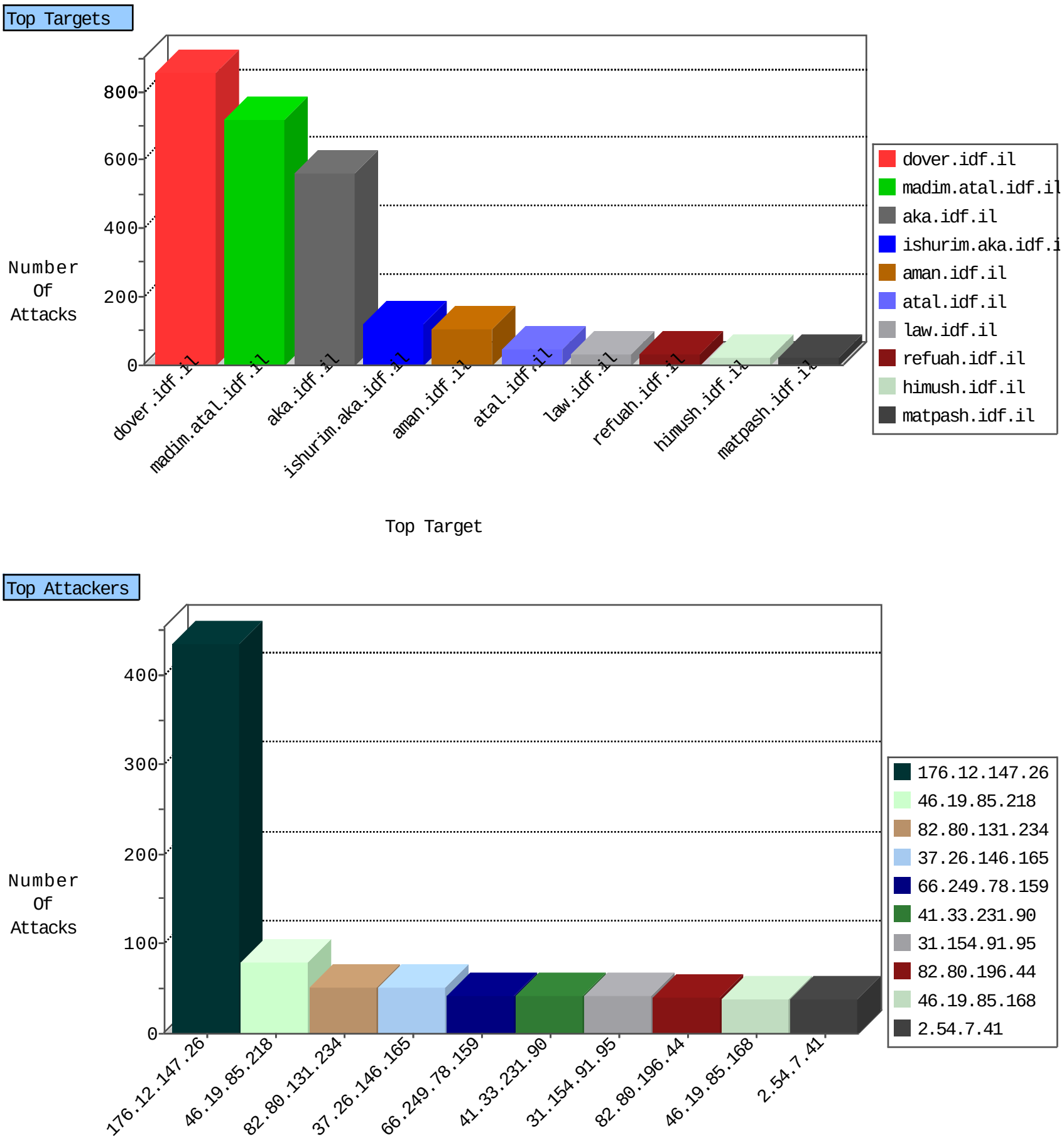
11-22-2015-11:04:00 to 11-22-2015-12:04:00

IDF Under Attack
Daily Report



11-22-2015-11:04:00 to 11-22-2015-12:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.201	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	11
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.67.29.136	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
31.210.176.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
79.176.170.37	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
66.249.78.190	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3
79.178.152.39	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.235.65.230	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.179.29.82	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
115.230.124.164	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
2.54.34.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
207.244.83.130	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
31.168.245.120	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
178.17.171.80	Moldova, Republic of	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
104.192.0.226	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
178.17.171.80	Moldova, Republic of	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
178.17.171.80	Moldova, Republic of	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
46.19.86.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.158.166	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
178.17.171.80	Moldova, Republic of	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

11-22-2015-11:04:00 to 11-22-2015-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.22.165	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	8
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
37.26.148.236	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
195.160.240.11	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-22-2015-11:04:00 to 11-22-2015-12:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
46.19.86.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.36.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.137.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.43.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.19	Ukraine	law-forum.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.185.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.0.102.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.52.181.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.9.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.114.17.100	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.169.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.212.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.231.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-22-2015-11:04:00 to 11-22-2015-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
31.154.91.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
46.19.85.218	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
109.64.192.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
197.0.248.133	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
100.100.82.73		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
168.63.137.102	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
176.13.12.50	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
100.100.22.12		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	18
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
212.235.103.203	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
176.13.12.50	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.232	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
100.100.102.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.154.92.23	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.116.215.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.178	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
100.100.118.41		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
94.230.86.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.228.176.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.176.7.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.219.161.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.36.1	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	8
2.54.174.1	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.227	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.34.250		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.200	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.96	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.147.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	294
176.12.147.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
176.12.147.26	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.12.147.26	Block	68
82.80.131.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
2.54.7.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
176.13.0.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
176.13.10.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
2.54.181.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
2.54.33.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
79.179.140.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
46.19.85.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.13.22.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
82.80.239.236	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	5
207.241.226.40	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 207.241.226.40	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
207.241.226.40	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	3
37.26.148.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.4.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.229.29.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.12.138.96	Israel	147.237.0.19	madim.atal.idf.i	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
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
2.54.37.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.140.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.222.212	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
176.13.14.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.80.239.236	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.239.236	Block	2
82.80.239.236	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
46.19.86.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.149.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.34.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
88.198.16.122	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 88.198.16.122	Block	1
212.76.123.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.11.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.164.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.164	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
46.121.75.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.36.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.25.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.168.28.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-22-2015-11:04:00 to 11-22-2015-12:04:00