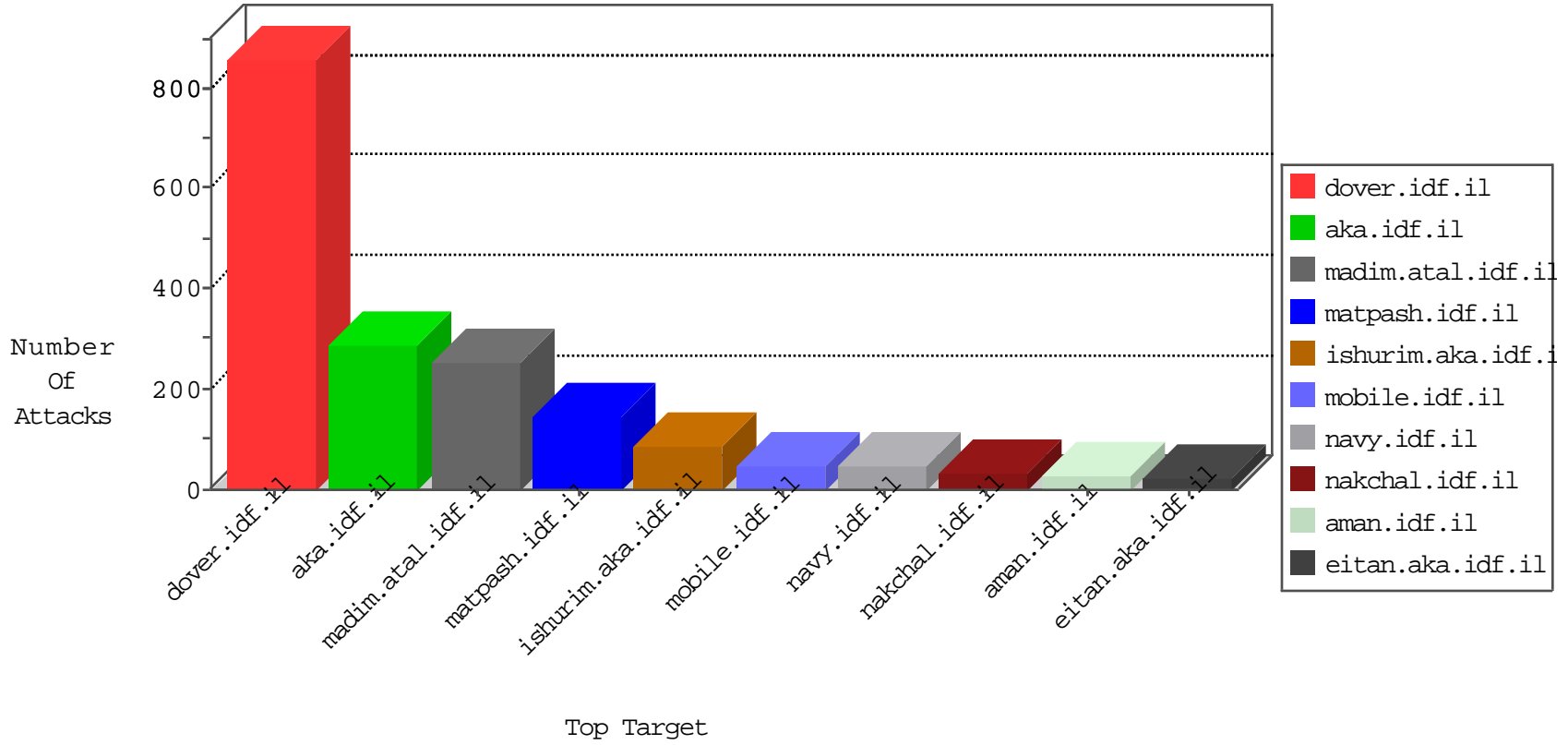


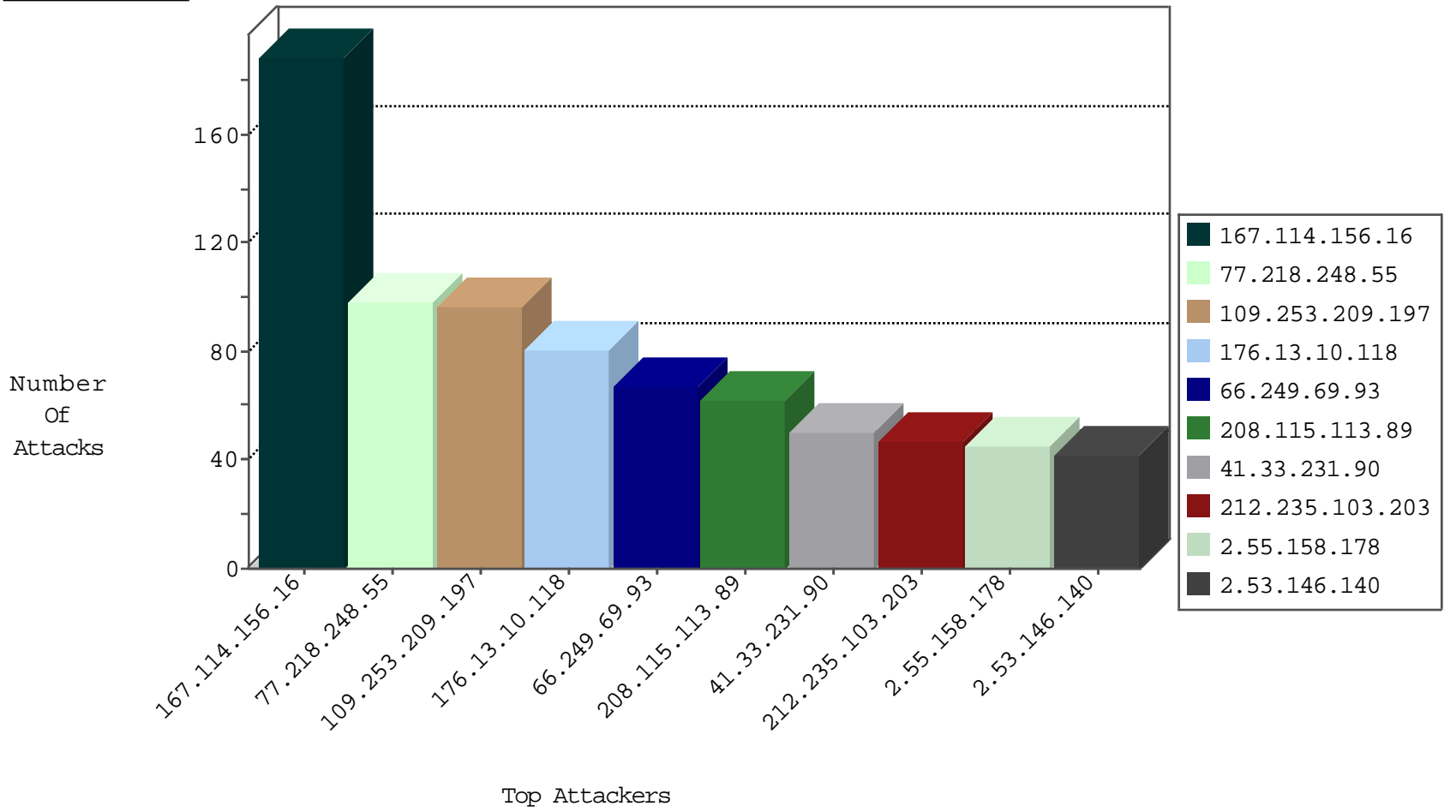
IDF Under Attack Daily Report



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	TCP handshake violation, first packet not syn	drop	9874
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	8471
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3681
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
185.82.52.225	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
185.82.52.225	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
194.89.24.53	Finland	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	2
183.60.48.25	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
66.249.69.93	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

04-21-2016-13:04:00 to 04-21-2016-14:04:00

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
82.81.106.102	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
199.203.92.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
156.198.59.94	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
84.111.105.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.130.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.225.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.169.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.214.73.227	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -f -sS	1
84.109.162.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.165.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.135.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.218.248.55	Sweden	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	98
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
212.235.103.203	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	47
2.53.146.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
2.55.134.233	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.64.36.90	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
8.37.231.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.228.162.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.130.175.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.22.131.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
201.244.100.102	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
89.144.103.226	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
5.22.131.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
85.130.225.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.69.80.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.243	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.89.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	9
176.13.18.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.64.36.90	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.14.243.178	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.175.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.130.183.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.22.131.33	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.70.56.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.180	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.139.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.198.151.45	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
