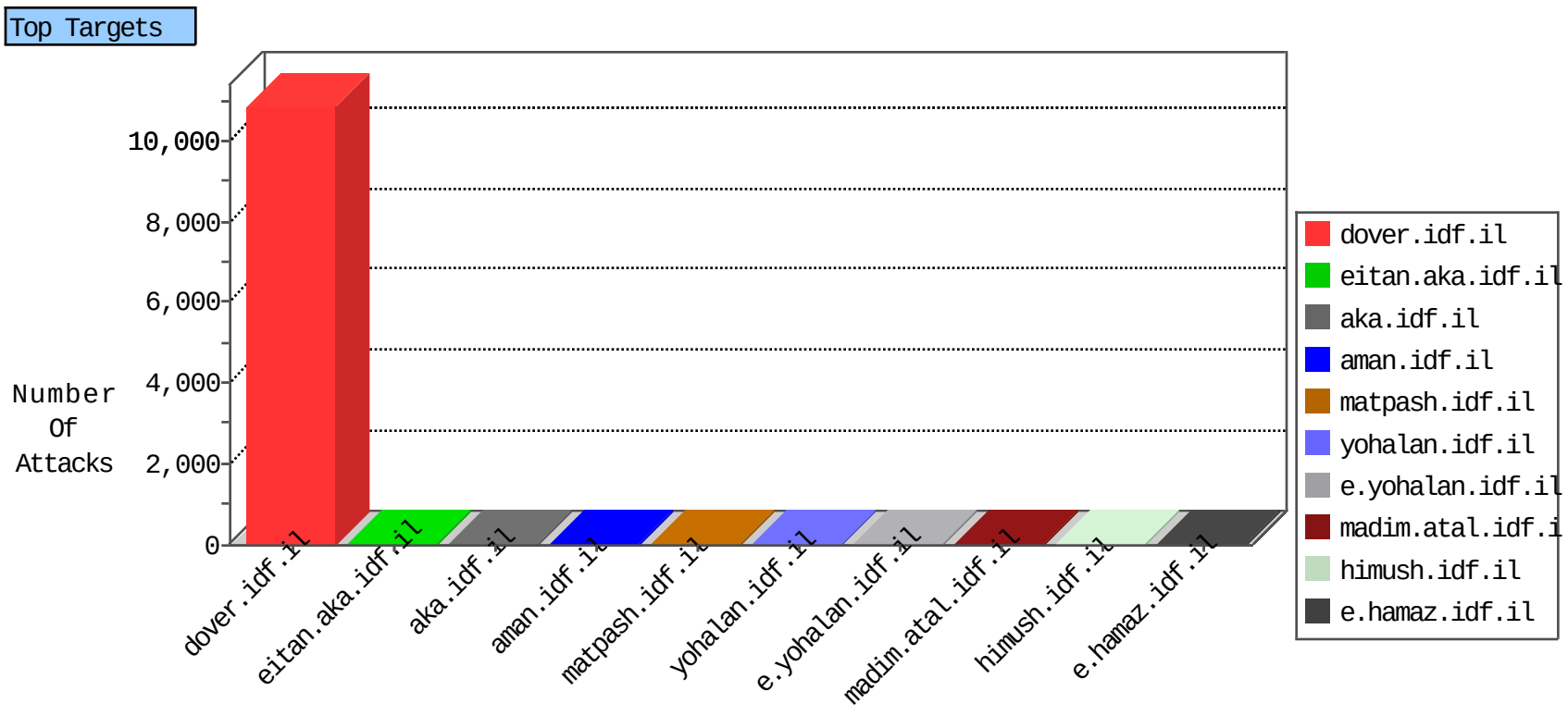
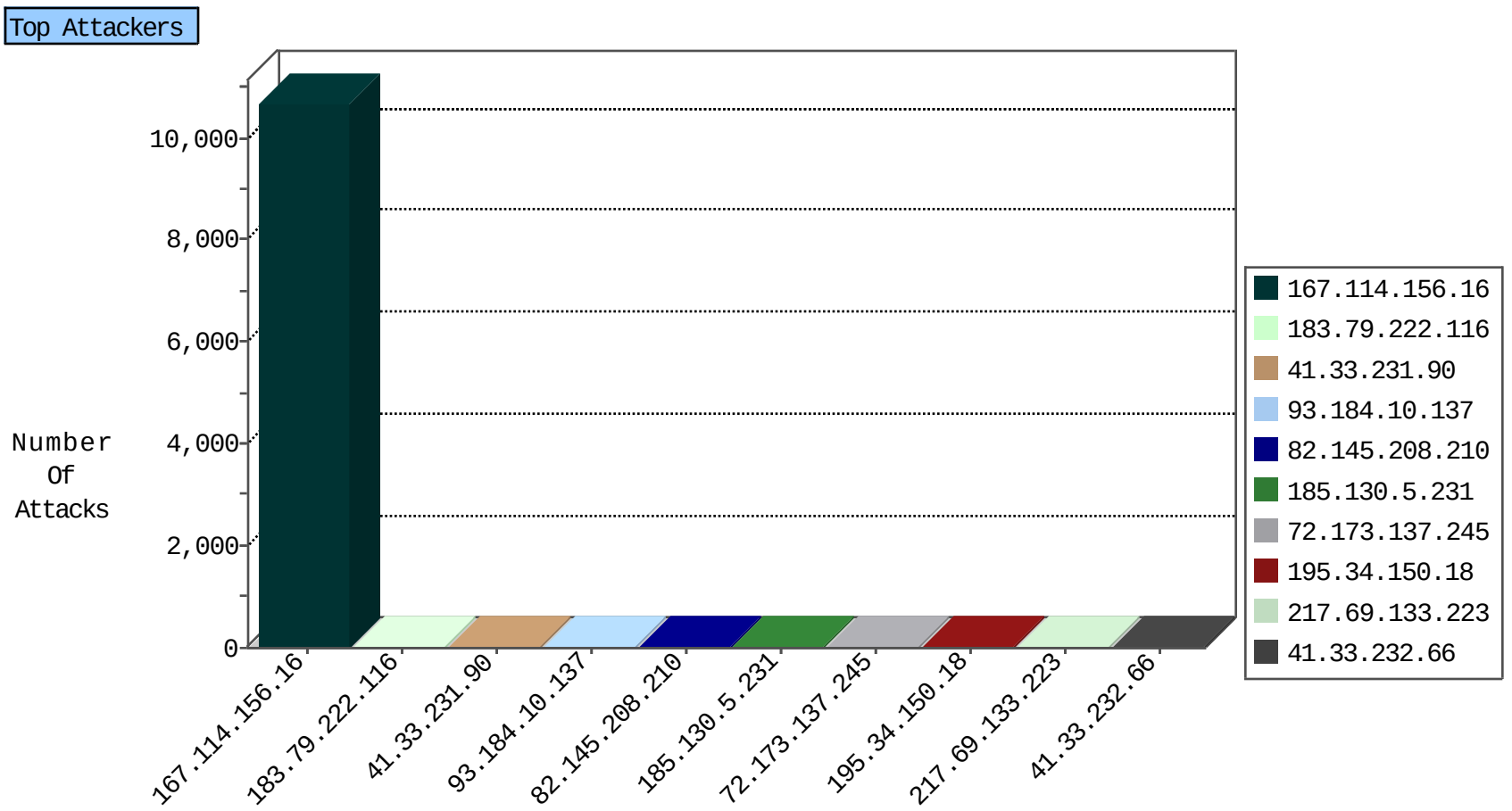
01-15-2016-03:04:04 to 01-15-2016-04:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-15-2016-03:04:04 to 01-15-2016-04:04:04

