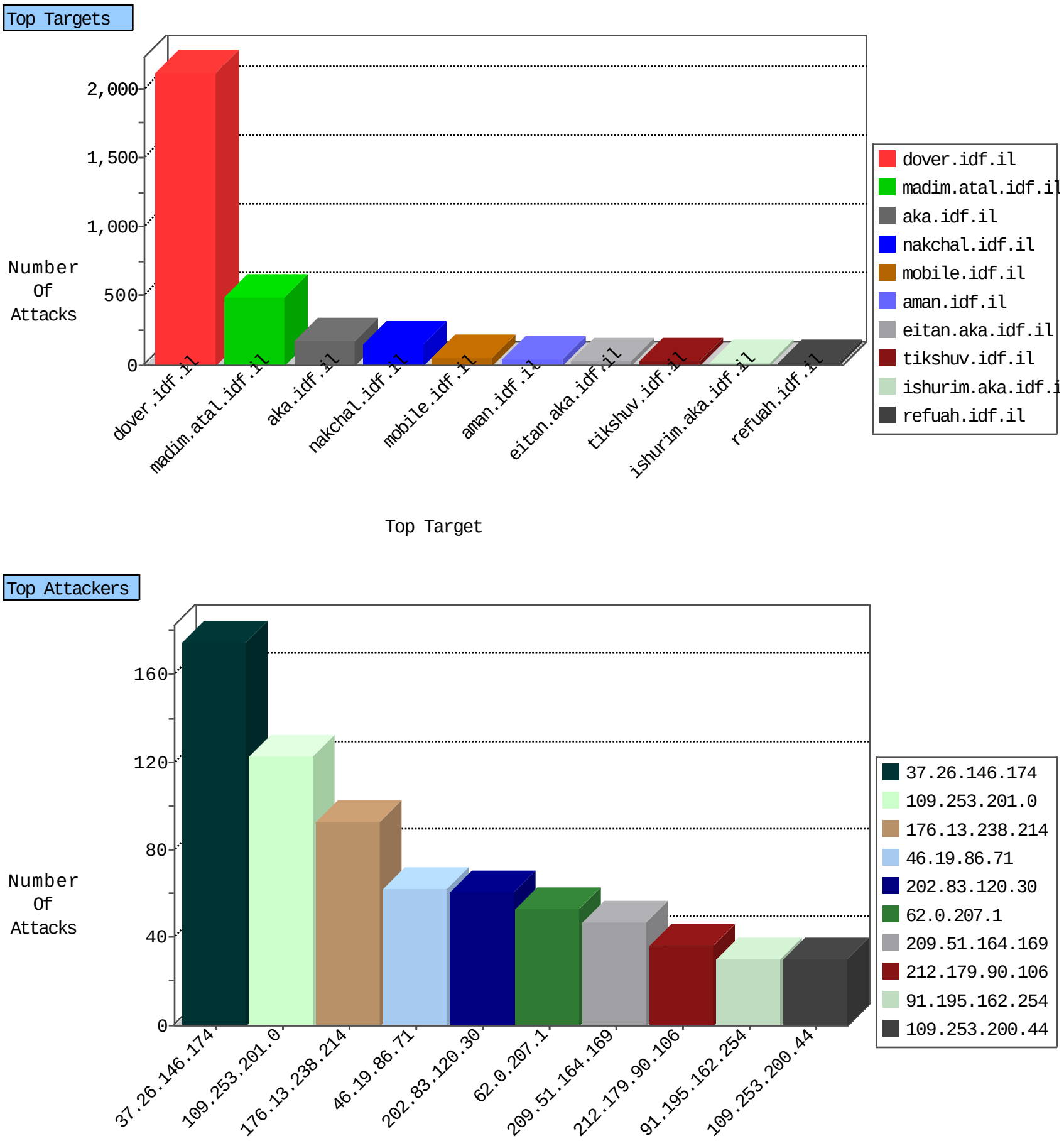
09-28-2016-15:04:02 to 09-28-2016-16:04:02

