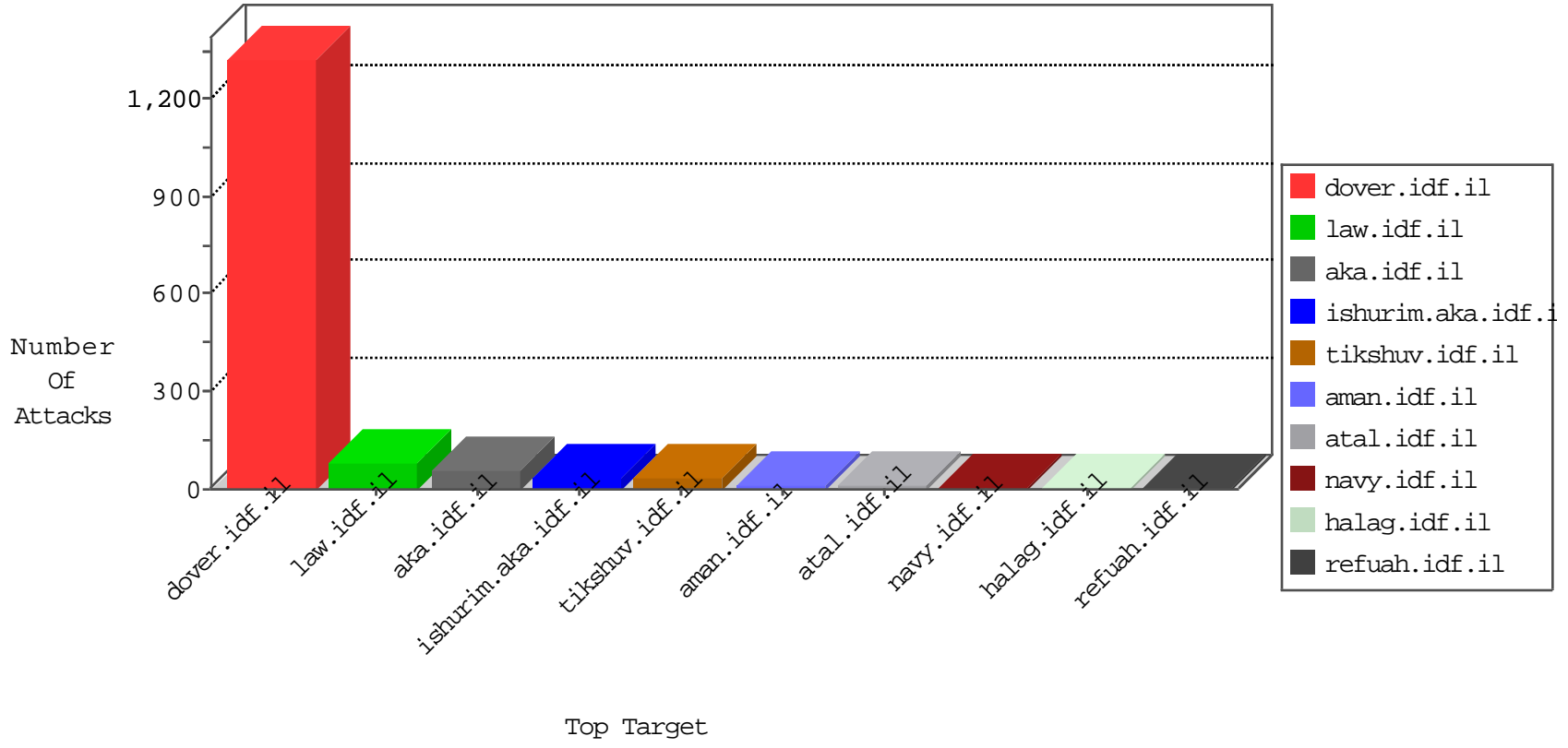
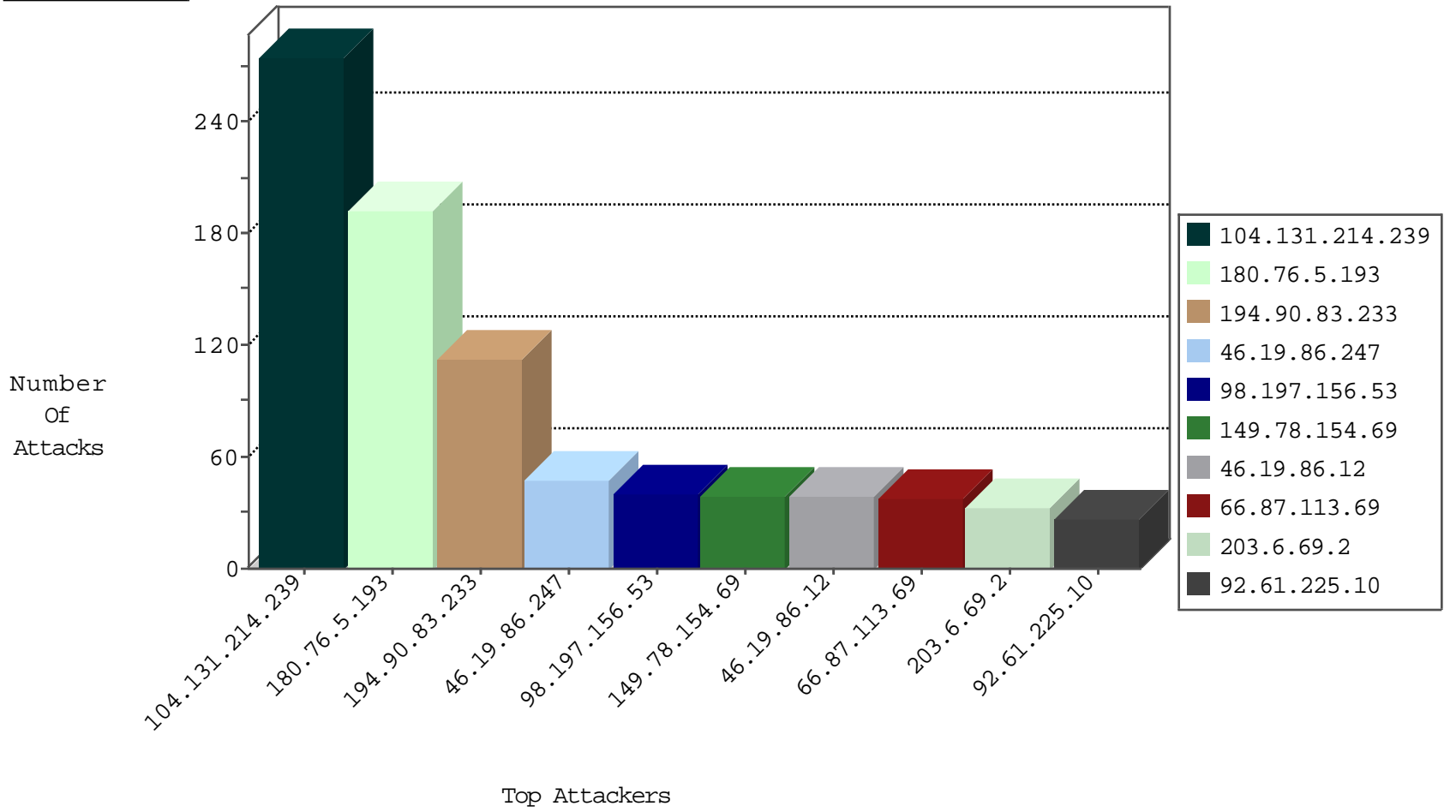




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.181.131.71	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	224
2.54.38.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
82.166.165.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
2.54.140.70	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
2.54.140.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
211.137.190.38	China	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Http	drop	1
2.54.146.217	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
104.131.214.239		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.14.183.124	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	113
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	79
62.219.164.244	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.192.138	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	2
71.93.88.133	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.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	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.156	aman.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
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.50	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yochanan.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
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
71.6.165.200	United States	147.237.76.196	e.sviva.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
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yochanan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.202	e.halag.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	7
61.160.224.128	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.49.45.41	China	147.237.77.205	prisha.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
46.19.86.149	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
5.231.205.182	Germany	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.130		147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.78.154	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.64	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.49.45.41	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
210.61.150.154	Taiwan	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.0.60	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
104.131.214.239		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	268
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	112
46.19.86.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
98.197.156.53	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
46.19.86.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
66.87.113.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
203.6.69.2	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
146.185.35.148	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
37.26.148.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
37.115.187.198	Ukraine	147.237.72.166	aka.idf.il	SAM rule	drop	drop	18
132.70.66.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
162.243.61.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	17
80.246.133.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
212.235.98.139	Israel	147.237.72.167	ishurim.aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	14
46.120.74.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.132.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
98.127.196.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.160.216.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
70.209.52.23	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
