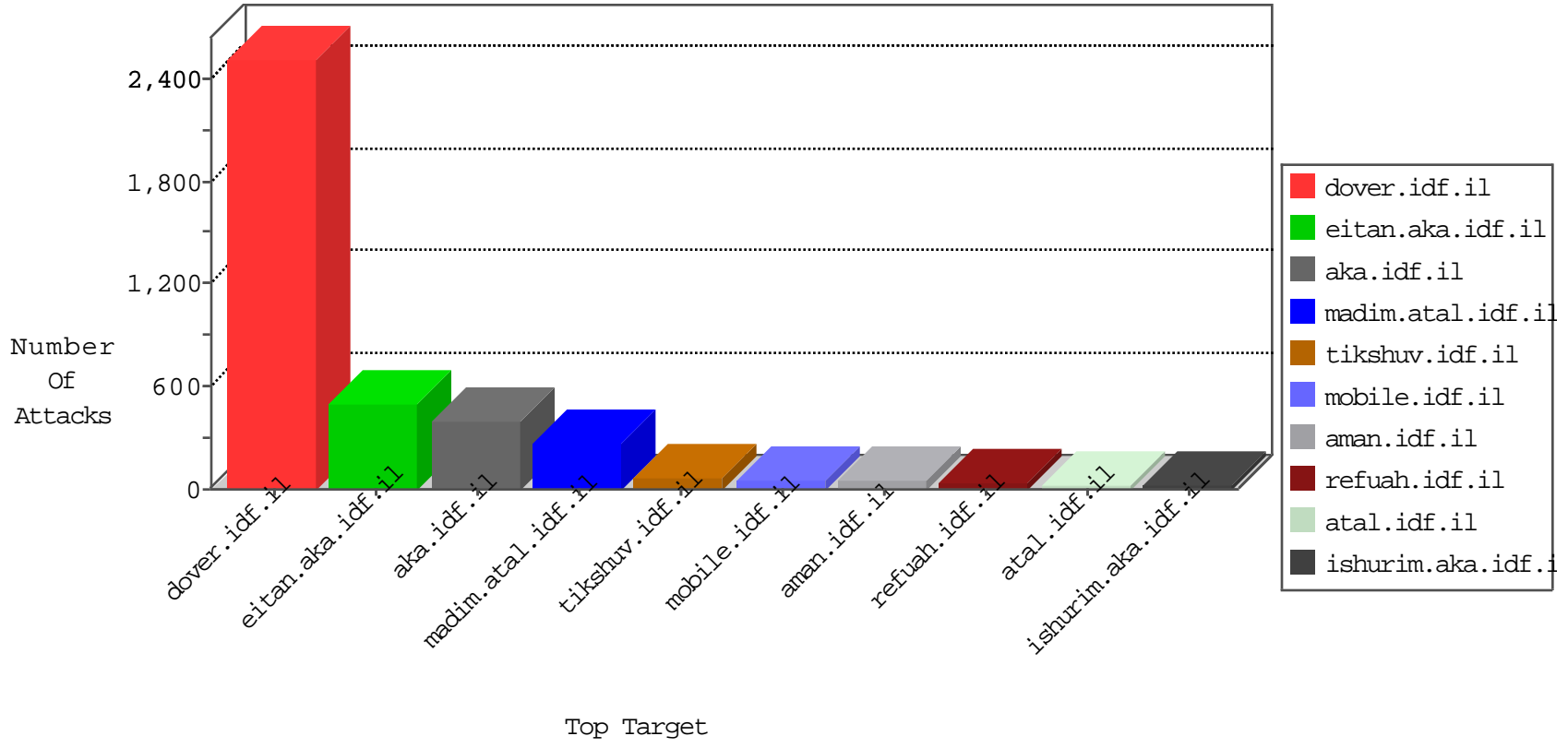


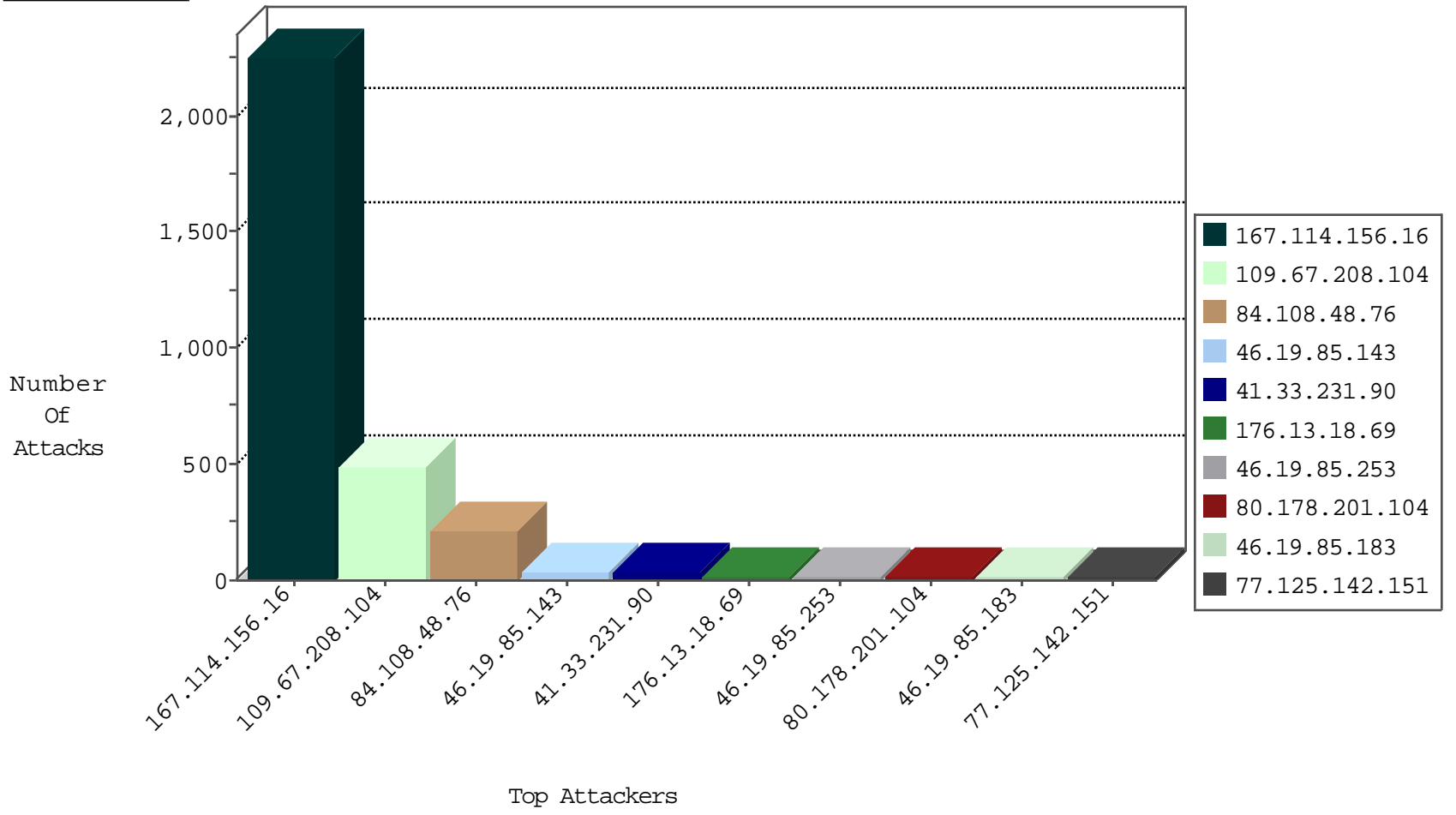
IDF Under Attack Daily Report



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	3126
46.19.85.143	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
146.185.57.7	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
37.204.243.111	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	forward	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

12-22-2015-15:04:00 to 12-22-2015-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.141.5	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.28.164.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.101.221.14	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.75.6.126	147.237.76.177	India	noore.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.214.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.197.103.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.173.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.206.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.73.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.201.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.27.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.75.6.126	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
119.81.208.132	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.196.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.162	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	1
80.230.21.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.12.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.69.30.108	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.208.104	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	447
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.181.123.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.151.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.180.12.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.199.224.24	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
66.249.75.201	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.210.186.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.182.205.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
94.159.170.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.228.242.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.164.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.134.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.51.36	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	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.228.242.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.164.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.51.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.116.250.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.230.98.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.142.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.142.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.223	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.254.202	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.224	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.192	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.31.106.40	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.109.165.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.26.149.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
