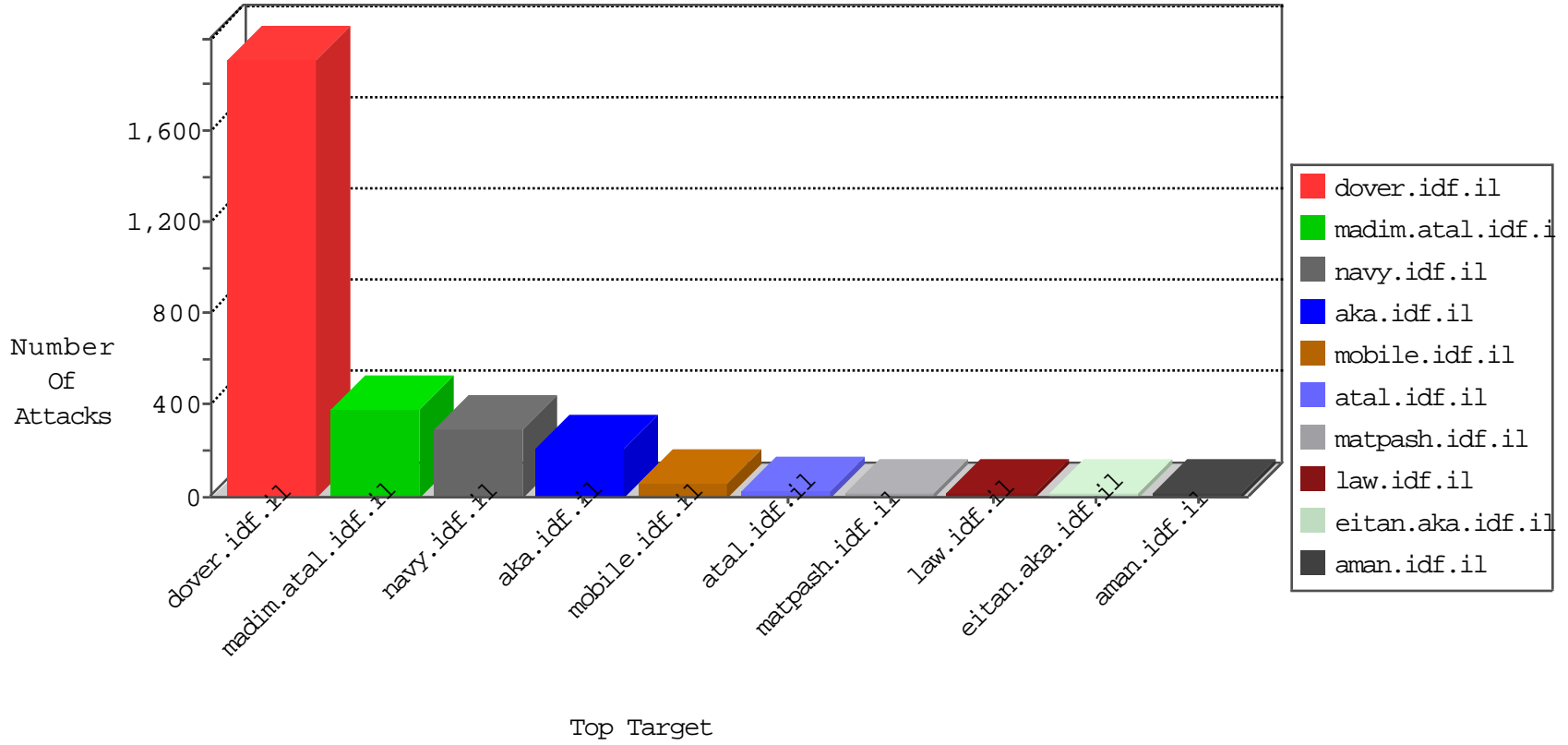


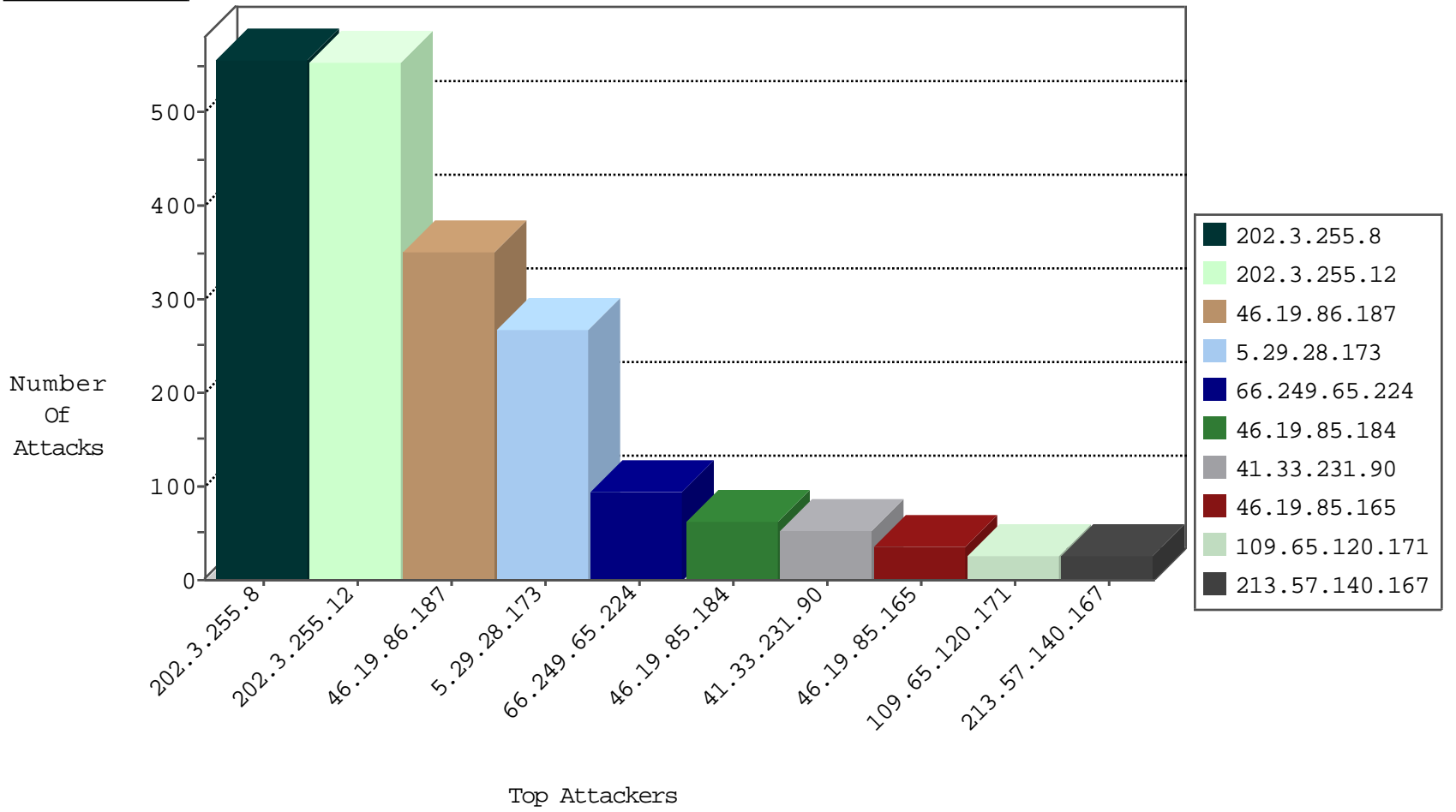
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3097
192.116.177.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
176.13.13.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
46.117.36.202	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
79.177.159.135	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
79.177.159.135	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
109.65.139.167	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.183.98.119	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.65.26.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.179.107.151	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
104.254.56.115		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
2.54.43.160	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	520
202.3.255.12	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	516
46.19.85.184	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	50
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	5
81.228.140.28	147.237.77.212	Sweden	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
220.245.240.26	147.237.77.121	Australia	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.148	United States	ggcenter.aka.idf.il	ET DROP Dshield Block Listed Source	1
176.12.136.112	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
110.77.212.150	147.237.77.234	Thailand	halag.idf.il	ET SCAN NMAP -sS window 1024	1
220.245.240.26	147.237.77.121	Australia	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
220.245.240.26	147.237.77.121	Australia	e.navy.idf.il	ET SCAN NMAP -f -sS	1
119.183.190.223	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.85.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
213.57.140.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
107.167.105.163	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
157.166.167.129	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.27.95.52	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.39.172.135	Kuwait	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
100.100.54.64		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.65.120.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
77.127.225.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.65.120.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.228.101.213	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.94.8	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
149.78.44.0	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
149.78.83.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
188.161.1.69	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
199.16.156.124	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	9
46.19.85.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.181.167.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.179.119.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.12.136.112	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