82.205.102.233	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.179.13.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.149	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
181.64.209.57	Peru	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
82.166.165.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
75.157.36.133	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.182.121.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.108.96.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.109.109.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
91.199.69.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.52.14.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
147.236.138.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
62.128.35.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
194.90.134.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	4
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.14.233.94	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.222	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//captcha.ashx	Block	18
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//captcha.ashx	Block	5
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//main/gyus/gyus/general.aspx	Block	3
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
63.141.249.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17436-en/dover.aspx/trackback/	Block	1
77.237.154.221	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/870-4414-he/patzar.aspx	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9688-he/refuah.aspx	Block	1
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct199 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
66.249.64.215	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
2.54.45.176	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.222	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//main/gyus/gyus/general.aspx	Block	1
87.68.33.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.136	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71782-he/maarachot.aspx	Block	1
188.165.15.192	France	147.237.76.30	himush.idf.il	Unknown Parameter PageNum in www.chimush.atal.idf.il/994-he/himush.aspx	None	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/edim/fund/funddesc.asp	None	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/shared/ajax/createcaptchainage.aspx	Block	1
5.22.130.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
157.55.39.222	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/home/default.aspx	Block	1
94.180.197.44	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.git/index	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/january/29.stm	Block	1
212.76.98.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.83.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13802-he/kkkkkkk=ccdf7342kkkkkkk_ccdf7342	Block	1
31.193.51.59	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
104.131.214.239		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
66.249.73.197	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listfaq/1935	Block	1
212.199.244.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
62.128.35.129	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
66.249.67.23	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
188.165.15.14	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/may/mevukash.stm	Block	1
37.115.187.54	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
109.186.26.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.73.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1678	Block	1