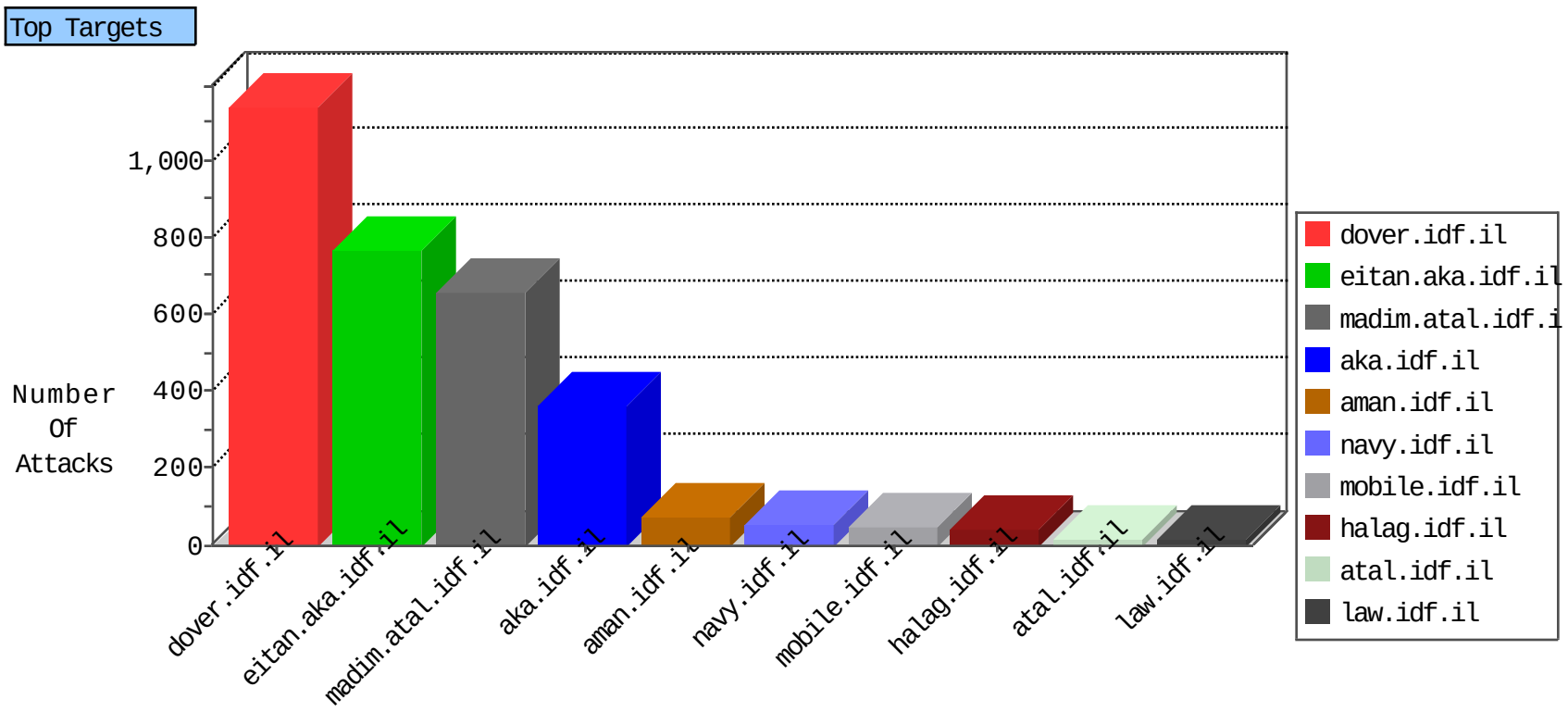
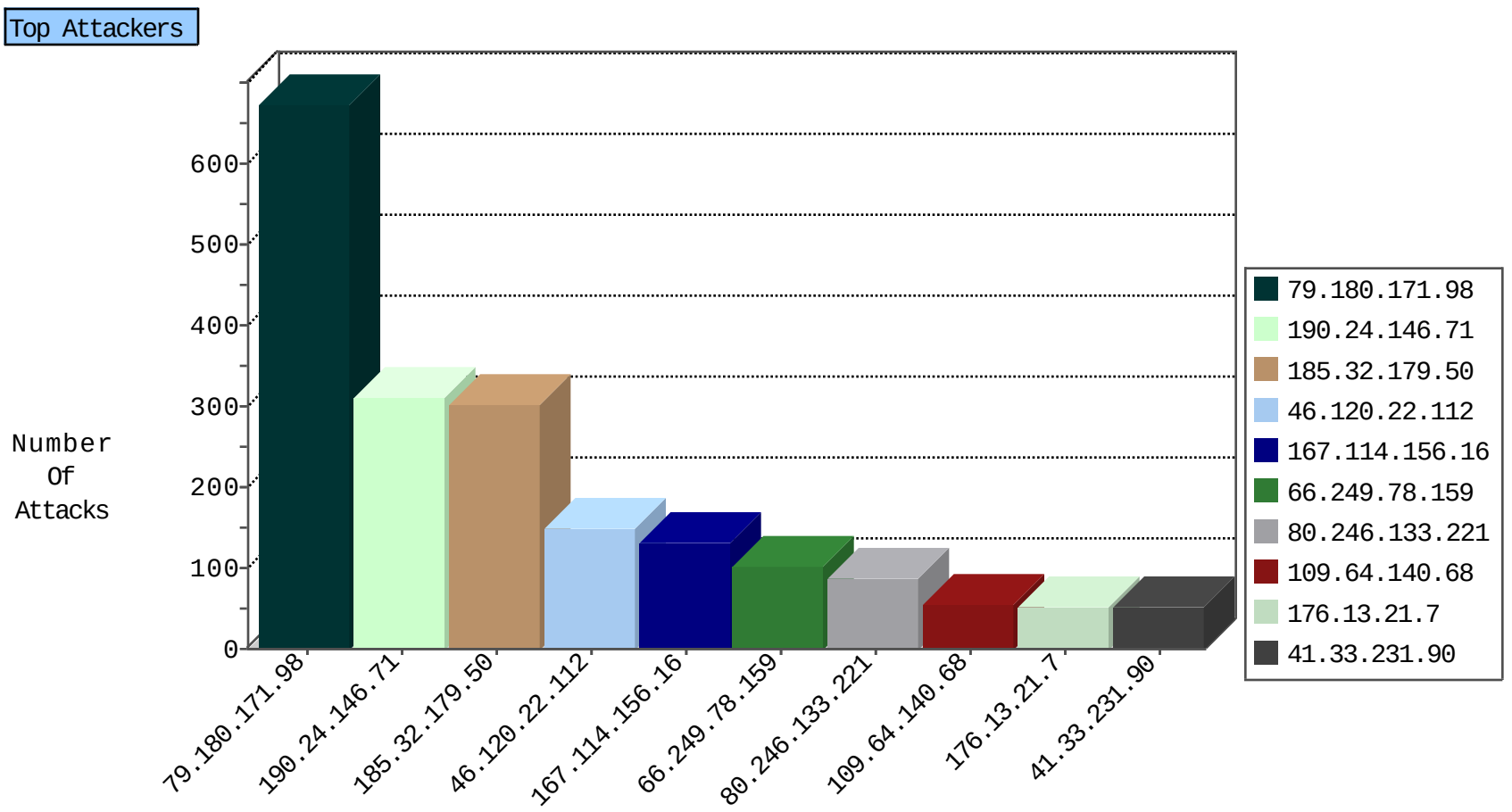
11-21-2015-21:04:07 to 11-21-2015-22:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-21-2015-21:04:07 to 11-21-2015-22:04:07

