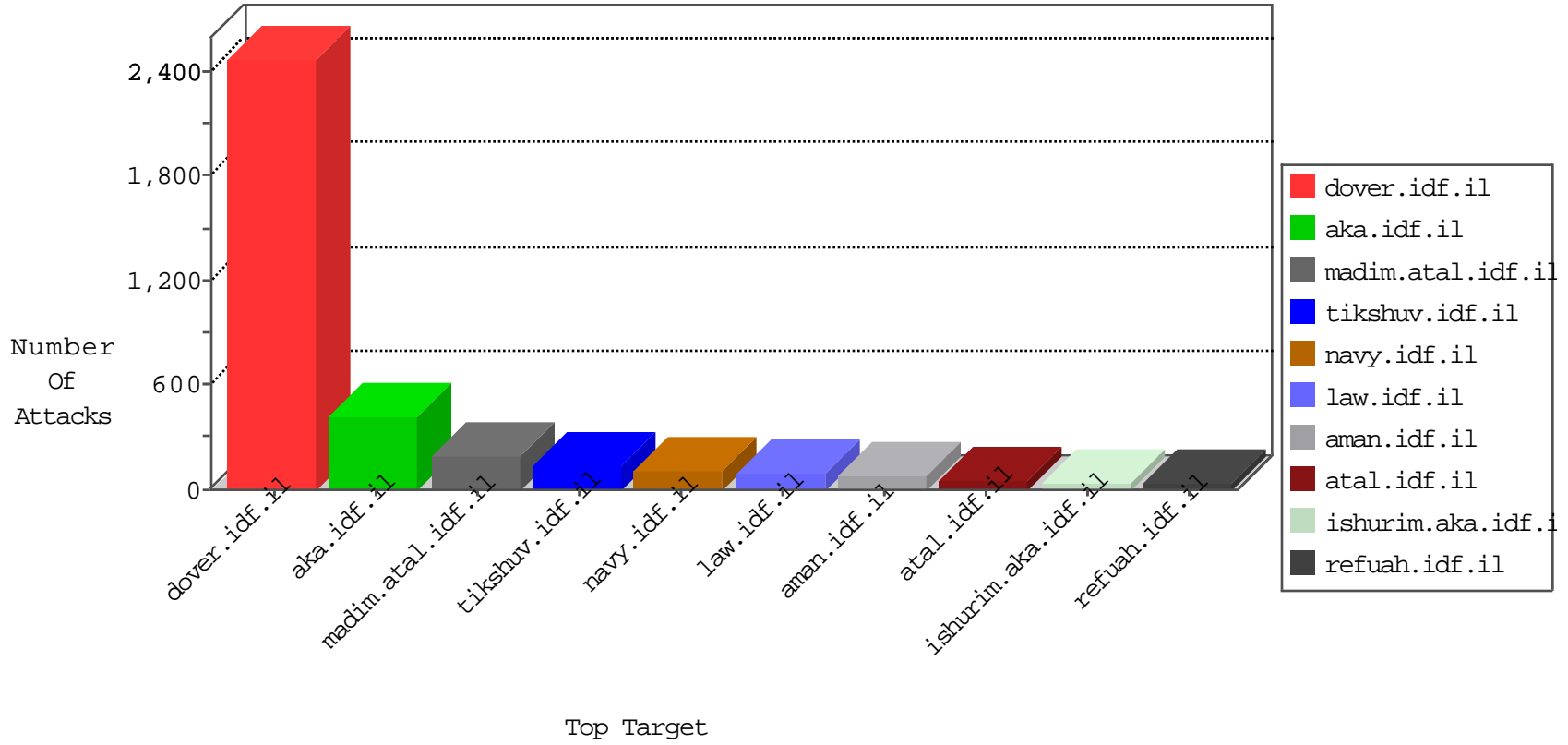


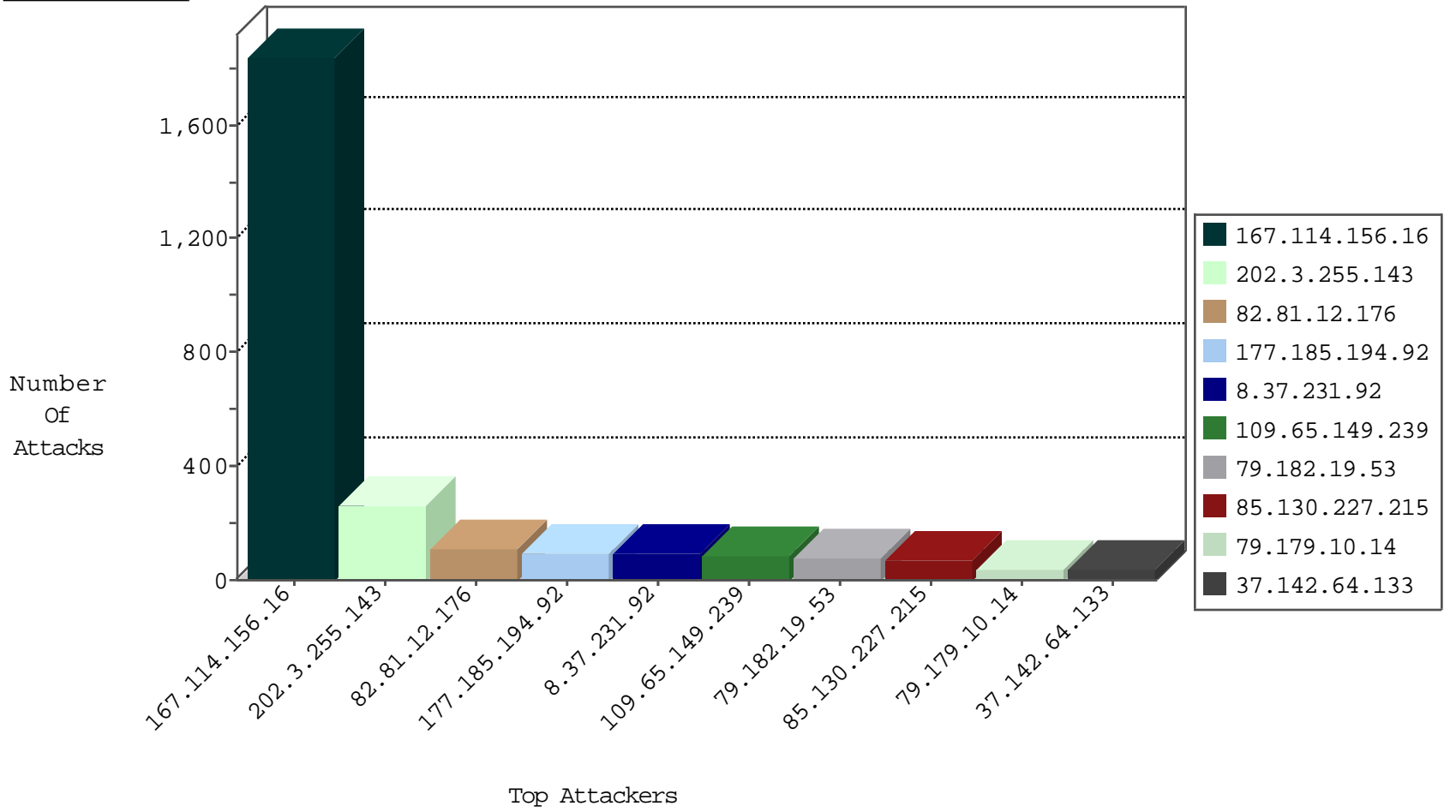
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3231
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
80.43.252.98	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
8.37.231.92	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
151.80.109.172	Italy	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
198.27.124.14	Canada	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.212	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1
199.30.16.178	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.90.147.145	Israel	147.237.0.34	tikshuv.idf.i	C212: HTTP: prefix 1.01 in the URL	Block	8
109.67.52.220	Israel	147.237.0.34	tikshuv.idf.i	C212: HTTP: prefix 1.01 in the URL	Block	6
79.181.235.48	Israel	147.237.0.34	tikshuv.idf.i	C212: HTTP: prefix 1.01 in the URL	Block	6
79.182.216.163	Israel	147.237.0.34	tikshuv.idf.i	C212: HTTP: prefix 1.01 in the URL	Block	5
37.142.64.10	Israel	147.237.0.34	tikshuv.idf.i	C212: HTTP: prefix 1.01 in the URL	Block	2
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
216.185.43.135	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
162.248.143.161	Canada	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
176.13.13.214	Israel	147.237.0.34	tikshuv.idf.i	C212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
177.185.194.92	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	224
177.185.194.92	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	93
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
216.185.43.135	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
202.194.97.136	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
202.194.97.136	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
176.117.26.115	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.65.222.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.185.20.218	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.53.196	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
202.194.97.136	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.109.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.92	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	90
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.182.20.112	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
87.69.165.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
85.130.227.215	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
85.130.227.215	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
85.130.227.215	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	21
105.200.74.148	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
2.88.39.140	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.99	Israel	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	14
37.142.64.133	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
105.200.74.148	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.88.158.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
77.127.178.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
141.0.15.247	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
89.138.177.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
37.26.148.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.177.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
197.162.112.109	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.120.161.206	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	9
66.249.93.184	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.93.182	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.34.165.207	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
94.159.149.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.140.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.184.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.28.174.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.212	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.51.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.3.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.227.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.230.25.148	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.111.126.10	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
