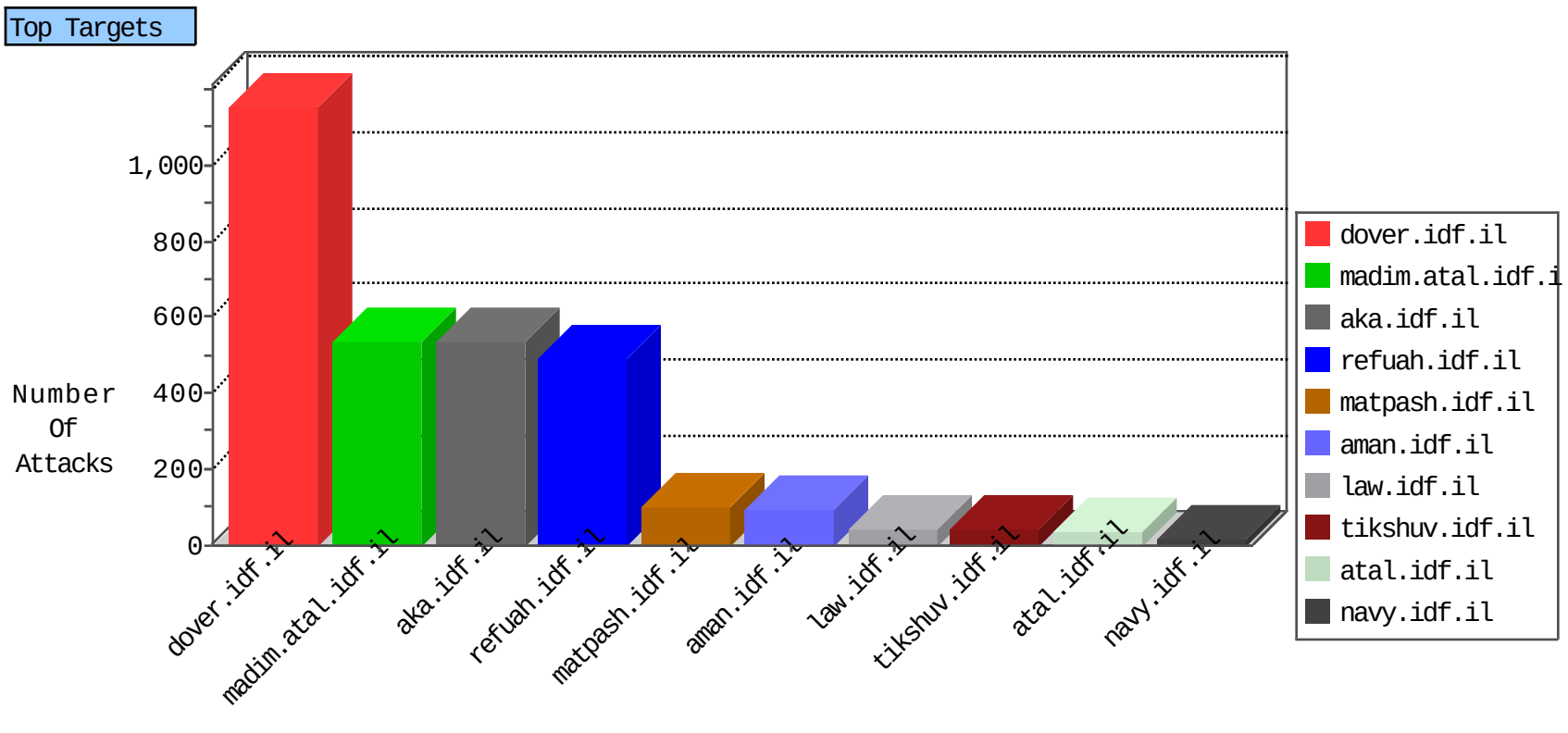
11-24-2015-16:04:05 to 11-24-2015-17:04:05