IDF Under Attack
Daily Report



09-28-2016-15:04:02 to 09-28-2016-16:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.182.47.169	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
217.65.35.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
132.72.78.122	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.154.45.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
109.253.133.210	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
213.8.128.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
63.141.250.156	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
172.1.1.123	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.53.29.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
198.204.247.221	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
173.208.198.11	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
192.187.118.21	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
198.204.255.74	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
173.208.207.133	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
192.187.118.21	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
173.208.213.195	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
192.187.118.66	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
173.208.213.197	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	1
69.30.193.251	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1

09-28-2016-15:04:02 to 09-28-2016-16:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
144.76.29.66	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-28-2016-15:04:02 to 09-28-2016-16:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.88.235.154	147.237.77.205	China	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
77.127.40.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.23.1.12	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
58.220.2.5	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
213.151.57.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.208.165.101	147.237.72.217	Russian Federation	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.255.108.192	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.77.131	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.21.248.87	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.74.121.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.21.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.39.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.220.2.5	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
217.23.1.12	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
58.218.200.137	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
199.203.223.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.60.86.73	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
185.24.76.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.183.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.255.108.192	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.77.131	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.220.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.29.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.195.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-28-2016-15:04:02 to 09-28-2016-16:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.207.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	53
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
192.118.78.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.53.147.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.13.231.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
91.195.162.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.183	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.246.138.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
81.218.144.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.31	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
212.143.27.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.253.208.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
209.51.164.169	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
192.118.78.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
209.51.164.169	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.53.180.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
5.102.253.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.15	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
209.51.164.169	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
213.8.128.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.228.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.133.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.162.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.5.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.212.29.185	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.118.27.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.14.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.124.34.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.31	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.210.216.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.232.18.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.166.204.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
192.116.131.98	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	8
176.13.245.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.13.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.162.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
109.253.201.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	123
176.13.238.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
46.19.86.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
109.253.129.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.16.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.166.118.192	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
84.108.219.89	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.142.6.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sacher	Block	2
80.255.2.224	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
109.65.133.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.133.250	Block	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
77.139.34.234	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String [[#22]]<&}[[˙{ד¯#4כ]]ˆ†r«″?ü* "0¦»>ûר",:ˆI[[#21]]¾[[#25]]>'µÞÙ¬G[[ע#7]]03#[[¼]]0#[[mx·₪O]]צˆfÛf±•¦Ú [[#19]]ֶ_^e:ב	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	Block	1
141.226.161.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
85.250.104.125	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	NULL Character in Parameter Name [[#22]]<&}[[˙{ד¯#4כ]]ˆ†r«″?ü* "0¦»>ûר",:ˆ I[[#21]]¾[[#25]]>'µÞÙ¬G[[ע#7]]03#[[¼]]0#[[mx·₪O]]צe^_ֶ]]91#[[ˆfÛf±•¦Úב:	Block	1
37.26.147.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
204.79.180.223	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.65.133.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
66.249.69.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8785-he/refuah.aspx	Block	1
80.246.139.153	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
213.8.118.201	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
66.249.76.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
89.138.105.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	NULL Character in Query String [[#22]]<&}[[˙{ד¯#4כ]]ˆ†r«″?ü* "0¦»>ûר",:ˆ I[[#21]]¾[[#25]]>'µÞÙ¬G[[ע#7]]03#[[¼]]0#[[mx·₪O]]צe^_ֶ]]91#[[ˆfÛf±•¦Úב:	Block	1
212.25.107.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
77.138.128.54	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
109.67.4.204	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/https:/madim.atal.idf.il/	Block	1
66.249.69.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8925-he/refuah.aspx	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	Illegal URL Path Encoding ®ֶ[[#30]],•חךשפי x|~»•%	Block	1
2.53.23.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.11.208	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
74.82.4.67	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
89.138.246.113	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 89.138.246.113 (Open Mode)	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
77.138.128.54	France	147.237.72.166	aka.idf.il	Unknown HTTP Request Method "’ÍSÓÙ[[#21]]¤¦f[[#2]][[#12]]¢E*§àõ±¦kfZœ?º[[#1]]6’ç@RþdÙV8•#èT¥[[#25]] ‘a‰åR‡Þ8pX‘MI+–±U[[#25]]A°ëçÕ–Ž[[#20]]À•kêÎCª in URL ®ֶ[[#30]],•חךשפי %•»~|xר	Block	1