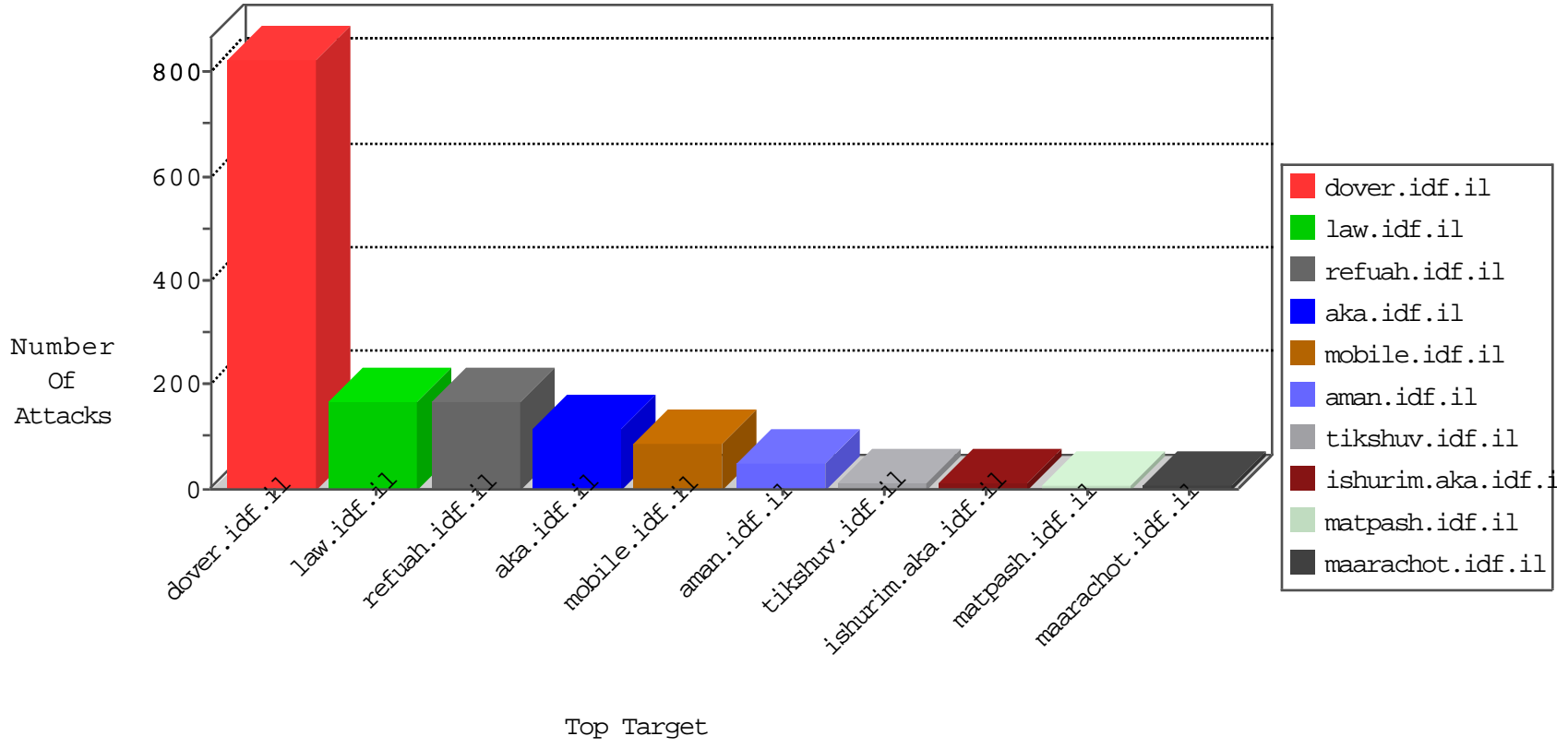
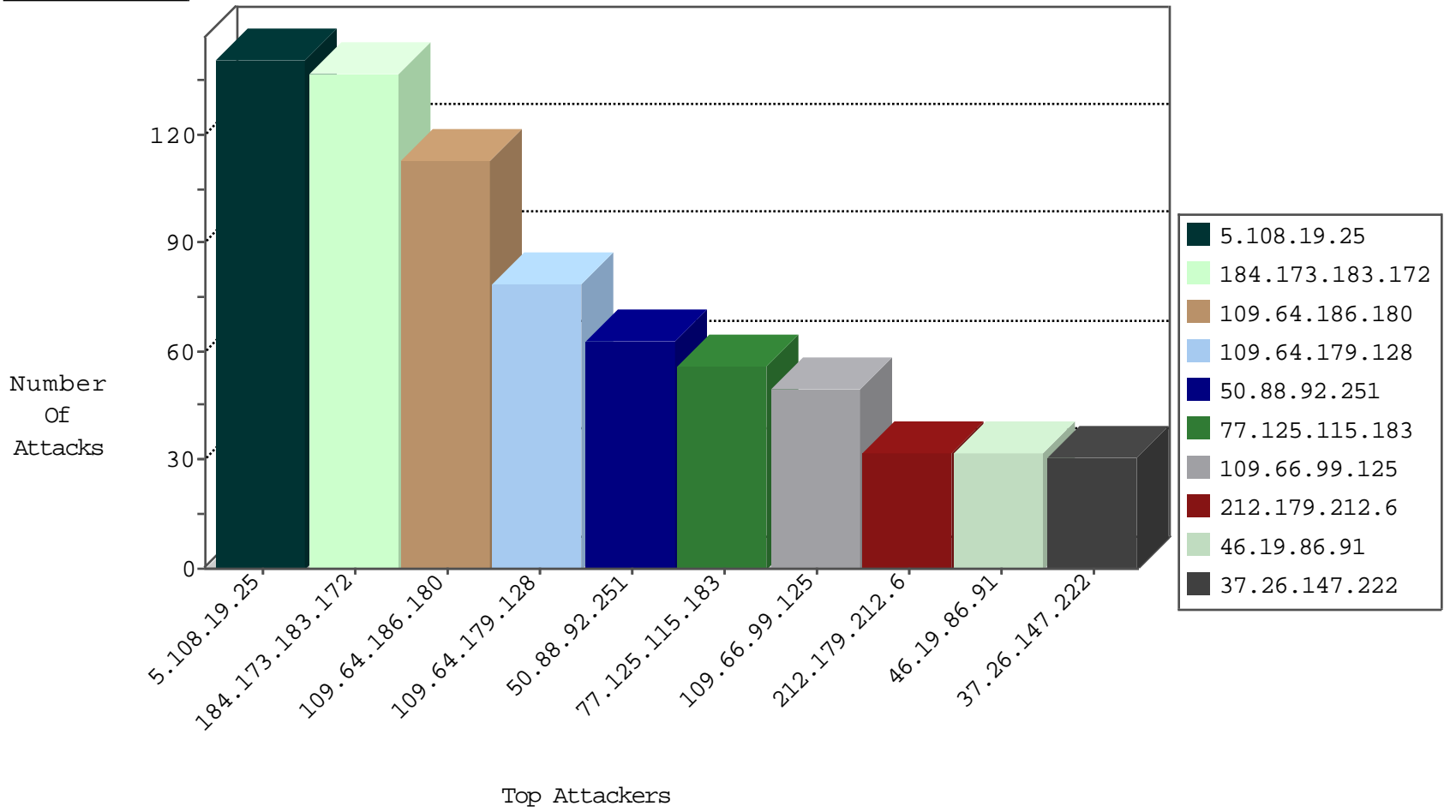




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.254	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1136
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	546
212.179.212.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
80.230.95.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
37.26.147.210	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
5.29.27.40	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
5.29.27.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block Udp_All_Nets	drop	4
77.127.118.71	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
77.127.118.71	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
185.32.176.54	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
84.109.178.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
185.32.176.54	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
124.232.142.220	China	147.237.76.31	nakchal.idf.il	Block Udp_All_Nets	drop	1
176.12.142.28	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
58.189.59.83	Japan	147.237.76.198	e.yohalan.idf.il	Block Udp_All_Nets	drop	1
93.172.21.149	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	137
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	2
79.180.194.249	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.250.170.36	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	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	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	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.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	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
2.54.129.76	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.9.218	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.204.117	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
2.54.0.175	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.139.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.95.110.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.248	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.120	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
207.87.255.162	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.165.129.51	Spain	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
122.0.80.239	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
122.0.80.239	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
122.0.80.239	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
162.144.97.151	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	1
122.0.80.239	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
122.0.80.239	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.108.19.25	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	137
109.64.186.180	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	110
109.64.179.128	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
50.88.92.251	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
77.125.115.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
109.66.99.125	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	50
46.19.86.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
37.26.147.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
85.250.170.36	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
150.209.207.134	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
46.19.85.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
5.102.214.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
207.46.13.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
31.168.170.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
178.234.114.182	Russian Federation	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	11
212.179.212.6	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
93.173.61.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.85.68	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
2.54.160.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
78.108.169.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.22.129.172	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
154.121.251.26		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.107	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
