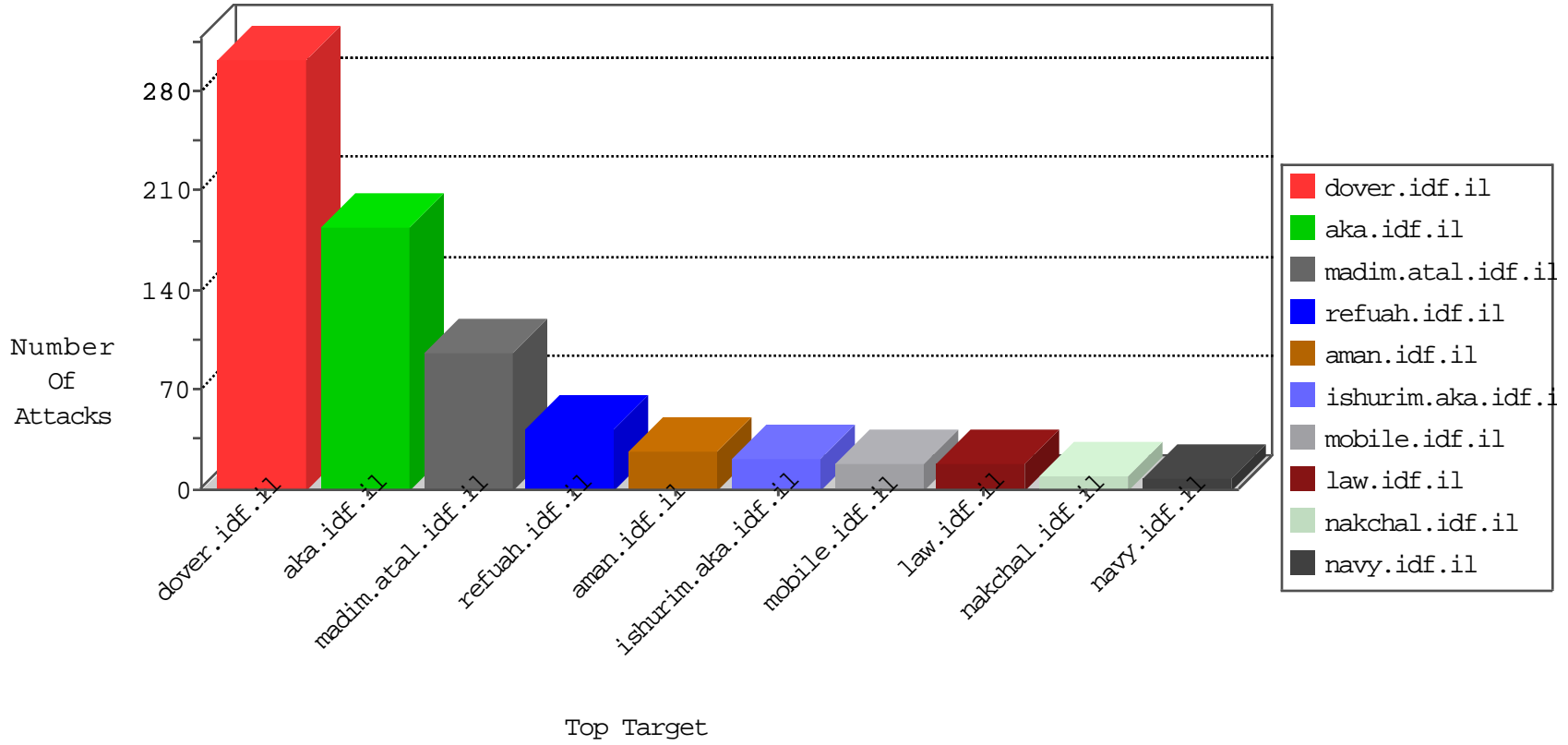


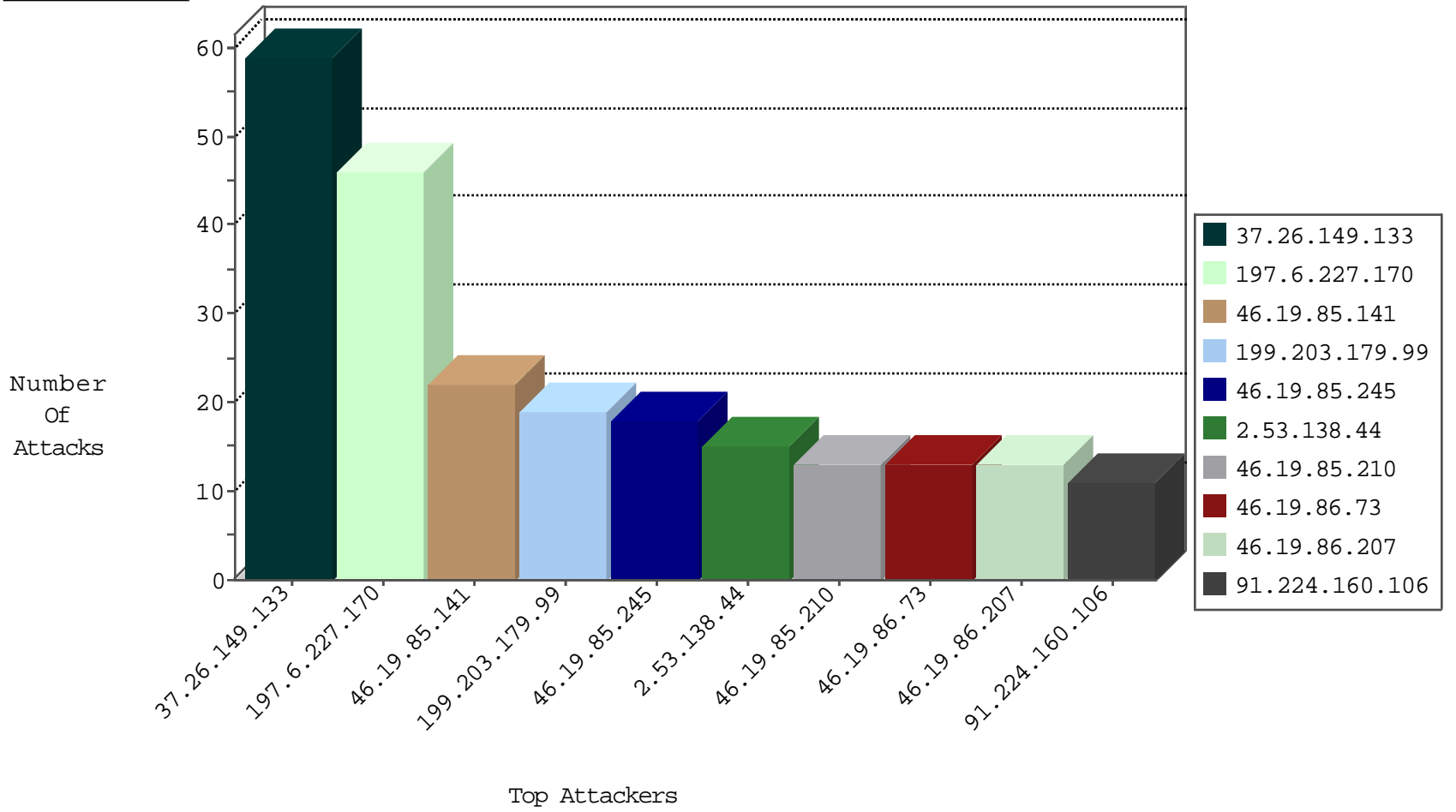
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
2.53.34.61	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
185.73.222.9	Netherlands	147.237.8.50	e.tikshuv.idf.il	L4 Source or Dest Port Zero	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
91.224.160.106	Netherlands	147.237.77.212	e.dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
73.14.6.116	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
94.102.49.190	Netherlands	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
73.14.6.116	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
85.65.3.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.23.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.157.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.219.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.169.39.109	147.237.77.216	Saudi Arabia	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.0.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
197.6.227.170	147.237.77.216	Tunisia	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.24.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.56.190.151	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.90.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.92	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.152	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.6.227.170	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	36
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
2.53.138.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
31.154.2.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
213.8.204.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
197.6.227.170	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.203.179.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
199.203.179.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.230.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
89.237.110.149	France	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.141	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
83.130.74.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.199.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.160.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.160.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.41.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.178.101.40	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.191	Israel	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.26.149.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.138.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.60.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.138.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.130.175	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.53.132.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.224.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.126.26.94	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.235.215	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
212.143.80.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
109.253.194.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
213.8.115.122	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.182.125.119	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.23	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.226.232.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
77.127.39.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.86.207	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.207	Block	9
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.222.204	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	5
212.235.13.100	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
212.235.13.100	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/4/	Block	3
37.26.146.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.196.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
80.246.136.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.86.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/tags/tags.aspx	Block	2
77.139.69.32	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.69.32	Block	2
37.26.149.138	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.179.28.34	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	2
77.139.69.32	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
2.53.16.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.41.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.168.11.194	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
2.53.5.27	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.23.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.57.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.139.224	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
217.194.193.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.49.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.172.150	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-23238-he/dover	Block	1
109.253.230.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.193.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.9.101	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.94.155	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sachar/	Block	1
199.203.122.49	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
31.44.128.241	Israel	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.166.181.20	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
185.32.179.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.97	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
176.13.7.27	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.155.44	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.138.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.210.22	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
2.53.30.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.21.194	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
185.120.124.24	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
31.210.188.2	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1