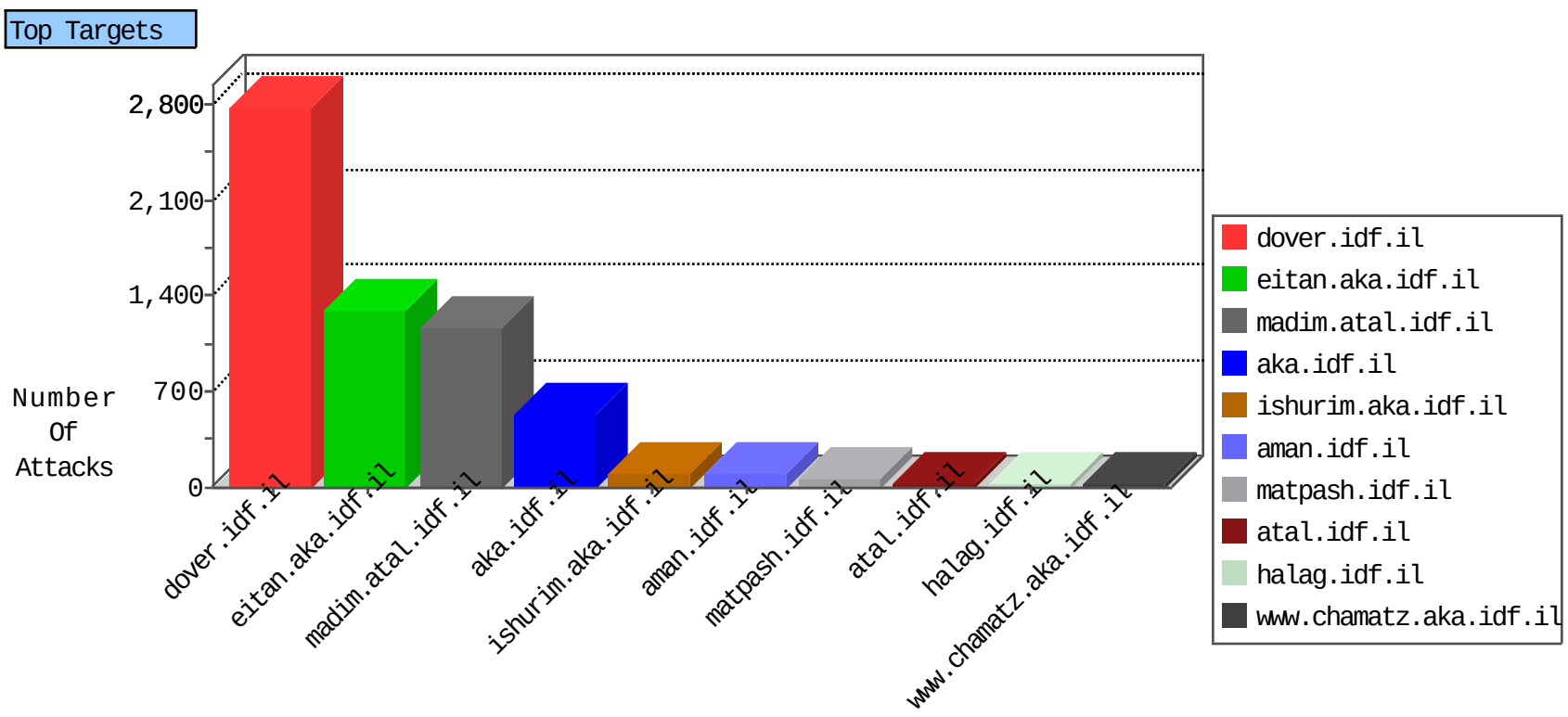
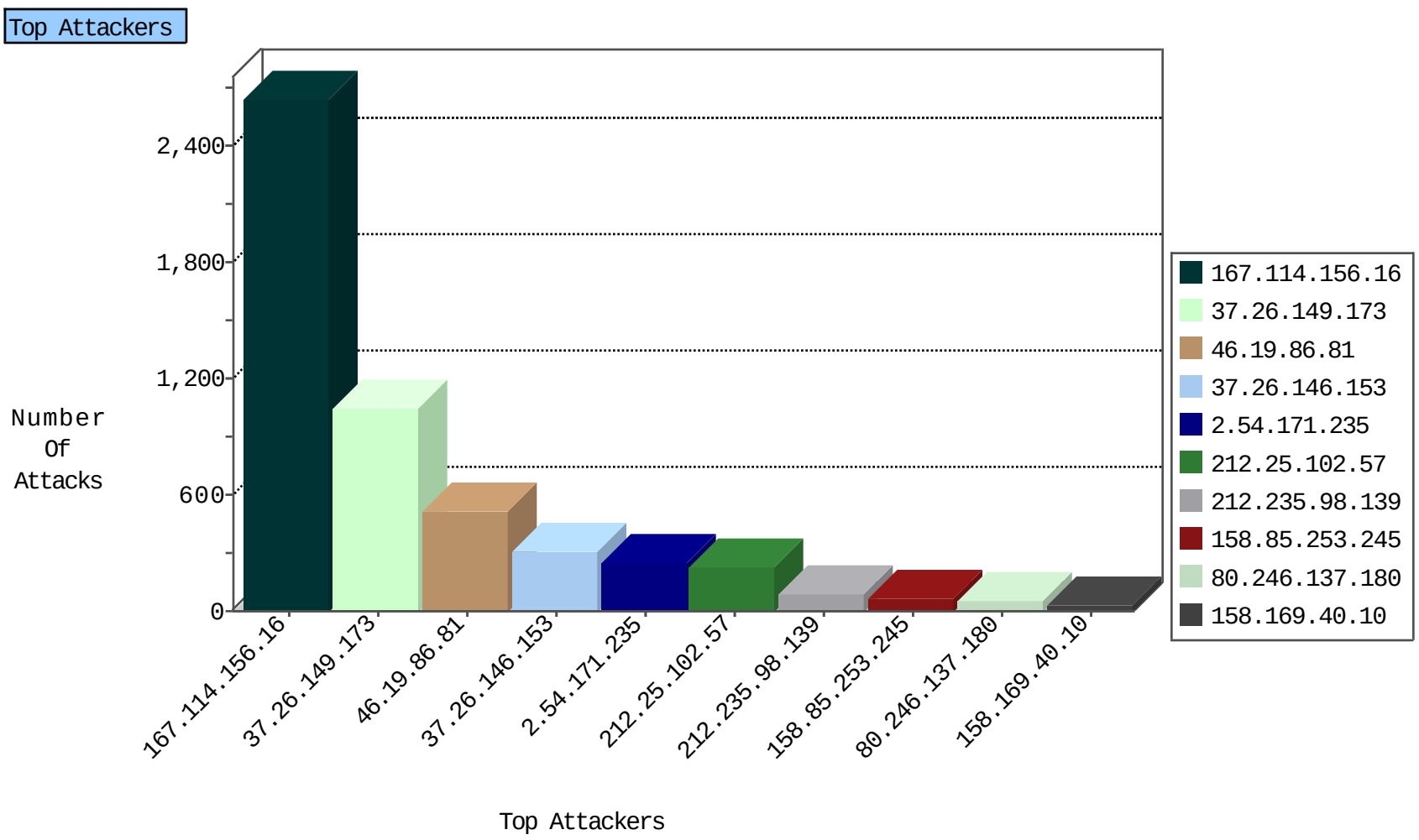
12-09-2015-10:04:05 to 12-09-2015-11:04:05