5.22.129.172	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	7
46.19.86.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
2.54.129.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.179.155.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
92.98.185.240	United Arab Emirates	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.179.212.6	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
79.176.155.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
37.26.147.210	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
50.122.221.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
149.78.41.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
89.139.12.129	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
37.26.147.210	Israel	147.237.77.216	dover.idf.il		Bad TCP sequence	monitor	4
87.68.41.118	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
84.229.35.26	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
77.125.213.171	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
85.250.107.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.111.15.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.179.128	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.64.179.128	Block	7
79.177.18.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
5.22.129.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
149.78.233.30	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.178.178.246	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.76.96.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/www.navy.idf.il	Block	3
93.172.15.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.148.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.194.249	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
154.121.251.26		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 154.121.251.26	Block	2
109.66.183.58	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
31.154.10.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.222.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/gyus/faq.aspx	None	1
79.181.185.118	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.129.51	Spain	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
52.6.13.145	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
157.55.39.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19422-he/dover.aspx	Block	1
2.54.58.217	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
79.178.14.222	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
203.133.171.19	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
167.114.156.198	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/chinuch/gallery/showpicture.asp	None	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
46.19.86.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.151.63.196	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
80.178.28.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.126.151.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
188.165.129.51	Spain	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.66	Block	1
2.222.107.214	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
207.46.13.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19417-he/dover.aspx	Block	1
176.12.136.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	1
46.121.108.84	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
149.88.25.115	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
80.246.140.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.89.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
188.165.129.51	Spain	147.237.77.216	dover.idf.il	WordPress SoakSoak Malware - 1	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
4.28.133.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
207.46.13.96	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
178.234.114.182	Russian Federation	147.237.77.74	law.idf.il	Multiple Admin Blocking from 178.234.114.182	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/halochamim	Block	1
46.121.108.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
2.52.1.138	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
84.95.200.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
77.237.138.51	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
192.187.124.251	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1