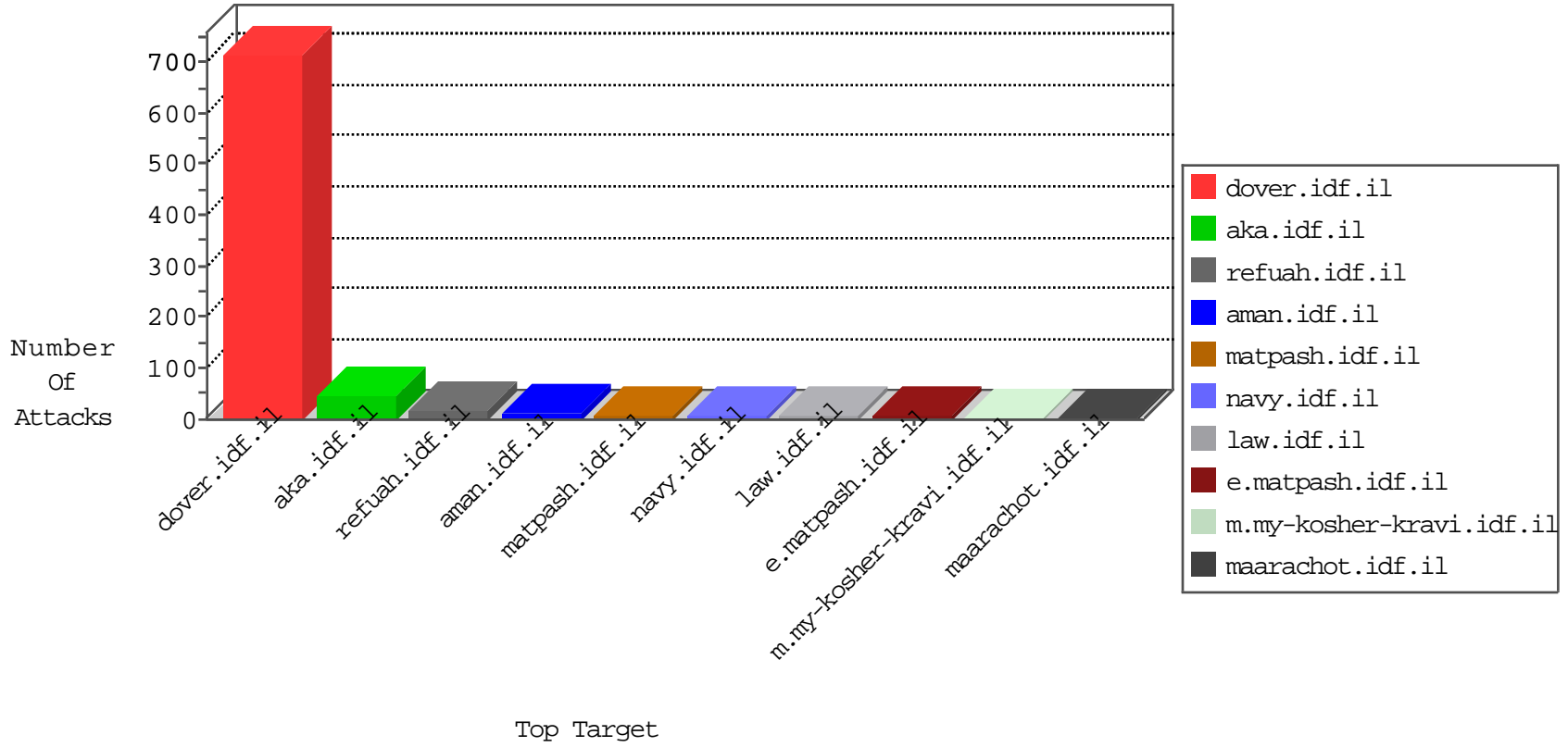
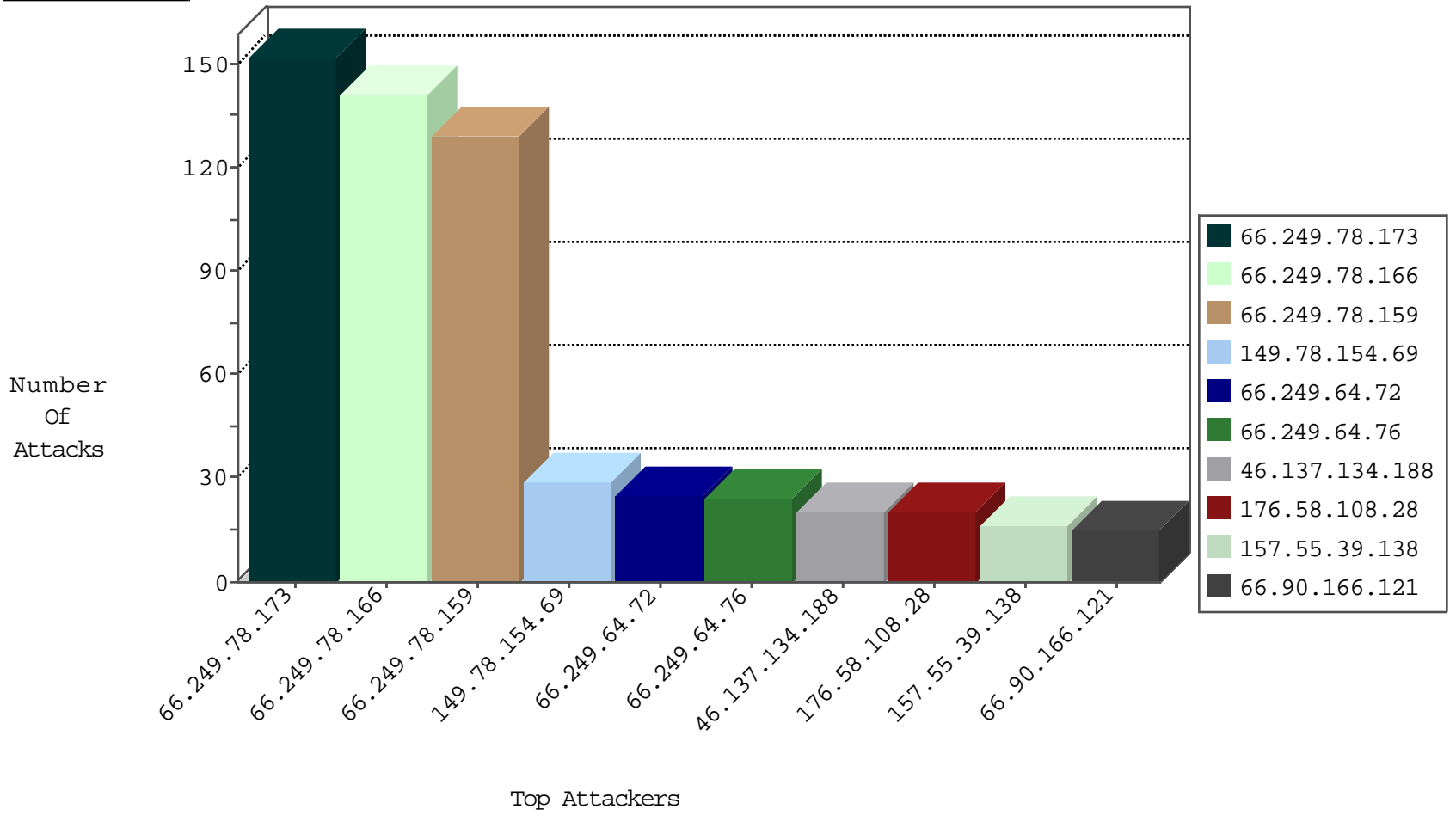


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	228
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
195.37.190.86	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
124.232.142.220	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
124.232.142.220	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.147	chimuch.aka.idf.il	Block_Ntp_All_Net	drop	1
124.232.142.220	China	147.237.76.34	ychalan.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
188.120.148.218	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
196.33.158.34	South Africa	147.237.77.235	sviva.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
93.115.83.16	Anonymous Proxy	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
98.118.10.246	United States	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
74.73.231.54	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
180.251.0.236	Indonesia	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.44	e.refuah.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
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
183.232.128.156	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.161	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.153.119.116	United Kingdom	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
91.230.45.251	Slovakia	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
81.200.91.2	Russian Federation	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 3072	1
218.77.79.43	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
205.189.20.55	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.161	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
183.232.128.156	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.140	Netherlands	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.229.166.28	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
218.77.79.43	China	147.237.77.179	e.mazi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
61.240.144.67	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
176.58.108.28	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
66.90.166.121	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
107.196.32.7	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.19.85.179	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
109.65.169.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
188.120.148.218	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
157.55.39.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.185.12.165	South Africa	147.237.77.216	dover.idf.il	SAM rule	drop	drop	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.247.36.123	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
114.79.13.141	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
94.228.34.250	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
188.120.148.218	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
174.84.226.148	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
141.161.133.216	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
180.251.0.236	Indonesia	147.237.77.216	dover.idf.il	Havij Automated SQL Injection tool	Web Server Enforcement Violation	reject	2
157.55.39.61	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.37.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
162.234.45.241	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
190.162.234.149	Chile	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
