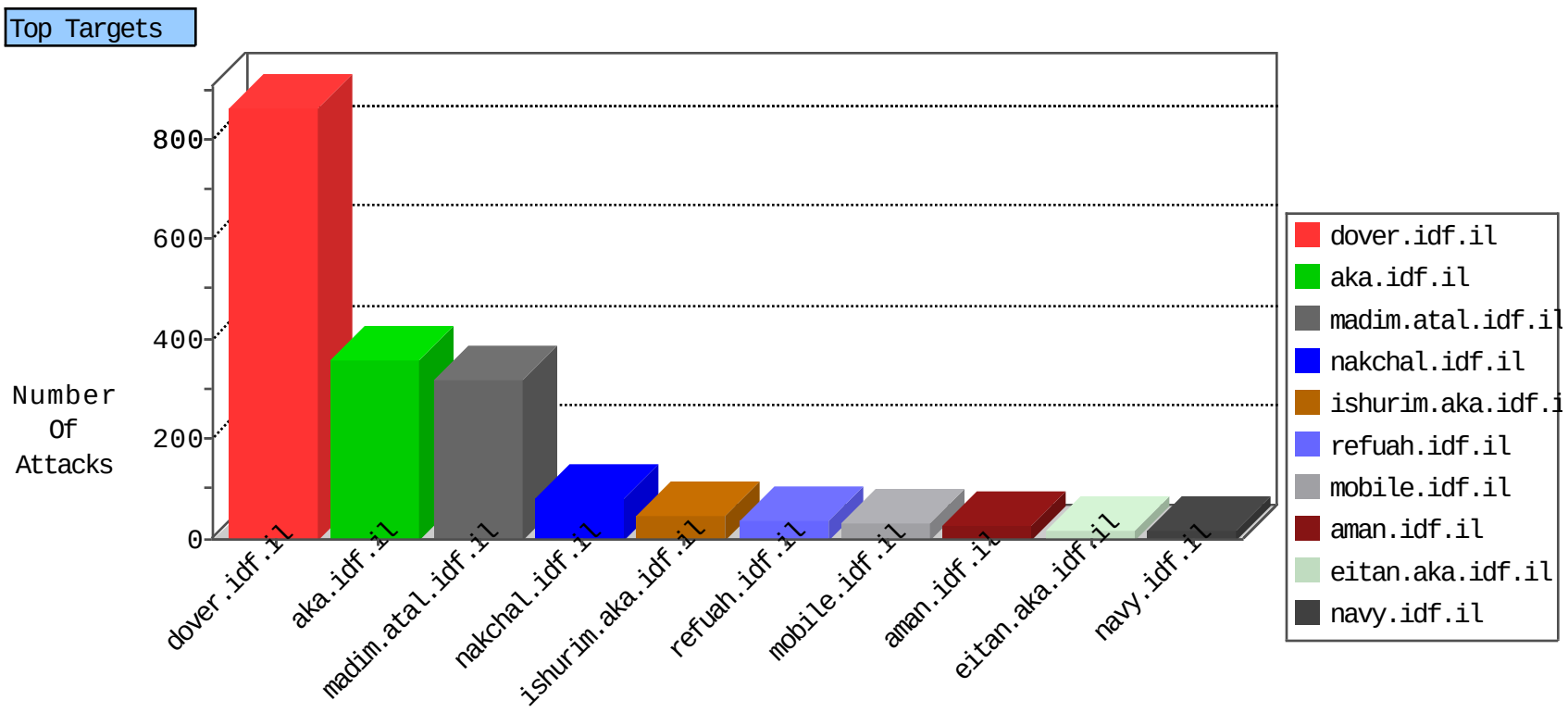
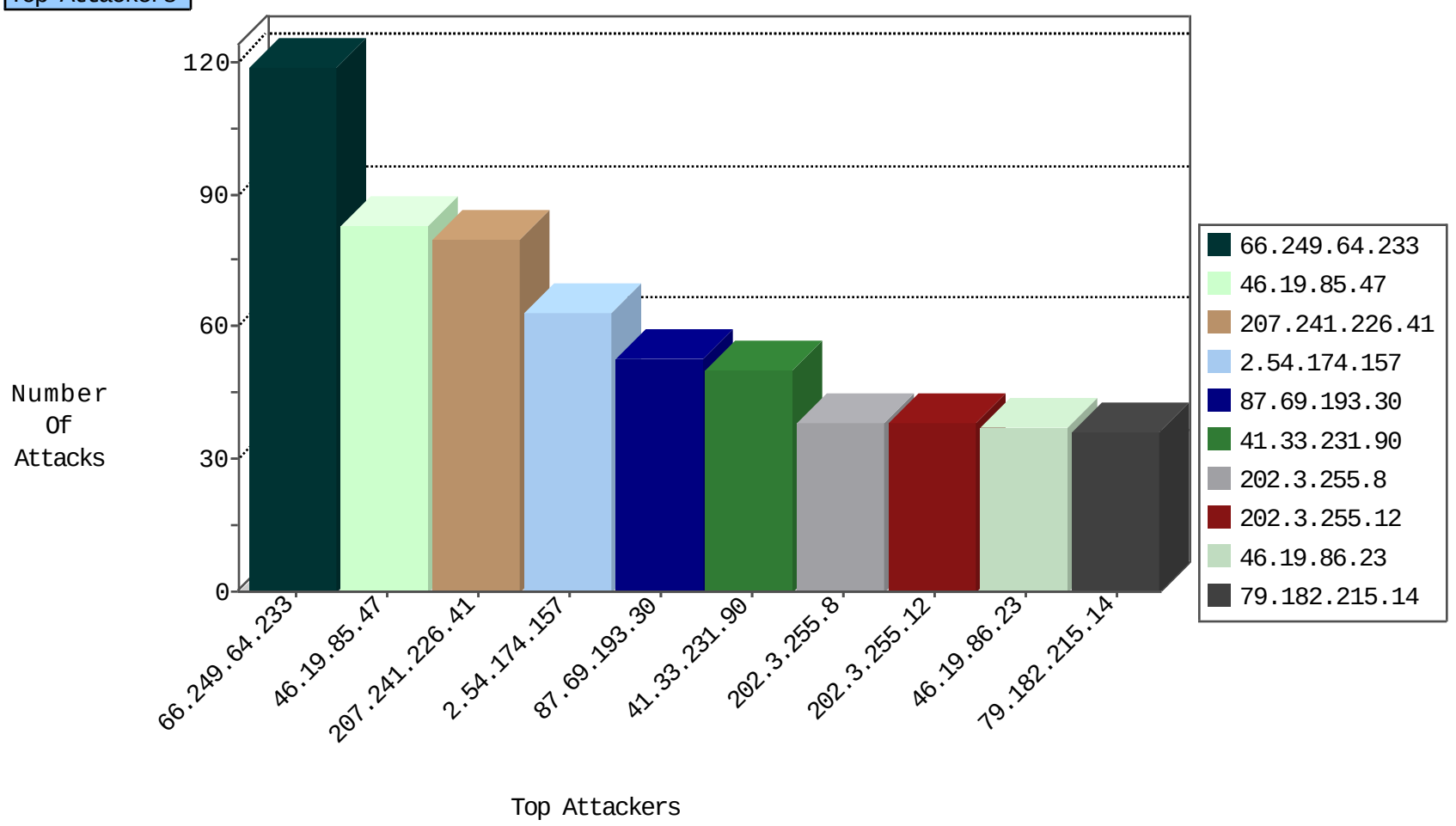
11-20-2015-12:04:09 to 11-20-2015-13:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-20-2015-12:04:09 to 11-20-2015-13:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.23.48.252	Denmark	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3377
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
185.32.179.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	117
10.0.0.1		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
62.219.99.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
37.26.149.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.66.178.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
79.177.131.81	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
185.32.179.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
10.0.0.11		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.45.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
95.128.56.36	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.174.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-20-2015-12:04:09 to 11-20-2015-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.15.235	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-20-2015-12:04:09 to 11-20-2015-13:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-20-2015-12:04:09 to 11-20-2015-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	106
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
109.67.144.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
37.26.146.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
172.56.34.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.10.195		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
194.112.8.5		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	17
100.100.77.33		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
5.29.217.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.202.219.72	Cameroon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
82.80.27.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
82.80.27.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.178.35.85	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.138.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
2.54.169.12	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.183.163.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.207.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.120.145.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
100.100.16.15		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
109.64.41.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.108.27.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.67.165.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.120.145.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
