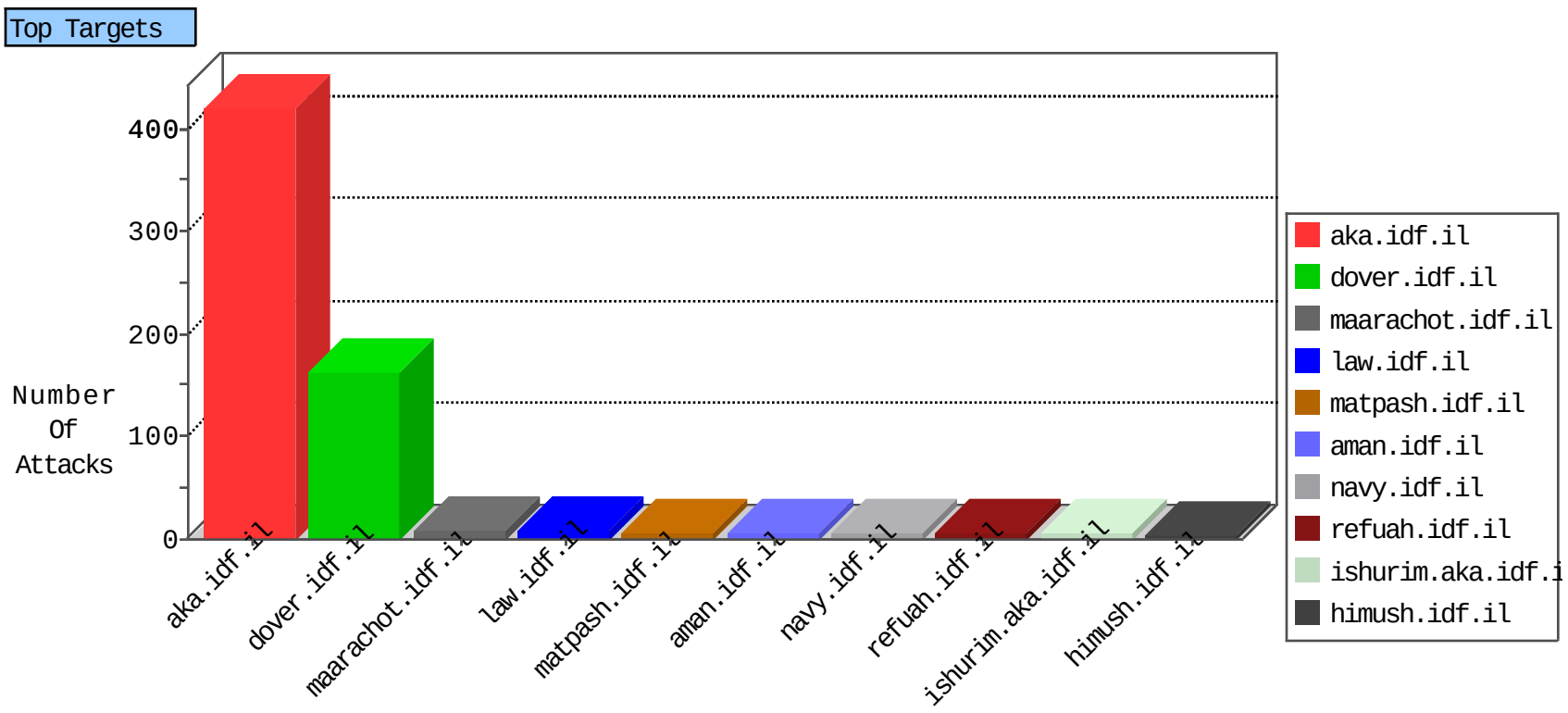
05-09-2015-01:03:01 to 05-09-2015-02:03:01