136.243.36.97	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.120.148.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.46.145.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
136.243.36.97	Germany	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
185.53.44.63		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	120
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	75
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	65
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	27
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	20
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	16
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	14
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	11
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
46.229.164.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
95.130.13.153	France	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 95.130.13.153	Block	2
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	2
185.53.44.105		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/alnajah/alnajah.stm	Block	1
74.73.231.54	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
180.76.4.239	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/print_text.asp	Block	1
66.249.75.9	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
221.121.250.28	Japan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 221.121.250.28	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.195	Block	1
109.253.142.124	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
185.53.44.61		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.61	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13355-en/dover.aspx forcerecrawl: 0	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0102-1.stm	Block	1
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1312-he/refuah.aspx	Block	1
52.4.251.232	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
185.53.44.119		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0107-1.stm	Block	1
95.56.24.75	Kazakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/wp-includes/pomo/so.php	Block	1
180.251.0.236	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/	Block	1
221.121.250.28	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/merkava4/english/table.stm	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/klali.aspx	Block	1
113.210.137.189	Malaysia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/wp-includes/text/tiff.php	Block	1
189.141.204.248	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/wp-content/themes/hello.php	Block	1
185.53.44.66		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/6.stm	Block	1
172.252.82.198	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
157.55.39.53	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/	Block	1
66.249.69.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1681-he/refuah.aspx	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unknown Parameter </script in www.aka.idf.il/ishurim/main/url	None	1
185.53.44.201		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
184.105.247.195	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.75.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
114.79.13.141	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/wp-content/uploads/rss.php	Block	1
66.249.67.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71859-he/maarachot.aspx	Block	1
192.187.110.98	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1