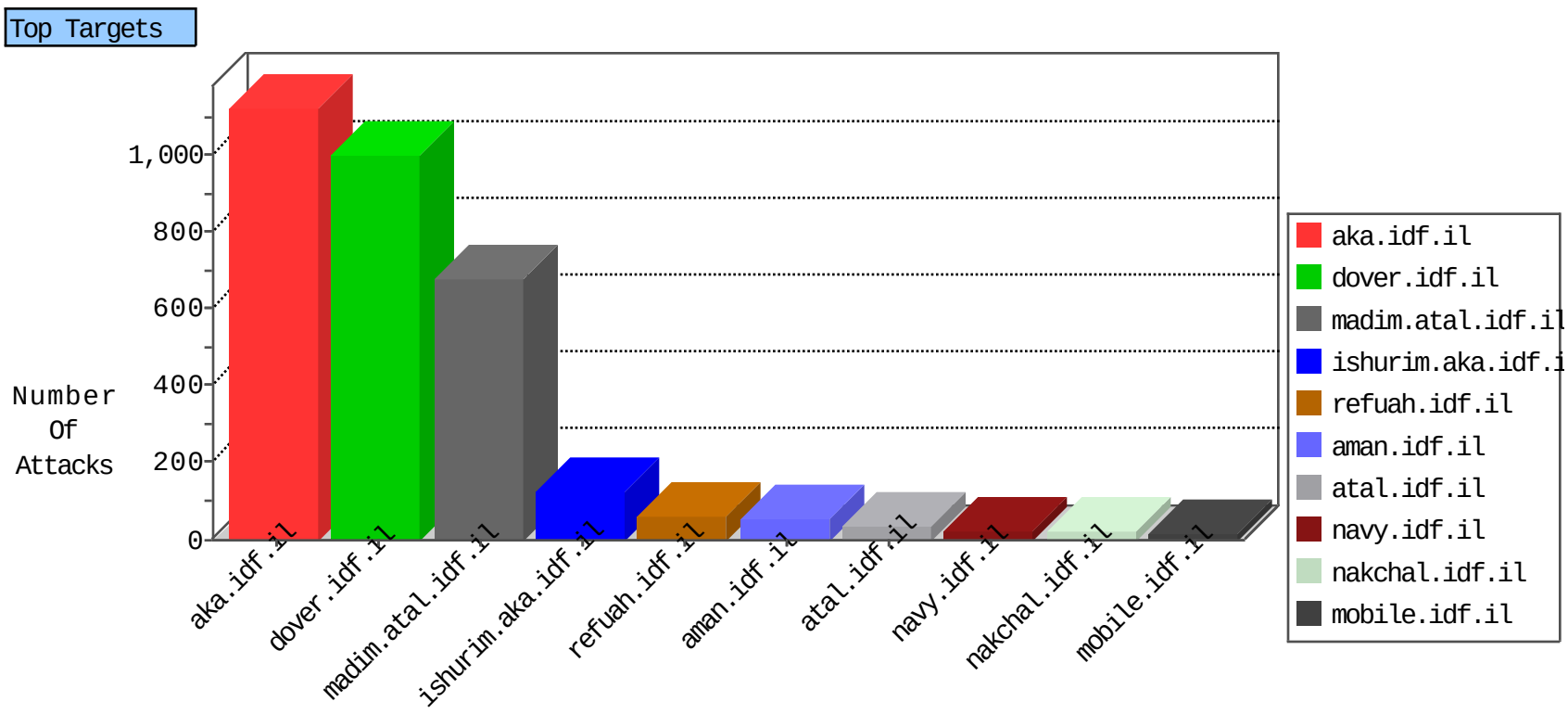
11-22-2015-09:04:06 to 11-22-2015-10:04:06

