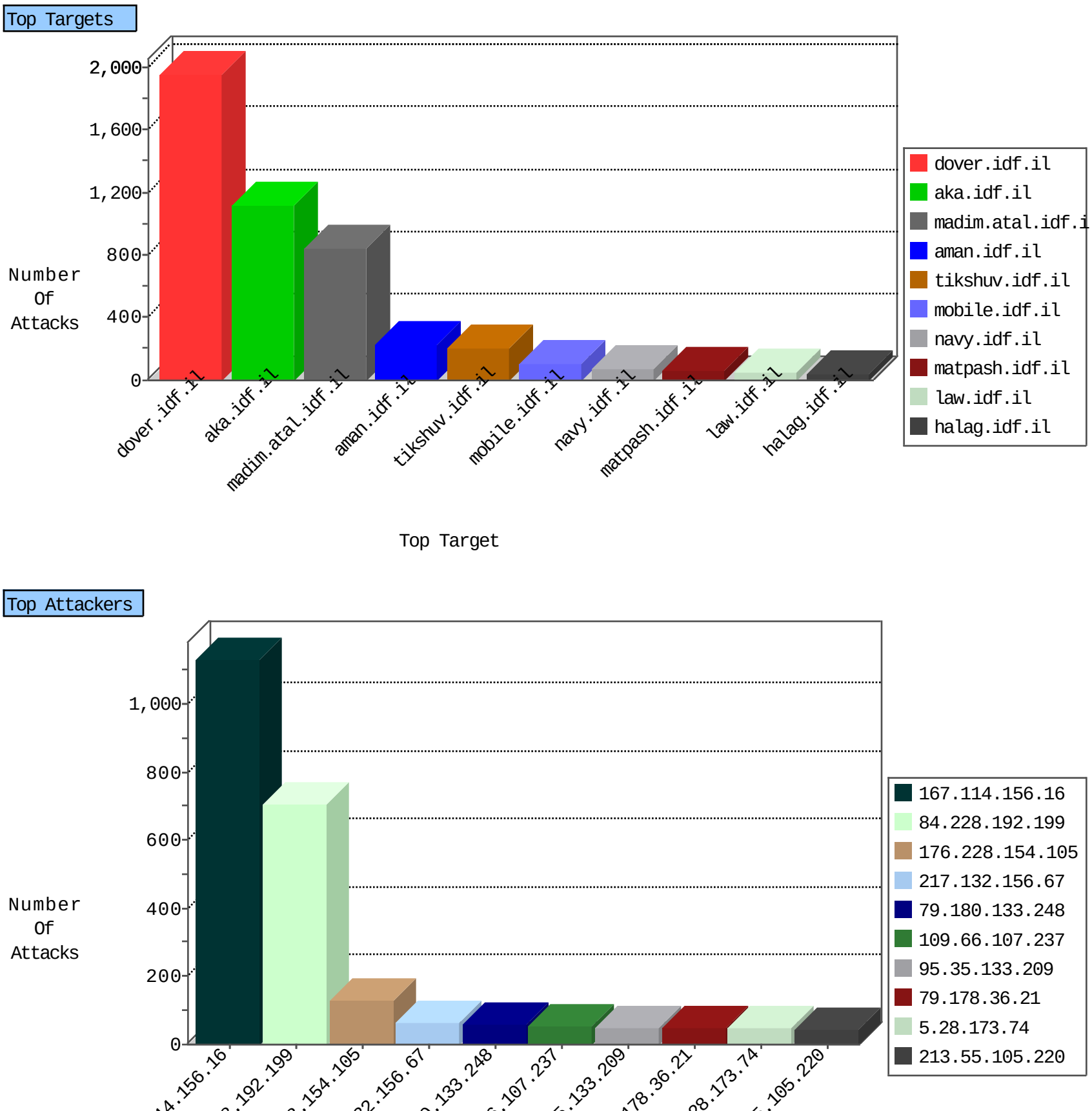
01-08-2016-14:04:04 to 01-08-2016-15:04:04