149.78.237.89	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
109.66.184.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.250.124.204	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.229.152.31	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.253.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.8.204.68	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	5
5.102.253.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.161.206	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
141.0.12.15	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.253.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.43.252.98	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.240	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.144.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.155	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.149.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
79.182.19.53	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	75
79.179.10.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
37.142.64.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.54.169.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.140.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.65.149.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
37.26.149.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.144.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
198.20.241.135	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
213.151.63.18	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
5.9.60.113	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
109.253.139.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.120.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.143.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Å	Block	2
89.138.177.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.195.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.68.55.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.210.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
162.248.143.161	Canada	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
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	2
95.86.78.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Å	Block	2
91.189.176.230	Norway	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
81.218.125.104	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
5.9.60.113	Germany	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
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	2
2.54.152.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
88.198.4.37	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
185.56.144.88	Netherlands	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
109.253.204.111	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
212.179.217.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.5.188	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
162.247.72.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.120.79.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.222.233	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
94.136.40.100	United Kingdom	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
192.169.202.14	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
79.180.98.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.158.68	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.93.184	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
113.11.250.192	Singapore	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
89.188.72.212	Denmark	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
186.202.153.93	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
50.62.208.71	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
207.46.13.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ahukewj-ienfrp_jahvdtbgkhd8_cw0qfggnmaa&sig2=fknsk6ifabc6y15_vmmf7g&usg=afqjcnhcdsh5ryhkeugapxlds97fowjwnw	Block	1
173.254.103.187	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1