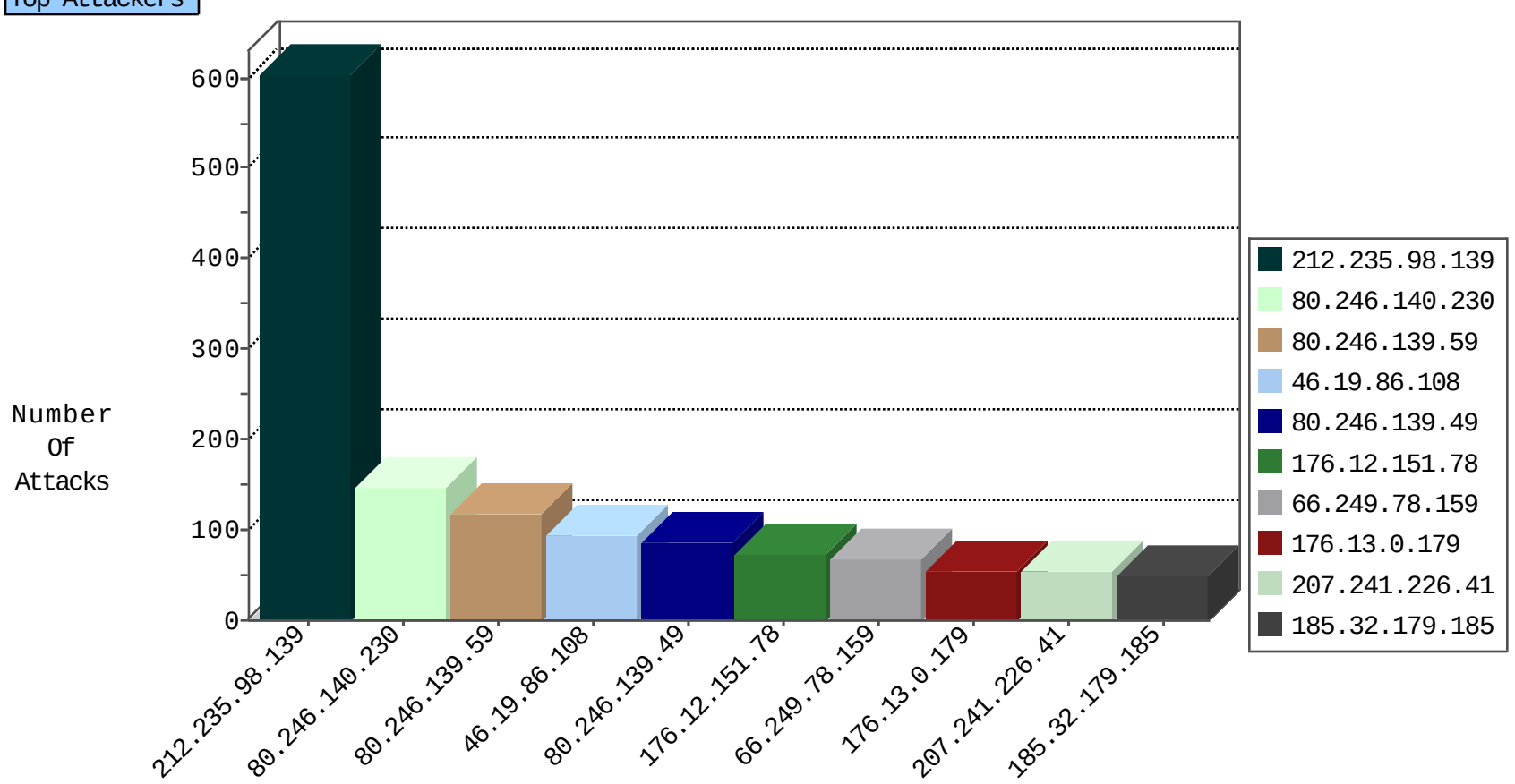
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-22-2015-09:04:06 to 11-22-2015-10:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.9.120	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	77
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	76
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	31
46.19.85.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
176.12.137.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
212.25.103.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
204.93.154.201	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	7
109.65.81.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
176.13.13.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.121.41.50	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.86.106	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.86.114	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.170	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.199.93.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
71.6.158.166	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
2.52.22.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.183.15.18	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.4.193.203	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
95.35.184.209	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.121.41.50	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
195.200.205.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
100.100.50.148		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-22-2015-09:04:06 to 11-22-2015-10:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.138.10	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
149.78.2.151	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
111.206.116.217	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
46.120.35.171	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
209.88.198.1	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-22-2015-09:04:06 to 11-22-2015-10:04:06

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	2
46.151.55.35	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
109.65.149.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.125.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.214.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.6.150.158	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.11.120	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
176.13.20.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.164.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.69.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-22-2015-09:04:06 to 11-22-2015-10:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	605
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
207.241.226.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
46.19.85.218	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	43
174.90.223.60	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
100.100.2.48		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
2.52.55.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.52.180.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.142.201.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
37.142.201.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
100.100.74.51		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
100.100.38.208		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
95.86.118.139	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.201.170.252	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.13.5.169	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
37.26.146.138	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
86.108.24.237	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
93.172.14.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.12.146.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.33.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.59	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
91.197.103.1	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.56.125		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.65.81.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.186.97.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
176.12.146.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.183.15.18	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.186.97.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.167.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
100.100.50.148		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.0.179	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
46.19.85.170	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.126.88.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.175.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.79	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

11-22-2015-09:04:06 to 11-22-2015-10:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
80.246.140.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
80.246.139.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
80.246.139.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
80.246.139.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
176.12.151.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
80.246.140.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
176.13.0.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
185.32.179.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
80.246.140.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	31
80.246.139.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	22
185.32.179.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	15
176.12.151.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
46.121.67.244	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.67.244	Block	14
46.19.86.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.181.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
207.241.226.41	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
176.13.20.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.7.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.115.177.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	3
176.13.7.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.137.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
207.241.226.41	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	3
157.55.39.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.75	Block	2
46.19.85.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.109.33.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.149.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.47.88	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	2
95.86.118.139	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
85.250.144.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
31.210.186.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
99.157.74.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	2
207.241.226.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/piwik.php	Block	1
109.186.46.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
192.118.11.120	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.137	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
87.69.28.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
62.219.187.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 62.219.187.197	None	1
176.12.146.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.143.172.93	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
80.246.136.53	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
204.93.154.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1

11-22-2015-09:04:06 to 11-22-2015-10:04:06