149.88.22.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.180.173.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.250.80.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.125.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.57.223	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.117.19.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.64.157.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.2.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.120.145.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.3.146.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.134.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.178.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.41	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	77
2.54.174.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
87.69.193.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
2.54.14.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
87.69.166.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	8
212.179.230.11	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	8
212.179.230.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	8
217.194.206.122	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 217.194.206.122	Block	7
95.86.76.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
176.13.22.165	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	4
79.182.201.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
93.172.70.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
2.54.128.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.182.215.14	Block	3
46.19.85.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.23.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.182.215.14	Block	3
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.182.215.14	Block	3
185.32.179.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.182.215.14	Block	3
2.54.135.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.46.39.58	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.182.215.14	Block	3
176.13.20.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.127.255.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.182.215.14	Block	2
31.168.68.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.25.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
207.241.226.41	United States	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	2
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.182.215.14	Block	2
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	2
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.108.47.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
46.19.86.179	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/205-he/patzar.aspx	Block	2
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.182.215.14	Block	2
109.65.16.33	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
176.13.5.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.182.215.14	Block	2
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
185.3.146.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.157.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.157.56	Block	1
79.183.155.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.145.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.215.14	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.182.215.14	Block	1
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-20-2015-12:04:09 to 11-20-2015-13:04:09