176.13.7.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.48.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
84.108.48.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
109.67.208.104	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
176.13.18.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.85.253	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	17
80.178.201.104	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.178.201.104	Block	16
84.108.48.76	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 84.108.48.76	Block	15
37.26.148.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
185.32.179.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1598	Block	4
120.52.73.37	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	4
79.183.213.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
176.13.6.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
200.8.146.216	Venezuela	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
136.243.109.205	Germany	147.237.0.34	tikshuv.idf.il	Distributed Illegal HTTP Version	Block	3
176.13.23.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
221.178.182.132	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
8.43.65.40	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
172.246.226.48	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
136.243.109.205	Germany	147.237.0.34	tikshuv.idf.il	Distributed Malformed URL	Block	3
176.13.0.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.27.156.37	Russian Federation	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	3
37.142.152.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
80.178.144.144	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.178.144.144	Block	2
87.255.70.30	Moldova, Republic of	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
79.178.49.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
119.163.41.11	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/901-8581-he/tikshuv.aspx#.vnmgev196uk	Block	2
190.203.71.95	Venezuela	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/templates/sendtofriend	Block	2
46.117.228.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.139.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.25.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.64.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
218.205.17.158	China	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter FolderId	Block	2
2.54.45.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
172.246.226.56	United States	147.237.0.34	tikshuv.idf.il	Distributed Malformed URL	Block	1
95.76.161.34	Romania	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
87.255.70.30	Moldova, Republic of	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/901-8581-he/tikshuv.aspx#.vnmgev196uk	Block	1
196.22.142.44	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.176.130.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.80	United States	147.237.77.170	maarachot.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
111.67.11.193	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.142.190.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.aspxdfds	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1785-he/dover.aspx	Block	1
46.236.24.53	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1