IDF Under Attack
Daily Report



01-08-2016-14:04:04 to 01-08-2016-15:04:04

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	3147
213.55.105.220	Ethiopia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
23.102.50.22	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
80.77.174.155	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.141	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.142	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
107.150.60.245	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
142.54.160.211	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
65.181.113.88	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.137	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

01-08-2016-14:04:04 to 01-08-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-08-2016-14:04:04 to 01-08-2016-15:04:04

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	4
87.68.254.73	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
109.64.210.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.247.190.52	147.237.77.243	Italy	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
90.148.77.34	147.237.8.27	Saudi Arabia	e.madim.atal.idf.i	ET SCAN NMAP -sS window 4096	1
80.82.69.146	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.12.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.161.132.231	147.237.77.178	Mexico	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.125.111.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
134.213.177.204	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
109.65.57.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.176.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.156.251.10	147.237.76.202	Germany	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.228.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.155.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.64.50.153	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.118.197.128	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
134.213.177.204	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.85.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.186.73.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-08-2016-14:04:04 to 01-08-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.133.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
176.228.154.105	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
84.228.192.199	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
176.13.10.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
213.55.105.220	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.87.84.217	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
50.118.197.128	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
5.28.173.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
5.28.173.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
109.253.214.127	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
213.8.204.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
141.0.15.92	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
80.246.136.249	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
87.68.66.98	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.228.154.105	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
213.8.204.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
109.253.142.193	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
66.87.84.217	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
37.26.147.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
37.26.147.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
37.26.149.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.116.190.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.182.21.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.52.15.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
2.52.19.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.116.190.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
95.35.133.209	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
185.3.147.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
50.118.197.128	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.135.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.158.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.42.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
2.54.42.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.158.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
79.178.36.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
37.142.68.3	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.178.36.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
2.52.19.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
80.246.137.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
79.182.120.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.120.93.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.182.120.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
45.35.64.142		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.120.93.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.192.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.192.199	Block	385
84.228.192.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 84.228.192.199	Block	174
84.228.192.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.228.154.105	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
109.66.107.237	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
84.110.209.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
95.35.133.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
79.176.218.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.52.130.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
79.180.133.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	7
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.123.29	Block	5
46.117.125.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
80.246.136.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
79.176.178.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
109.253.143.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.88.150.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.119.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
2.54.58.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
113.110.150.243	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Unknown HTTP Request Method ÂŽ in URL	Block	1
84.111.187.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/tmuna	Block	1
37.8.73.169	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
109.65.155.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 217.132.156.67	Block	1
2.52.18.222	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.86.70.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Illegal HTTP Version 4q4Ã?ÃœÃ˜Â¯[[#28]]KÃ¤OVVÂ¤6oÂ°Â»Ã¿ÃŠÂ‘GÃ©%Ã¨_[[#18]]Â²ÃŒÂ–rÂ•Â?Ã“Ã?[[#19]]G'g.ehÃ, b&ÂªÂ¸Â§[[#19]]h[[#31]]Â¼B[[#8]]Ã¬	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
176.13.18.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.2.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
217.132.154.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
149.78.223.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.31	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
109.186.6.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.156.67	Israel	147.237.72.156	aman.idf.il	NULL Character in Parameter Name }Q-F[[#28]][[#0]]{Â¸â€¹v×›â€“×–MÂŸÖµ>Tp[[#29]]'Â»ÂŸ×?fÖµ[[#29]]ÂŒl in ×˜+Ãžv×“eÖ»×”•×³Â¯â€œ^~×œÃ›{%×£Â²4ÂŠÂ?â‚ª5×˜pu[[#12]]×¤-_Â?(,â€Ž×œs5[[#5]]5×š	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
2.54.137.201	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.64.37.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 217.132.156.67	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
62.219.210.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1