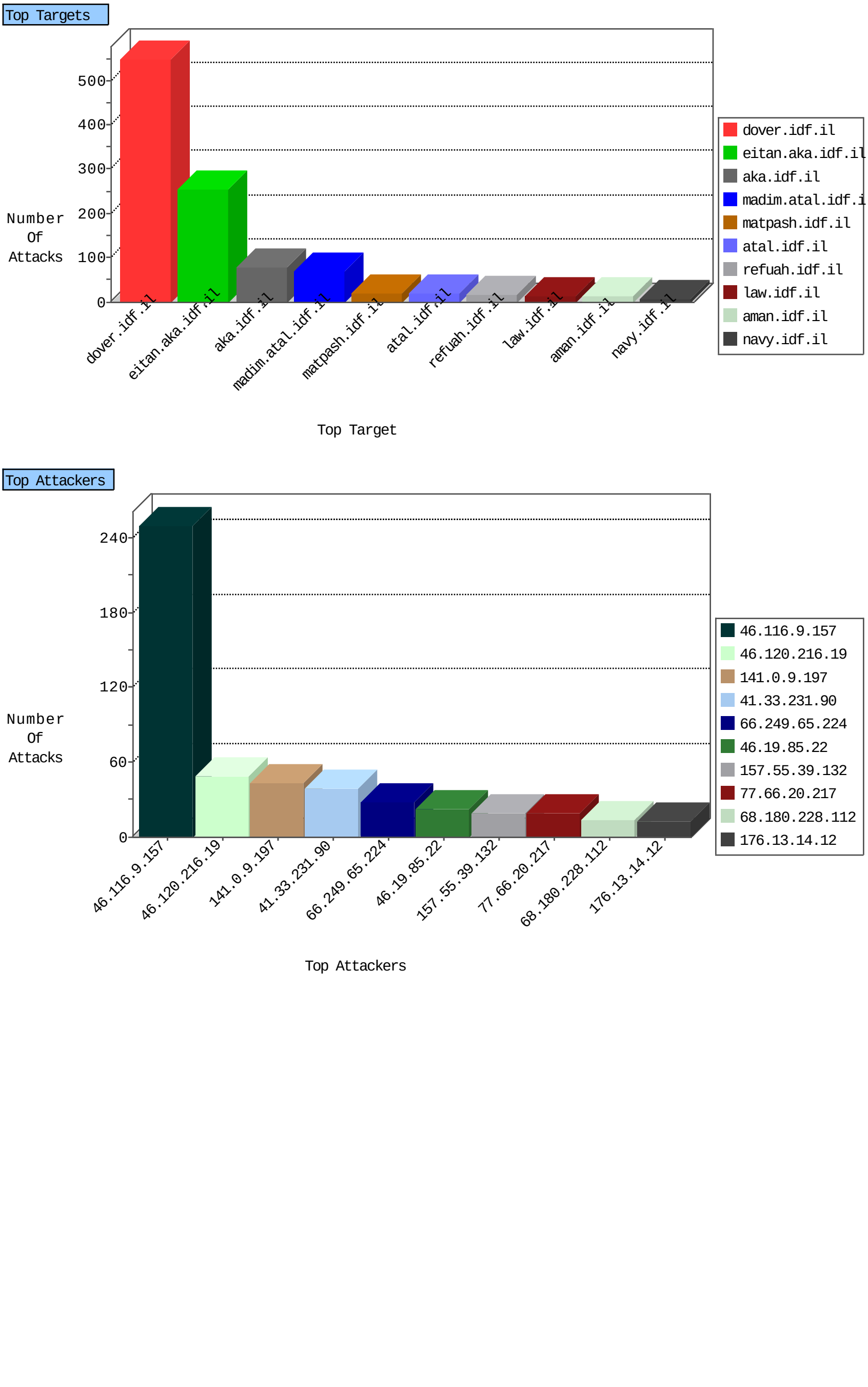
11-21-2015-09:04:00 to 11-21-2015-10:04:00

IDF Under Attack
Daily Report



11-21-2015-09:04:00 to 11-21-2015-10:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3311
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3241
82.166.22.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	92
176.13.14.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	73
2.54.129.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
115.239.228.8	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.8	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
204.42.253.132	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
37.26.149.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
204.42.253.132	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.4	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-21-2015-09:04:00 to 11-21-2015-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-21-2015-09:04:00 to 11-21-2015-10:04:00

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
201.163.164.149	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
188.214.128.12	147.237.76.176	Romania	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
58.213.166.105	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
201.163.164.149	147.237.72.217	Mexico	e.idf.il	ET SCAN Potential SSH Scan	1
201.163.164.149	147.237.72.156	Mexico	aman.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.77.170	Italy	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
201.163.164.149	147.237.72.167	Mexico	ishurim.aka.idf.i	ET SCAN Potential SSH Scan	1

11-21-2015-09:04:00 to 11-21-2015-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.9.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.116.9.157	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
157.55.39.132	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.60	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.102.9.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.186.228.59	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.177.159.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.186.228.96	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.100.113.241		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.180.20.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.200	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.100.85.105		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
54.237.147.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.166.22.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.187.221.14	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.30.25.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.22.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.139.161	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.149.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
64.233.172.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
131.253.25.192	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.192	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.12	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.187.221.11	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.119.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.22.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.92	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
87.69.246.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.92	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.138.212.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
157.55.39.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
81.218.229.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.16.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.65.108.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.247.36.80	Netherlands	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

11-21-2015-09:04:00 to 11-21-2015-10:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.9.157	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.116.9.157	Block	230
46.120.216.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	7
176.13.13.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	6
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	4
46.120.216.19	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.216.19	Block	4
176.12.137.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
77.126.62.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.56	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	2
81.218.229.198	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.229.198	Block	2
46.19.85.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
2.54.137.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	2
2.54.183.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.247.58	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/login/	Block	2
109.67.213.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.197.125	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/main/home/default.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
71.17.140.224	Canada	147.237.72.156	aman.idf.il	E-mail collector robots 14	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
213.139.53.6	Jordan	147.237.77.176	matpash.idf.il	Multiple Malformed URL from 213.139.53.6	Block	1
84.108.173.106	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
5.28.191.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/×©×§×• ×¤×™×ª×ª 9	Block	1
141.212.122.160	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
89.187.221.13	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
176.13.2.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
71.17.140.224	Canada	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.116.9.157	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
213.139.53.6	Jordan	147.237.77.176	matpash.idf.il	Multiple Unknown HTTP Request Method from 213.139.53.6	Block	1
84.228.21.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
5.29.191.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
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	1
141.212.122.160	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3197.pdf	Block	1
81.218.229.198	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/	Block	1
46.19.85.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.139.53.6	Jordan	147.237.77.176	matpash.idf.il	Abnormally Long Request request version	Block	1
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-21-2015-09:04:00 to 11-21-2015-10:04:00