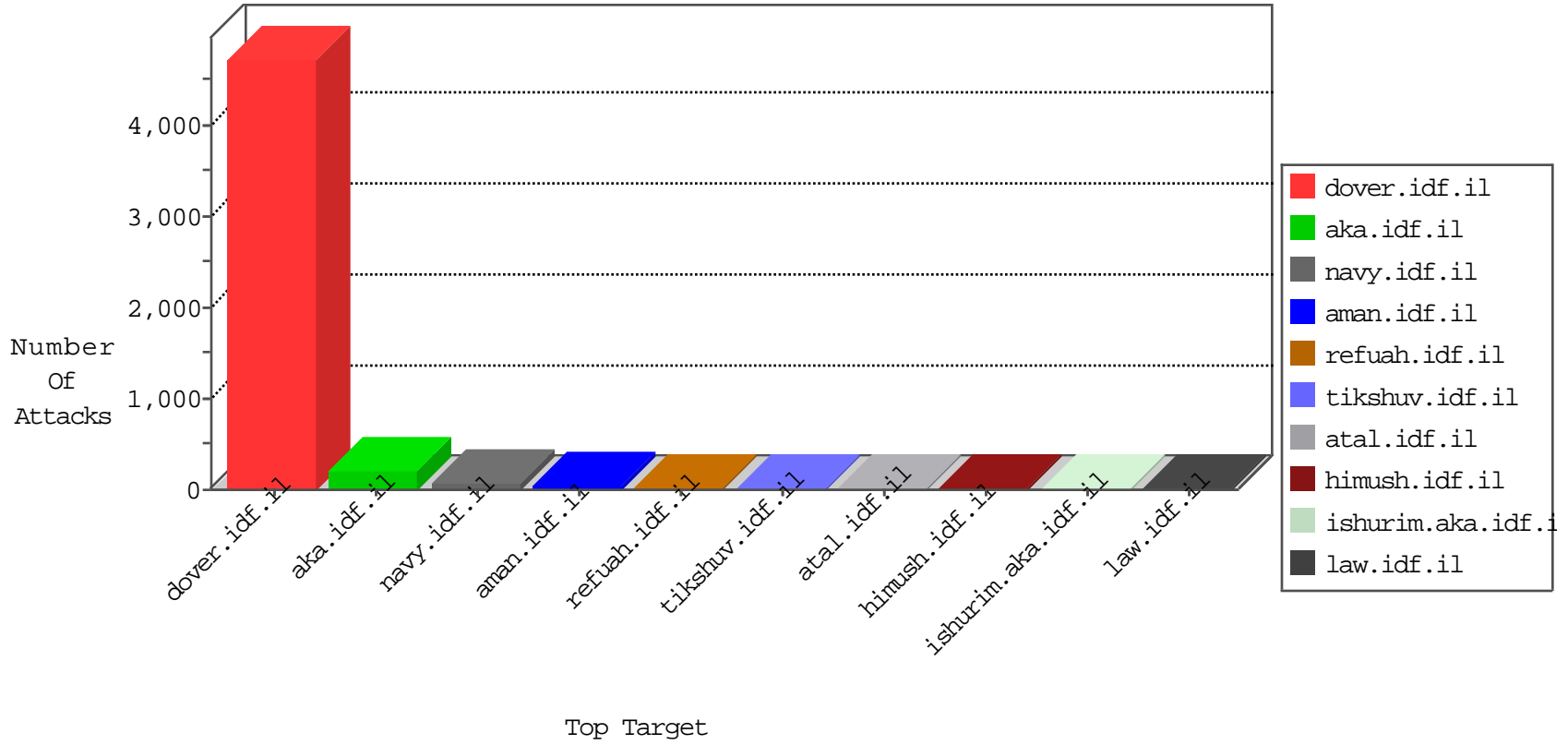
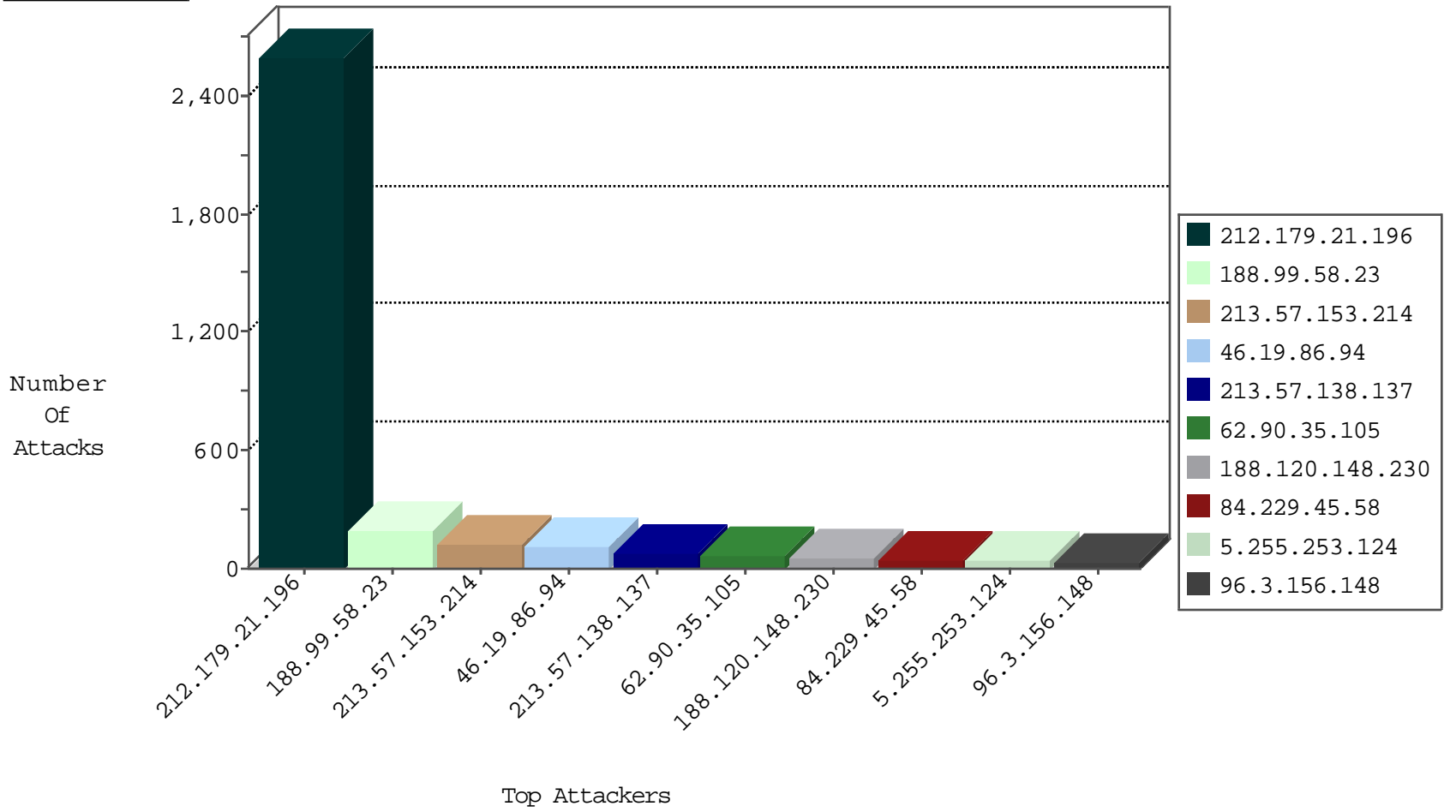


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
212.179.21.196	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2628
46.120.17.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	68
87.69.90.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
176.12.148.88	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	33
77.125.92.161	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
119.67.72.238	Korea, Republic of	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	3
37.142.236.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
43.229.52.201	Japan	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Top	drop	2
93.120.27.62	Romania	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
37.26.147.170	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
123.224.113.80	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.126.15.138	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
109.65.75.46	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
109.65.75.46	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.i	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.220	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
72.52.6.10	United States	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
50.200.184.90	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
87.69.86.177	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.0.200	mAu.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.i	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	7610: IP Reputation	Block	1
80.179.196.69	Israel	147.237.77.216	dover.idf.il	2023: HTTP: Cross Site Scripting in GET Request	Block	1
71.6.135.131	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.148	ggcenter.aka.idf.i	7610: IP Reputation	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.194	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.72.167	ishurim.aka.idf.il	7610: IP Reputation	Block	1
93.120.27.62	Romania	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.160.224.130	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.61.150.154	Taiwan	147.237.0.33	idf.il	ET SCAN NMAP -sS window 4096	1
37.26.147.199	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
185.45.192.252	Seychelles	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
175.139.183.57	Malaysia	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
132.68.145.107	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.169.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
79.182.55.86	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
69.159.196.84	Canada	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.89.137.3	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
50.243.68.162	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.52.131.212	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
183.247.165.129	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
175.139.183.57	Malaysia	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
128.199.167.194	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
82.221.47.101	Iceland	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
69.159.196.84	Canada	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2586
188.99.58.23	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	190
213.57.153.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	124
46.19.86.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	108
213.57.138.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	80
62.90.35.105	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	60
188.120.148.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
84.229.45.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
195.65.154.50	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
96.3.156.148	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
77.87.228.68	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
94.159.239.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
194.61.92.41	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
105.200.56.195	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
2.52.11.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
37.26.147.189	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
193.106.52.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
37.142.236.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
37.26.147.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
77.125.153.140	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
