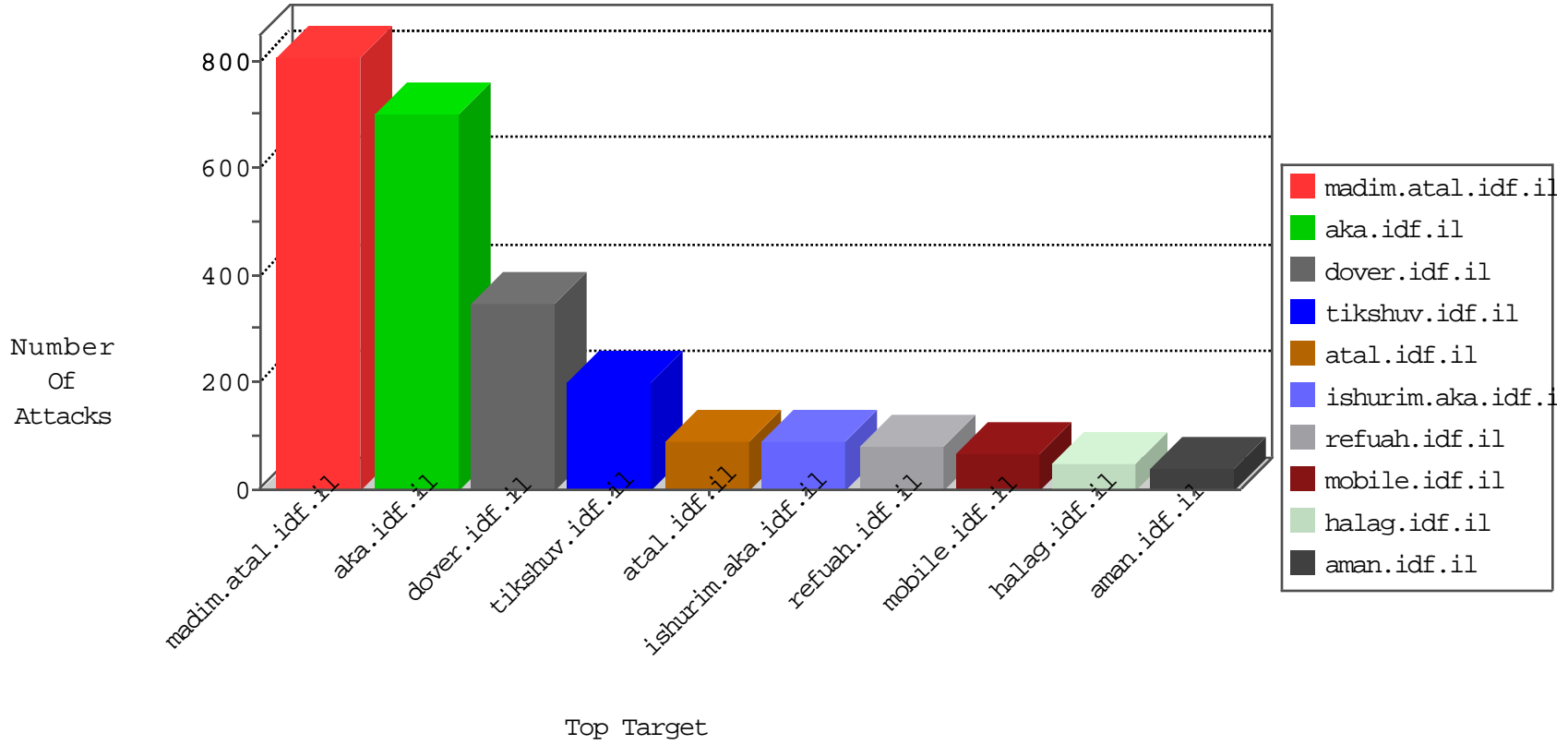


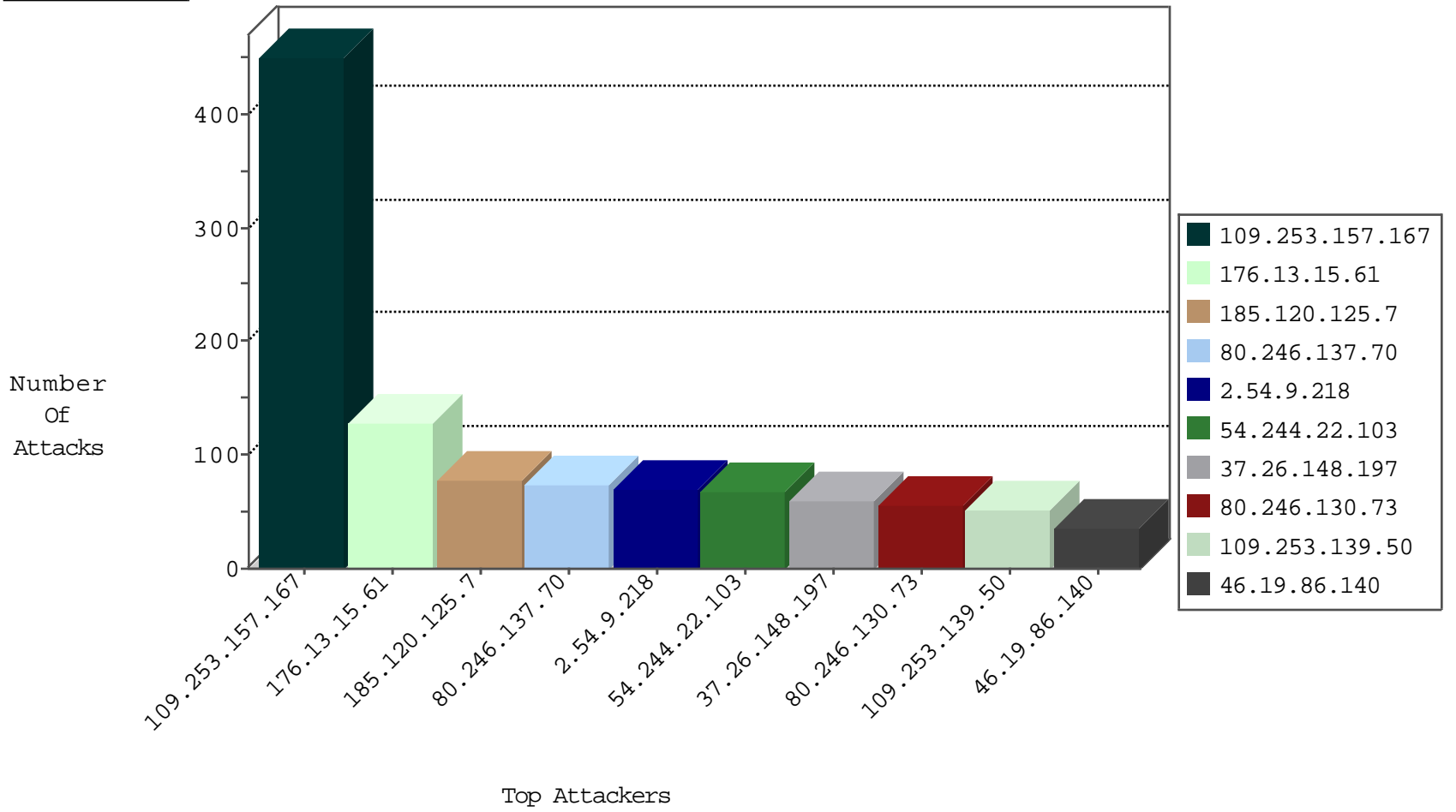
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
82.145.216.207	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
191.232.136.77	United States	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	1
94.76.3.122	Bahrain	147.237.72.167	ishurim.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
185.130.5.224		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

02-01-2016-13:04:03 to 02-01-2016-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.32.210.122	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.238	147.237.76.42	Israel	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	19
2.54.174.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
130.211.93.253	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
84.117.113.152	147.237.77.227	Romania	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.81.212	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.120.163.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.13.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.108.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.1.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.76.3.122	147.237.72.167	Bahrain	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.240.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.128.48.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.116.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
202.169.44.23	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	68
80.246.130.73	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
37.26.148.197	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	53
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
84.95.201.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
46.19.86.50	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
62.0.200.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
2.54.9.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
79.176.161.107	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
2.54.39.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
210.227.37.5	Japan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
176.13.22.215	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.52.164.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.9.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
213.8.204.53	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.132	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
2.54.9.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
81.218.251.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.186.111	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.96.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.9.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
79.178.96.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
212.113.88.24	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
77.125.151.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.54.9.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.54.250	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
77.125.151.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
109.253.198.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
109.253.198.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
188.120.148.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.65.224.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.201.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.29.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.115.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.238	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
109.253.194.22	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.147.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.168.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.136.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.13.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	306
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.157.167	Block	142
176.13.15.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
80.246.137.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
109.253.139.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
5.29.202.145	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.202.145	Block	33
37.26.149.166	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
2.54.43.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
79.176.240.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
80.246.137.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
5.29.236.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
185.32.179.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.54.187.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	7
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.146.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.15.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.16.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.59.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.190.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.209.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.221.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.144.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
79.178.56.97	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
109.253.133.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.210.187.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
80.246.136.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.171.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.63.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.142.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.9.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct135 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/datepicker.css	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
52.16.137.212	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on /	Block	1
194.187.168.237	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/home.png	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
2.54.172.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/960.css	Block	1
212.199.76.35	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 212.199.76.35 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.253.143.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.145.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.139.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	NULL Character in Method	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
52.27.95.112	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 52.27.95.112	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1