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	HTTP-POST-Segmented-DoS	dest-reset	7262
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3089
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1347
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	184
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48
31.44.133.252	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
79.182.51.161	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
149.88.7.175	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
31.181.238.173	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
185.3.144.120	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.180.63.246	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.26.147.230	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.29.118.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
115.239.228.8	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	1

11-21-2015-21:04:07 to 11-21-2015-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-21-2015-21:04:07 to 11-21-2015-22:04:07

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
58.250.164.246	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
58.250.164.246	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
121.78.125.181	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.250.164.246	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
74.117.209.135	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
210.50.197.154	147.237.0.17	Australia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
210.50.197.154	147.237.0.17	Australia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.50	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.250.164.246	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
176.12.140.79	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
58.250.164.246	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
74.117.209.136	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
210.50.197.154	147.237.0.17	Australia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.61	United States	e.cogat.idf.il	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.53	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1

11-21-2015-21:04:07 to 11-21-2015-22:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.171.98	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	585
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	311
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
80.246.130.123	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
80.246.133.221	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	31
37.26.149.174	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
213.57.142.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
95.86.126.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
213.57.142.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
46.19.86.200	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
109.67.148.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.75.106		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.165.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.106.218		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.66.154.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
85.65.81.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.179.119.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.136.235	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	10
100.100.7.189		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.136.235	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
176.4.33.173	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.18.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.66.190.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.179.180.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.174.154.28	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
188.120.148.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.154.3.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.51.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.64.172.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.68.33.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.130.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
149.88.7.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.211.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.120.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.174	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
100.100.107.242		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
132.64.24.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.1.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6

11-21-2015-21:04:07 to 11-21-2015-22:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	151
185.32.179.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	136
46.120.22.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
79.180.171.98	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.171.98	Block	88
109.64.140.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
80.246.133.221	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
176.13.21.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
46.120.22.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
5.29.145.216	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.145.216	Block	17
37.26.149.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
84.228.222.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
46.19.86.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
185.32.179.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	7
84.111.244.23	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	6
84.111.161.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
74.208.16.113	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 74.208.16.113	Block	5
79.183.130.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.183.27	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	3
212.34.11.77	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.11.77	Block	3
176.12.137.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.116.130.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.111.244.23	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/	Block	3
212.34.11.77	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.11.77	Block	3
2.54.144.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.144.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
164.138.118.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.65.209.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.137.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.244.23	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.111.244.23	Block	2
176.13.12.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.34.11.77	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.11.77	Block	2
2.54.139.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.16.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.117.63.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.81.38.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.117.182.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
194.187.168.19	Poland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8853-he/refuah.aspx	Block	1
183.79.219.188	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.36.231.143	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
157.55.39.142	United States	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/kamlar/contact/default.asp	Block	1
82.166.212.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
212.34.11.77	Jordan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method er.aspx in URL www.idf.ilhttp/1.1	Block	1
79.182.60.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/adguard-ajax-api/api	Block	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
109.65.120.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.136.40.100	United Kingdom	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/test/wp-admin/	Block	1

11-21-2015-21:04:07 to 11-21-2015-22:04:07