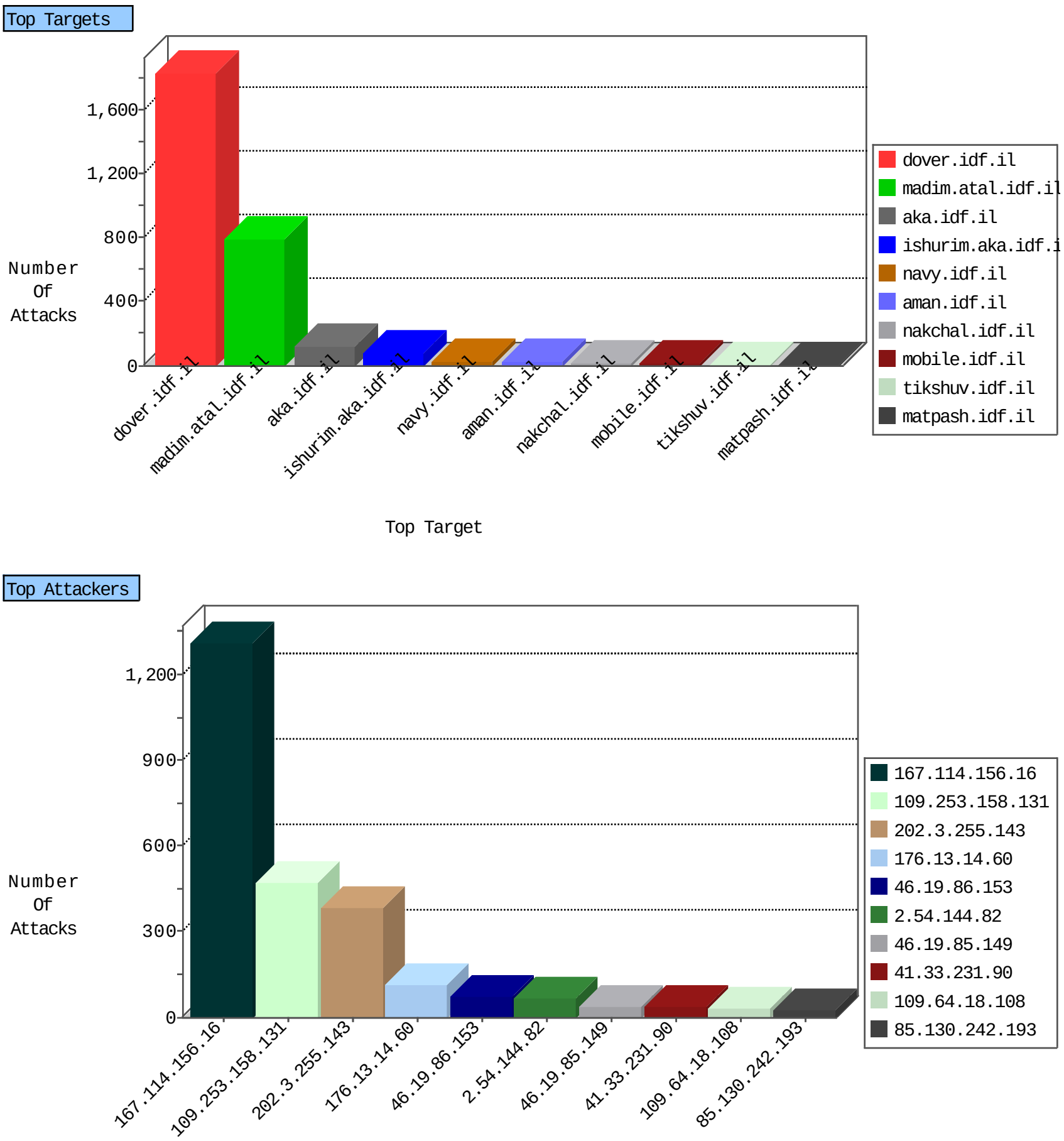
01-17-2016-07:04:09 to 01-17-2016-08:04:09

IDF Under Attack
Daily Report



01-17-2016-07:04:09 to 01-17-2016-08:04:09

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	3117
46.19.85.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
162.248.100.195	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

01-17-2016-07:04:09 to 01-17-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-17-2016-07:04:09 to 01-17-2016-08:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	340
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.130.5.234	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
158.255.2.12	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.170	India	maarachot.idf.il	ET SCAN NMAP -f -sS	1
80.246.130.160	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.234	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
182.72.109.162	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.170	India	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
85.17.249.176	147.237.77.216	Netherlands	dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
185.130.5.234	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 1024	1

01-17-2016-07:04:09 to 01-17-2016-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.153	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	72
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.26	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
197.248.120.246	Kenya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
172.58.24.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
85.130.242.193	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
85.130.242.193	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.142.188.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.126	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.242.193	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.171.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.112.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.140.107	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.8.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.166.140.117	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.143	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
2.54.13.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.115.252.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.203.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.126	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
62.219.118.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.43.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.52.43.104	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
81.218.193.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.115.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.8.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.43.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.158.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.164.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.54.94	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.234	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.76.34.103	Finland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.8	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.43.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.142.188.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.130.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.17.249.176	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
93.172.163.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
2.52.43.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.158.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	297
109.253.158.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
176.13.14.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.54.144.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
109.253.158.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	29
109.64.18.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.144.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
109.253.210.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
84.228.147.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.130.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.135.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.8.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.9.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.178.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.9.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.135.102.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.166.190.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
176.13.2.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.18.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.20.215	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.19.86.179	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/1133-22638-he/dover.aspx.	Block	1
87.69.34.139	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
5.196.72.199	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
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	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
117.203.79.166	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/kenessikum2010arbel.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.121.92.46	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/1133-22461-he/dover.aspx.	Block	1
87.69.37.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.147	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12535-he/dover.aspxÃ—Å¾Ã—ÂªÃ—â€™Ã—â„¢Ã—Â¡Ã—â„¢Ã—?	Block	1
2.52.183.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.243	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
69.58.178.57	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
93.172.163.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/patzar/klali/default.asp	None	1
109.253.159.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.0.16.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
87.69.110.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.18	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/home/pniot.aspx	Block	1
212.199.169.156	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	1