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	1600
93.184.10.137	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	3
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
188.138.17.205	France	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
61.182.170.38	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
116.84.114.56	Korea, Republic of	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

01-15-2016-03:04:04 to 01-15-2016-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-15-2016-03:04:04 to 01-15-2016-04:04:04

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	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
65.60.36.203	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
109.251.56.171	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.251.56.171	147.237.0.15	Ukraine	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
78.193.2.8	147.237.76.198	France	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
65.60.36.203	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
65.60.36.203	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
14.144.227.247	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.251.56.171	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.5.89.149	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
65.60.36.203	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

01-15-2016-03:04:04 to 01-15-2016-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9134
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1050
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop		drop	408
82.145.208.210	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
72.173.137.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
93.184.10.137	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
93.184.10.137	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.66.64.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
12.155.228.3	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.57.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
173.252.112.108	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
68.198.183.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
91.200.12.7	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
68.198.183.99	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
136.243.48.84	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.147.176	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
141.212.122.86	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
46.117.136.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.115	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.75.212.122	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
93.115.95.205	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
185.130.5.231		147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
72.252.202.42	Jamaica	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
149.78.53.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.87	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.17.99.183	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.231		147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
87.68.69.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
173.252.112.108	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.166.170.6	Lithuania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.122	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
93.115.95.207	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
185.130.5.231		147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.79.222.116	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.222.116	Block	14
183.79.222.116	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Illegal HTTP Version from 183.79.222.116	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	3
109.253.205.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.181.56.11	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type from 79.181.56.11	Block	2
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
183.79.222.116	Japan	147.237.76.200	eitan.aka.idf.il	Illegal HTTP Version ×˜×§×¥' HTTP/1.0	Block	1
85.64.151.138	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
72.252.202.42	Jamaica	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
40.77.167.43	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
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
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.181.56.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gen_204	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/Â	Block	1
85.64.151.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/login.aspx/login	Block	1
72.252.202.42	Jamaica	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
40.77.167.59	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
172.58.152.238	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
83.130.108.144	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	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
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.114	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.57.90.159	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl12$ctl01$ctl03$radQuestion in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
85.64.151.138	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.64.151.138	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
185.101.107.189		147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	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
79.181.56.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.56.11	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.69.133.221 (sigalgs DoS Attack)	None	1
183.79.222.116	Japan	147.237.76.200	eitan.aka.idf.il	Abnormally Long Request request version	Block	1
85.64.151.138	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 85.64.151.138 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1