205.167.7.244	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.232.28.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.169.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.225.65	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.36.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.130.175.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.185.235.183	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.209.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
176.13.10.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
2.55.158.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
37.26.148.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
17.138.55.96	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.55.96	Block	6
109.253.224.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.224.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.47	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	3
95.86.119.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.210.172.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.37.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.203	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/templates/general/mobile	Block	2
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.167.144	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
82.81.106.102	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method Š•[[#24]]Ä[[#7]]³ù[[#17]]U in URL	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
192.243.55.130	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/1901.doc	Block	1
85.64.46.5	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
80.149.240.82	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
174.129.237.157	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method	Block	1
94.143.60.212	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation Pa.&SortDir in www.idf.il/1361-he/dover.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
82.81.106.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wepdwujnju0mjiwmzkwzgs6rkqqt8dqa2jzrm6zmayedq==/	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Abnormally Long Request method	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
85.65.111.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.70	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1
80.178.213.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
174.129.237.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/login.php	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Header Name	Block	1
94.159.160.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
212.143.173.198	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.143.173.198	Block	1
176.226.167.125	Russian Federation	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.228.109.213	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.109.213	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.28.175.172	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
89.152.239.93	Portugal	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
207.46.13.115	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
80.246.139.228	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.1.199	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
2.53.8.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.226.167.125	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
84.228.109.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1