IDF Under Attack
Daily Report





12-09-2015-10:04:05 to 12-09-2015-11:04:05

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	DOS-Tool-SwitchbladG	dest-reset	3415
45.32.246.5		147.237.77.226	www.chamatz.aka.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	4
24.19.110.22	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
125.202.88.129	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
87.118.124.186	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

12-09-2015-10:04:05 to 12-09-2015-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.85.253.245	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	15
66.76.174.2	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
158.85.253.245	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
158.85.253.245	United States	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
69.12.70.34	United States	147.237.77.205	prisha.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1

12-09-2015-10:04:05 to 12-09-2015-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
158.85.253.245	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	35
66.76.174.2	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	15
134.191.232.71	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
212.179.227.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.210.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.226.206.204	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.181.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.111.59.158	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN Potential SSH Scan	1
187.111.59.158	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.117.174.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.111.59.158	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.160.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.114	147.237.77.233	Ukraine	atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
188.226.206.204	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.12.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.111.59.158	147.237.77.19	Brazil	law-forum.idf.il	ET SCAN Potential SSH Scan	1
79.176.211.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.111.59.158	147.237.76.38	Brazil	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
187.111.59.158	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
162.201.188.183	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.134.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.107.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 1024	1

12-09-2015-10:04:05 to 12-09-2015-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.173	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	864
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	85
80.246.137.180	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
158.169.40.10	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.22.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.85.254	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
212.179.224.209	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	17
46.19.85.174	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
132.64.27.72	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
183.79.221.20	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
176.13.11.198	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
84.94.221.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
84.94.221.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
77.126.98.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.200.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
138.134.102.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.246.137.180	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
132.64.27.72	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
176.13.10.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.109.139.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
176.13.10.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.64.25.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.25.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.153	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
158.169.150.8	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
77.127.24.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
158.169.150.9	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
5.28.158.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.58.80.11	Netherlands	147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
5.28.158.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.153	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.130.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.54	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
158.169.150.4	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.207	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
158.169.40.6	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
213.57.130.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
87.69.223.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.59.244	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
158.169.40.7	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
49.201.164.20	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.182.111.25	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

12-09-2015-10:04:05 to 12-09-2015-11:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	304
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	217
37.26.149.173	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	183
37.26.146.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	157
2.54.171.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	133
37.26.146.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	125
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	107
2.54.171.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
2.54.171.235	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.171.235	Block	32
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
37.26.146.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	22
176.13.17.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
87.68.247.158	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	15
176.13.2.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
176.13.7.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
80.246.136.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	4
176.12.147.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	3
176.13.22.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.65.111.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	2
176.12.140.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.12.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.95.255.130	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.143.158.216	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	2
85.250.32.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.111.6.81	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
183.79.221.20	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.221.20	Block	1
2.54.17.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
52.31.215.67	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.102.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.174	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
149.78.169.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
185.120.125.34		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.32.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.183.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.228.35.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.221.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
134.191.232.70	Israel	147.237.76.30	himush.idf.il	Unknown Parameter amp;rnd in www.chimush.atal.idf.il/shared/ajax/createcaptchaimage.aspx	None	1
77.127.86.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.101	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1

12-09-2015-10:04:05 to 12-09-2015-11:04:05