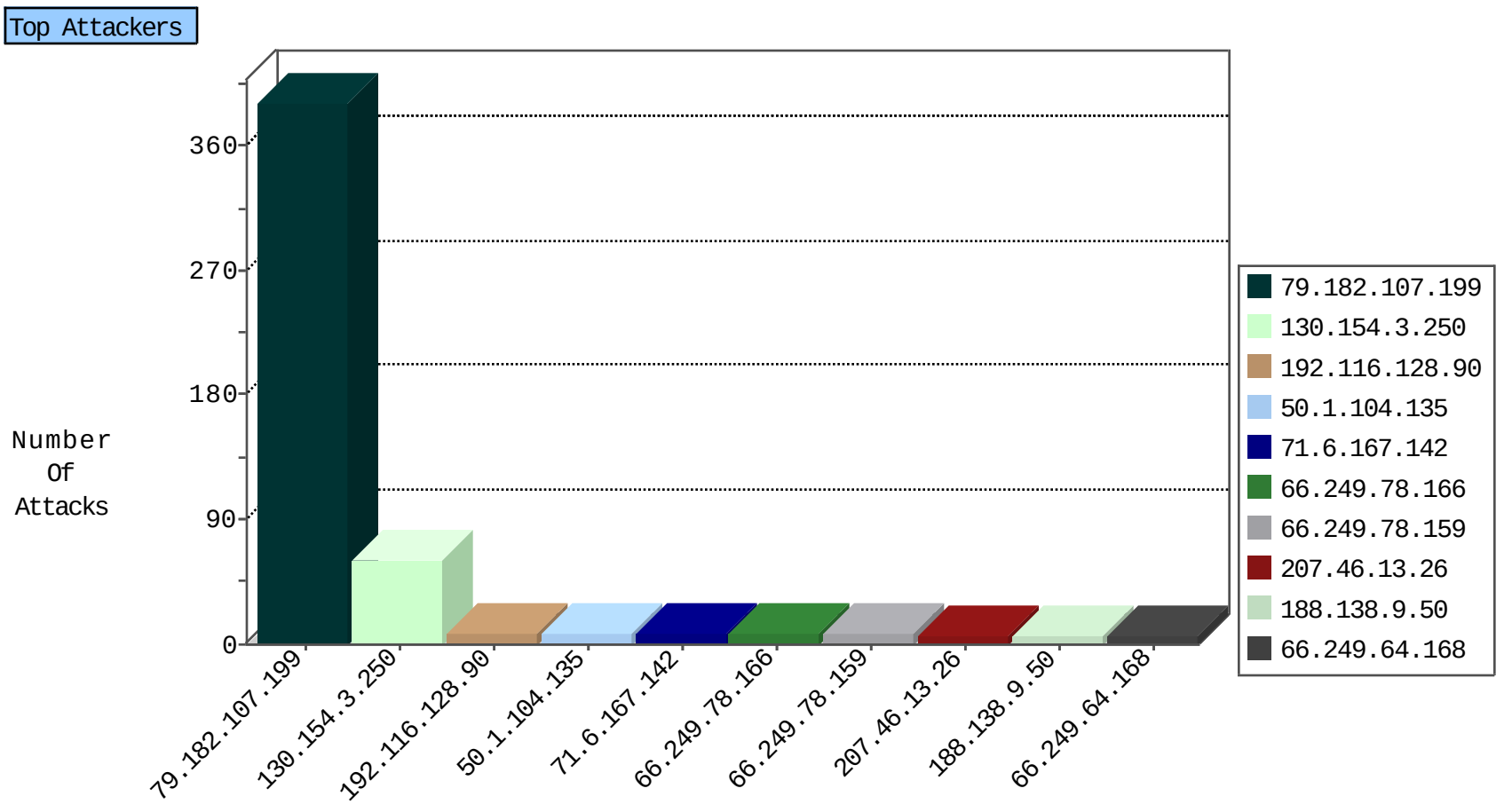
IDF Under Attack
05-09-2015-01:03:01

Top Targets



Top Target

Top Attackers



Top Attackers

05-09-2015-01:03:01 to 05-09-2015-02:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.109	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	166
220.181.108.185	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	29
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
79.178.13.232	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

05-09-2015-01:03:01 to 05-09-2015-02:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
46.121.64.34	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
79.176.13.101	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.119	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-01:03:01 to 05-09-2015-02:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
46.121.64.34	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
218.77.79.43	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
142.54.181.100	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
218.77.79.43	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
128.136.227.196	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
210.61.150.154	Taiwan	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
128.136.227.196	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
198.46.129.71	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
119.226.59.189	India	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
188.165.129.51	Spain	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
92.47.29.12	Kazakstan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
185.75.56.44		147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
175.136.197.37	Malaysia	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
60.18.162.244	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
175.22.14.71	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
175.22.14.71	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
142.54.181.100	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
210.61.150.154	Taiwan	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
128.136.227.196	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
210.61.150.154	Taiwan	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
119.226.59.189	India	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
188.138.9.51	Germany	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
175.136.197.37	Malaysia	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
175.22.14.71	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

05-09-2015-01:03:01 to 05-09-2015-02:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
130.154.3.250	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
192.116.128.90	Israel	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	8
50.1.104.135	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
190.254.237.178	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
68.196.254.209	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
88.198.25.217	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
101.251.236.91	China	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
31.210.187.170	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
128.242.249.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
184.173.183.170	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.125.138.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
50.141.78.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
185.2.101.170	Germany	147.237.0.35	akaws.idf.il	SAM rule	drop	drop	1
188.138.17.205	France	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
96.239.87.24	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
180.62.34.189	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

05-09-2015-01:03:01 to 05-09-2015-02:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.107.199	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.107.199	Block	391
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	4
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
178.137.19.143	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	2
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.26	Block	1
66.249.78.134	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2004/february/03.stm	Block	1
157.55.39.117	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
188.165.129.51	Spain	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.65.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/english/pages/default.aspx	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.107.199	Israel	147.237.72.166	aka.idf.il	Too Many 404: Response Code per Session	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	1
66.249.78.141	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
198.46.129.71	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-4601-he/patzar.aspx	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.162	Block	1
66.249.78.148	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
198.46.129.71	United States	147.237.77.176	matpash.idf.il	Multiple signatures from 198.46.129.71	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6658-he/patzar.aspx	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter 0559c450 in www.aka.idf.il/main/home/default.aspx	None	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/24.stm	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0211-3.stm	Block	1
66.249.67.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/870-6552-he/patzar.aspx	Block	1
157.55.39.199	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
65.55.210.28	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.129.51	Spain	147.237.77.176	matpash.idf.il	Multiple signatures from 188.165.129.51	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/klali.aspx	Block	1

05-09-2015-01:03:01 to 05-09-2015-02:03:01