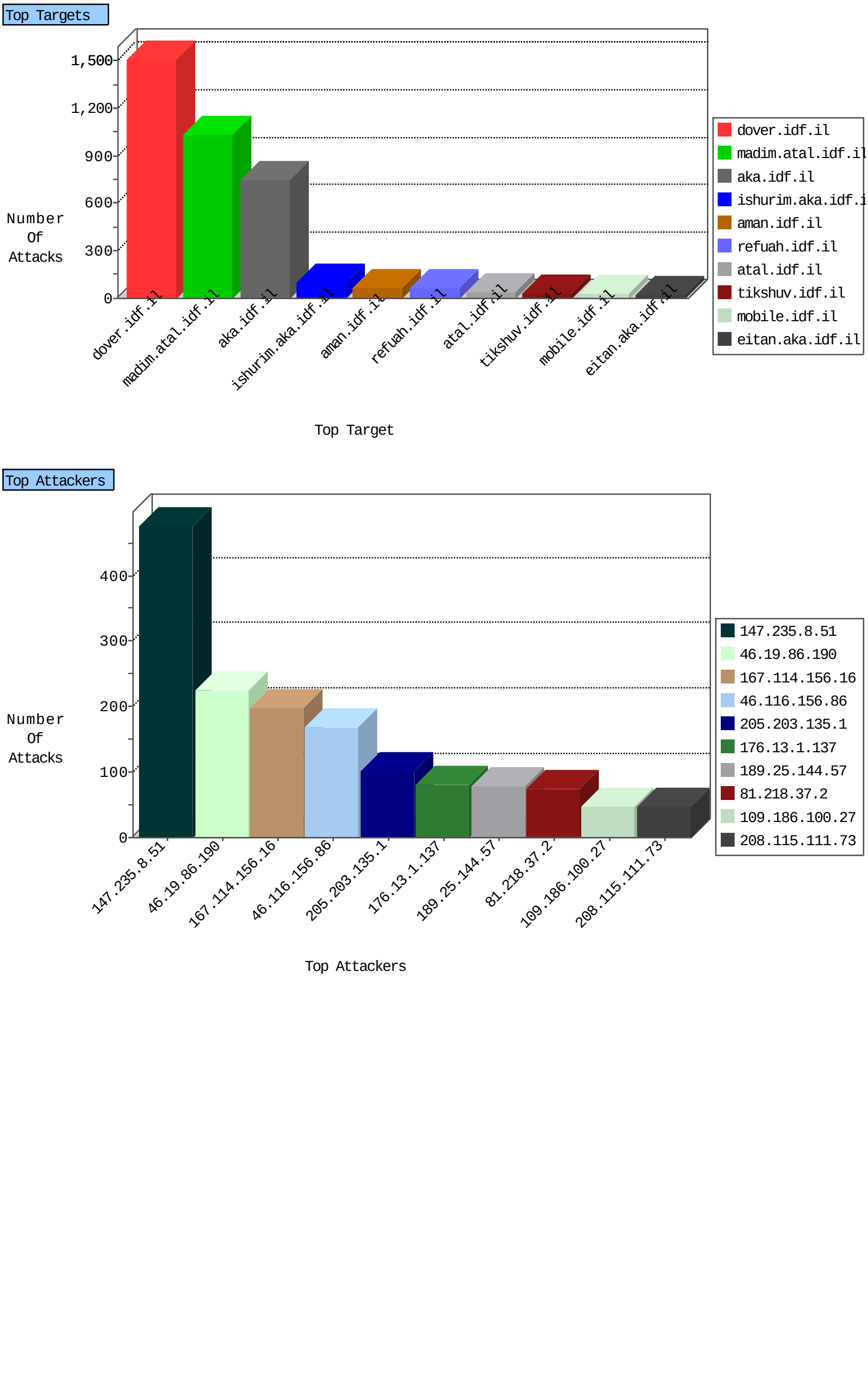
11-22-2015-17:04:07 to 11-22-2015-18:04:07

IDF Under Attack
Daily Report



11-22-2015-17:04:07 to 11-22-2015-18:04:07

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	12458
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4732
81.218.37.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	412
66.249.93.200	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	55
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	8
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	8
89.138.196.159	Israel	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	4
79.176.126.171	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
99.232.103.41	Canada	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3

11-22-2015-17:04:07 to 11-22-2015-18:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.54.18	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-22-2015-17:04:07 to 11-22-2015-18:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
95.35.185.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
168.235.64.163	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
62.219.149.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
169.54.233.119	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.3.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
42.118.40.87	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.162.171	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
2.54.154.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.163.140.142	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential SSH Scan	1
82.166.22.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.172.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.155.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.185.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.57	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
46.185.218.133	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.234.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.163.140.142	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.2.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.138.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.48.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-22-2015-17:04:07 to 11-22-2015-18:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
189.25.144.57	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
81.218.37.2	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	36
66.102.8.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
109.186.100.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
69.126.111.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
85.130.252.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.104.29		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
100.100.16.185		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
178.63.165.187	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.186.100.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	20
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
37.46.39.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	19
100.100.46.32		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
37.26.148.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
100.100.109.44		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
31.168.93.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.82.73		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
100.100.30.175		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.26.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
100.100.77.33		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
199.203.223.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
119.56.118.219	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
213.8.92.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
80.246.133.132	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.7.173		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
2.52.185.39	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.77.33		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.185.218.133	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
193.106.54.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.94.201		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.177.211.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
107.170.61.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
88.108.230.149	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
173.252.115.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.1.47.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

11-22-2015-17:04:07 to 11-22-2015-18:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 147.235.8.51	Block	114
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
46.116.156.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
176.13.1.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
46.116.156.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	66
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.13.0.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
77.125.164.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.218	Block	8
77.125.83.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.83.253	Block	6
79.179.139.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	5
46.116.233.194	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
109.66.119.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
46.116.233.194	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
176.12.140.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.141.26	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.141.26	Block	3
46.19.86.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.210	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.86.210	None	3
5.28.137.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.225.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
62.90.94.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
37.26.148.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.67.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
2.54.176.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.205.199	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
37.26.149.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.211.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.22.129.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	2
176.12.144.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	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
2.52.57.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
92.222.28.243	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.168.118.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.55.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.25.92.80	Germany	147.237.76.30	himush.idf.il	Unauthorized URL Access to /robots.txt	Block	1
5.29.149.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19771-he/idfgdover.aspx	Block	1
109.65.120.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.177.170.14	Poland	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/eitan/main/	Block	1
204.93.154.201	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

11-22-2015-17:04:07 to 11-22-2015-18:04:07