188.247.78.17	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.29.89.199	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.133.242	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.229.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.130.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.28.173	Israel	147.237.76.86	navy.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.28.173	Block	268
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	238
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
46.19.85.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
154.70.64.42	Ghana	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	3
83.130.106.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.30.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.206.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.167.153	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
176.12.141.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.28.135.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.12.143.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.207	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
185.3.146.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.139.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.152.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.154.94.8	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
79.180.31.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
54.183.192.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
207.46.13.189	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
82.81.27.14	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
5.29.28.173	Israel	147.237.76.86	navy.idf.il	Too Many 404: Response Code per Session	Block	1
109.66.123.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.229.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.71.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
82.81.27.14	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
79.180.224.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
37.26.147.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	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
84.94.204.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
64.110.133.37		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=xlc15.wvdzklxd.rqhtcalei4-	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
82.81.27.14	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Â¶[[#17]]Â~rÃ,Ã³Ã~Ã"7f\$Ãž crÃf!Ã"5Ã...>6Ã>Ãœ[[#19]]Ã<[[#0]]	Block	1
46.19.85.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.174.36	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
85.250.206.225	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.86.187	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	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
82.81.27.14	Israel	147.237.72.166	aka.idf.il	NULL Character in Method Â¶[[#17]]Â~rÃ,Ã³Ã~Ã"7f\$Ãž crÃf!Ã"5Ã...>6Ã>Ãœ[[#19]]Ã<[[#0]]	Block	1
79.181.167.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/login	Block	1
173.252.75.115	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1