46.19.85.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
212.179.56.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
5.29.124.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
37.142.255.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
46.19.86.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
84.94.221.148	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.137.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
192.114.105.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
213.6.0.57	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.86.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.64.68.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
37.142.255.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
31.168.78.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
80.246.133.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
213.8.109.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
80.246.130.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
172.56.23.27	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
80.246.130.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
61.185.9.93	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.228.86.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
77.126.15.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
93.172.23.253	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
54.88.168.129	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 54.88.168.129	Block	5
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	4
84.108.79.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	3
79.179.36.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
93.173.2.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.116.90.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	3
194.90.134.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	3
5.144.62.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.216	Block	2
50.243.68.162	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 50.243.68.162	Block	2
79.100.234.123	Bulgaria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.100.234.123	Block	2
80.179.96.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.32.178.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/938-he/atal.aspx	Block	1
132.68.145.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyud	Block	1
84.108.39.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.100.234.123	Bulgaria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
205.222.248.208	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1571-en/dover.asp	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19781-he/dover.aspx	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
87.68.36.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.133.4	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
2.52.131.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
185.32.178.215	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
71.185.177.222	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.88.168.129	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he/tikshuv.aspx#.vvcpovmqoqq	Block	1
149.88.107.86	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.6.71.218	Poland	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
212.150.174.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.199	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_text.asp	Block	1
2.52.154.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
80.246.133.255	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.90.35.105	Israel	147.237.72.166	aka.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
31.154.17.126	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
84.108.82.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
79.181.135.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.221.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
175.44.28.250	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/main.asp/trackback/	Block	1
109.65.26.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
50.243.68.162	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
2.54.151.246	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.90.178.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.240.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.205	Israel	147.237.76.31	nakhal.idf.il	Unauthorized URL Access to 147.237.76.31/1117-7668-he/nakhal.aspx	Block	1
157.55.39.152	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/sitemap/	Block	1
84.108.90.162	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1