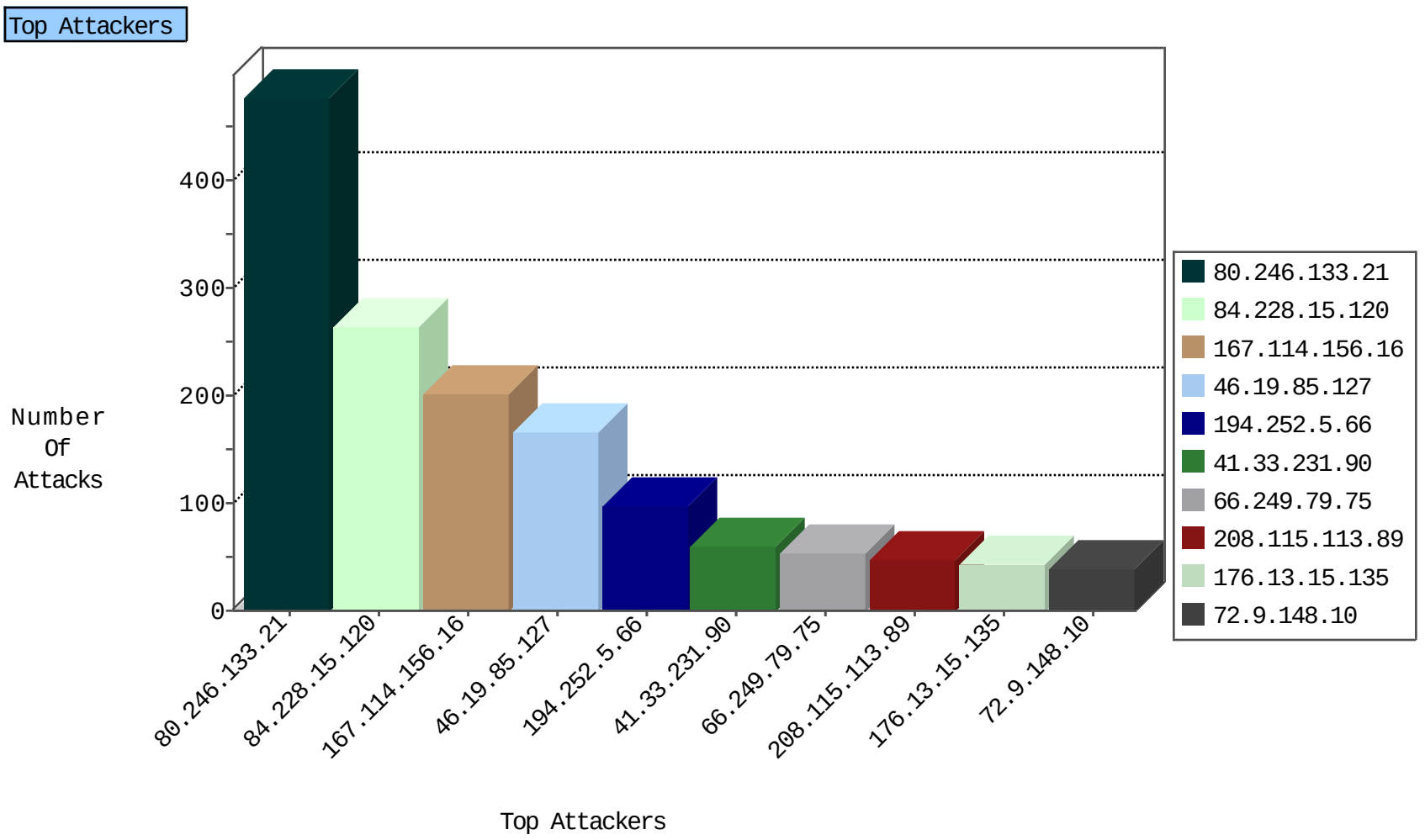
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-24-2015-16:04:05 to 11-24-2015-17:04:05

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	HTTP-POST-Segmented-DoS	dest-reset	6386
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	5316
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2132
66.249.78.96	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	107
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	18
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
81.218.74.164	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
66.249.79.75	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

11-24-2015-16:04:05 to 11-24-2015-17:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-24-2015-16:04:05 to 11-24-2015-17:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.52.172.223	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	13
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
93.173.0.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.162.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
46.19.86.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.33.129.103	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.12.147.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
119.109.35.4	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.60.175	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
84.229.38.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.213.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.76.42	Germany	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.230.141.115	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
199.180.133.185	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
194.29.32.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
124.219.246.33	147.237.8.24	Japan	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.67.23.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-24-2015-16:04:05 to 11-24-2015-17:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	470
194.252.5.66	Finland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	91
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
52.34.45.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
208.54.85.249	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
100.100.46.32		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	26
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
100.100.32.249		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
100.100.41.196		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.22.193		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
188.138.9.49	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.31.22		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.66.161		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.112.41		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.102.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
131.253.25.147	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.130.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
37.26.146.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.112.41		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
78.108.169.25	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.182	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.57.134.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.58	Israel	147.237.72.166	aka.idf.il	HTTP Format Sizes	'Cookie' header length exceeded maximum allowed length	monitor	9
109.65.139.57	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
70.39.187.108	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
173.252.115.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.57.134.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
157.55.39.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.168.28.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8

11-24-2015-16:04:05 to 11-24-2015-17:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.15.120	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.15.120	Block	127
84.228.15.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.13.15.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
84.228.15.120	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 84.228.15.120	Block	29
46.19.86.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
31.168.29.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.54.165.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
79.176.110.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
176.13.9.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.154.91.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
109.160.237.178	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.160.237.178	Block	4
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.111.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
109.66.61.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
192.117.153.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined	Block	2
79.179.22.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.22.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.130.215	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.130.215	Block	2
66.249.66.109	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
31.168.28.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.151	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.149.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.175.0.137	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
80.246.137.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/m/templates/getfile/getfile.aspx	Block	1
109.160.237.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.64.247.70	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	1
93.173.178.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.199.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.176.198.134	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
176.13.17.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.93.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1
149.78.112.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
31.168.152.83	Israel	147.237.0.34	tikshuv.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 31.168.152.83	Block	1
84.108.237.176	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docIyad in www.aka.idf.il/main/giyus/general.aspx	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/tehoor4.aspx	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
5.28.143.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
80.246.130.54	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 80.246.130.54	Block	1
185.3.146.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
89.138.250.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-24-2015-16:04:05 to 11-24-2015-17:04:05