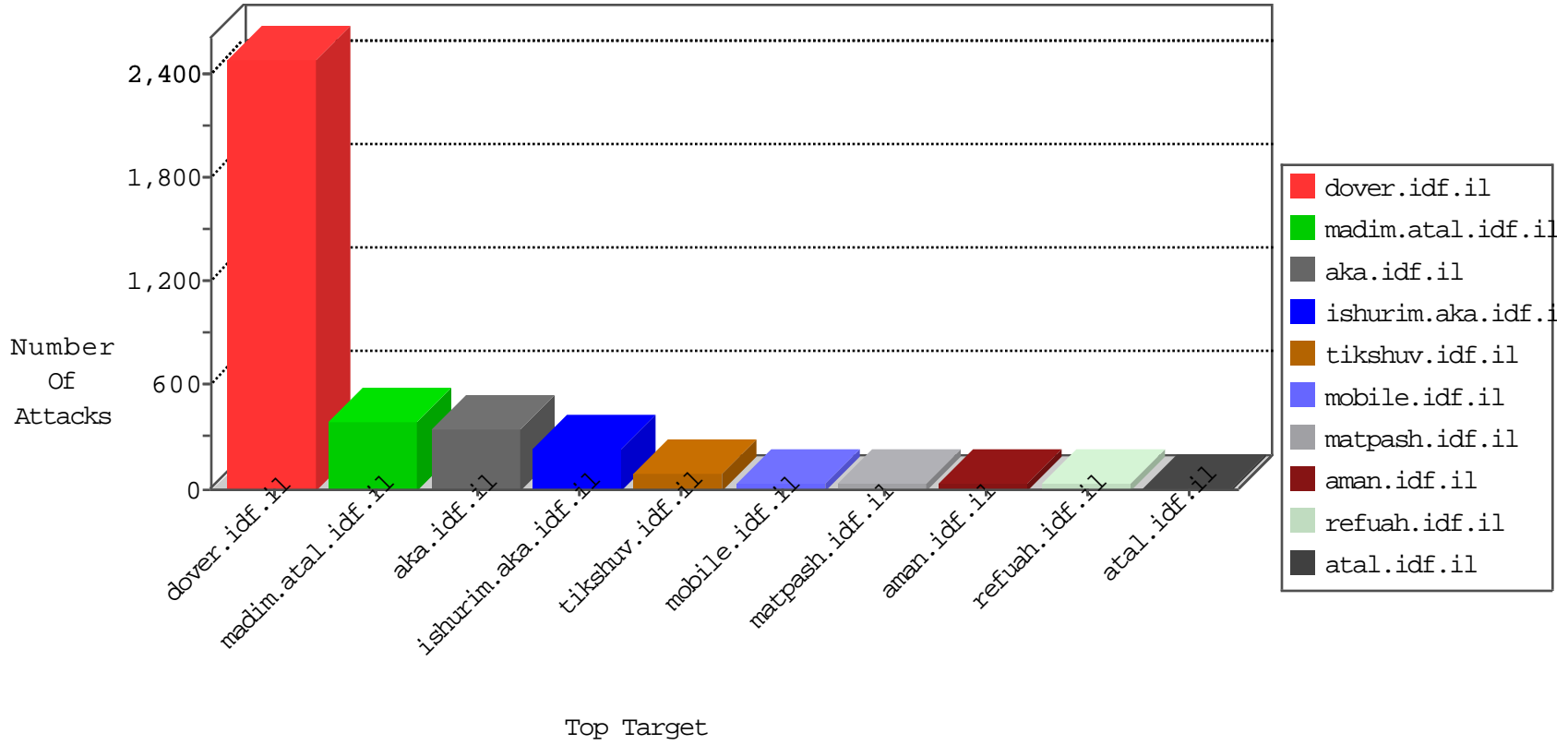


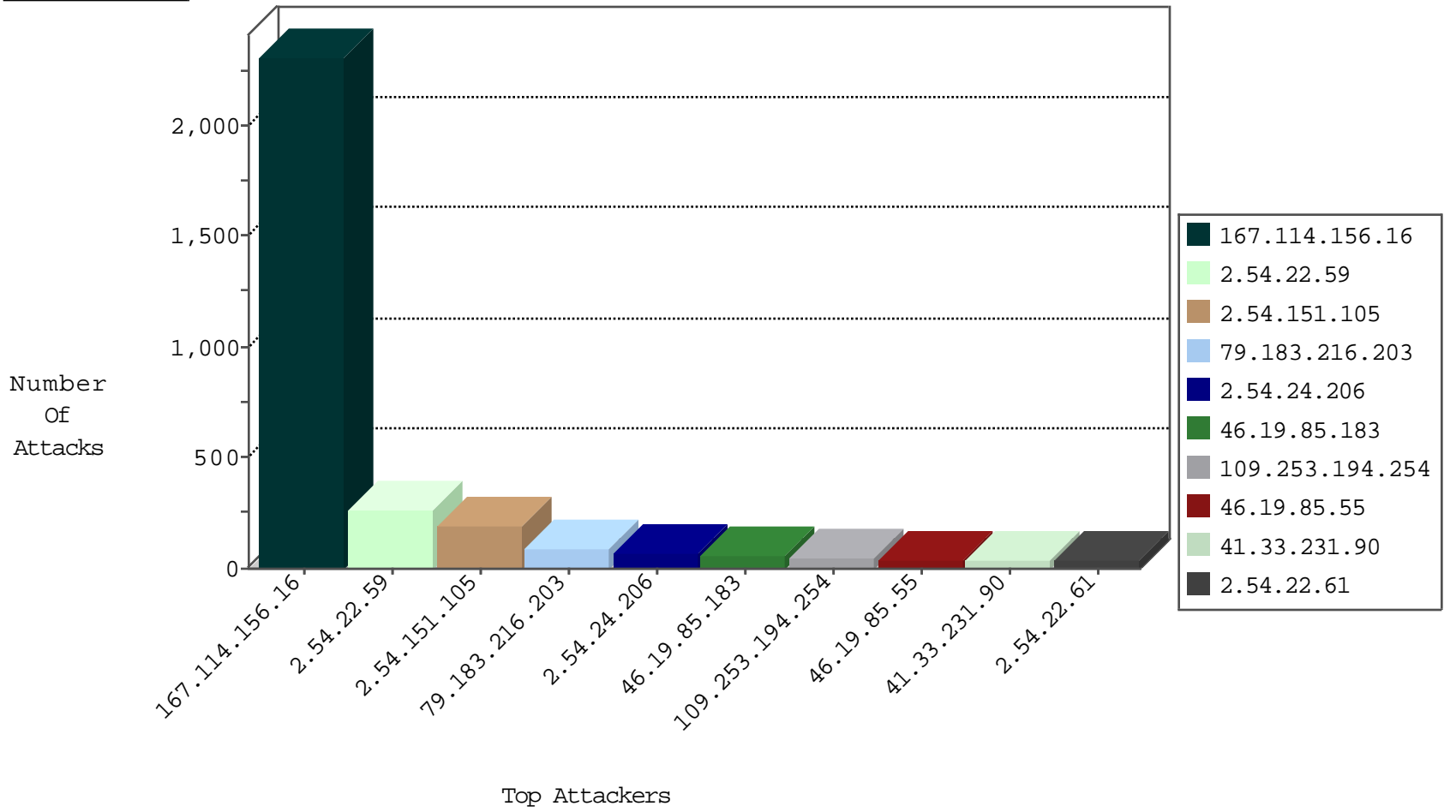
# IDF Under Attack Daily Report



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	3091
79.181.27.99	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
196.200.16.201	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.248.168.218	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.166	United States	147.237.77.176	matpash.idf.il	block-sp-trafl	drop	1
196.200.16.202	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.248.168.218	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.60	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	drop	1
196.200.16.203	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
95.100.174.66	Europe	147.237.76.177	ncoore.idf.il	Block_Udp_All_Nets	drop	1
196.200.16.200	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.54.160.213	United States	147.237.77.205	prisha.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.79.86.129	Netherlands	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
5.79.86.129	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	3
69.64.51.107	147.237.0.17	United States	m.ny-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.104.41.54	147.237.77.226	Moldova, Republic of	www.chamatz.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
182.72.109.162	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.76.148	Russian Federation	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
131.109.15.15	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
71.177.22.76	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
69.64.51.107	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.77.226	Moldova, Republic of	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.76.201	Moldova, Republic of	e.atal.idf.il	ET SCAN Potential SSH Scan	1
176.13.9.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.216.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.70.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.64.51.107	147.237.72.166	United States	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.151.105	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.55	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
2.54.22.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
46.19.85.117	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
176.13.18.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
2.54.24.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
113.78.16.128	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
79.182.151.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.24.206	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	13
2.54.182.63	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
2.54.24.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.24.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.24.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.161.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.201.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.22.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.123.156	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.217	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.116	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.199	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.2.197	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.24.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.133	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.2.197	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.106.47.50	Palestinian Territory Occupied	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
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
194.50.175.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.0.13.172	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
194.50.175.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.179.114.27	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.254	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.22.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.218.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.22.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
2.54.22.59	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.22.59	Block	105
79.183.216.203	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.183.216.203	Block	82
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
2.54.22.59	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.22.59	Block	42
109.253.194.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
109.253.143.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.130.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
31.168.75.47	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
5.79.86.129	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.79.86.129	Block	3
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.68.146.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.46.39.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.201.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.117.222.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	3
109.253.207.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.22.225	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
46.19.85.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.154.183.187	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
113.78.16.128	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 113.78.16.128	Block	2
2.54.147.29	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
5.102.254.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.235.68.81	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakchal.idf.il/1119-he/nakhal.aspx	Block	2
46.19.85.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.146.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.47.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.62.53.168	Russian Federation	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /admin/login	Block	1
77.87.21.70	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.54.22.59	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
176.13.15.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.218.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.6.247.242	Greece	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
109.67.128.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.44.176	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.32.179.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.110.143	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/xmlrpc.php	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.52.3.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
137.119.162.125	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
109.253.158.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.95.128.246	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
176.13.18.171	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 176.13.18.171	Block	1
77.87.21.70	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.6.247.242	Greece	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
209.88.198.1	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	1
109.67.191.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1