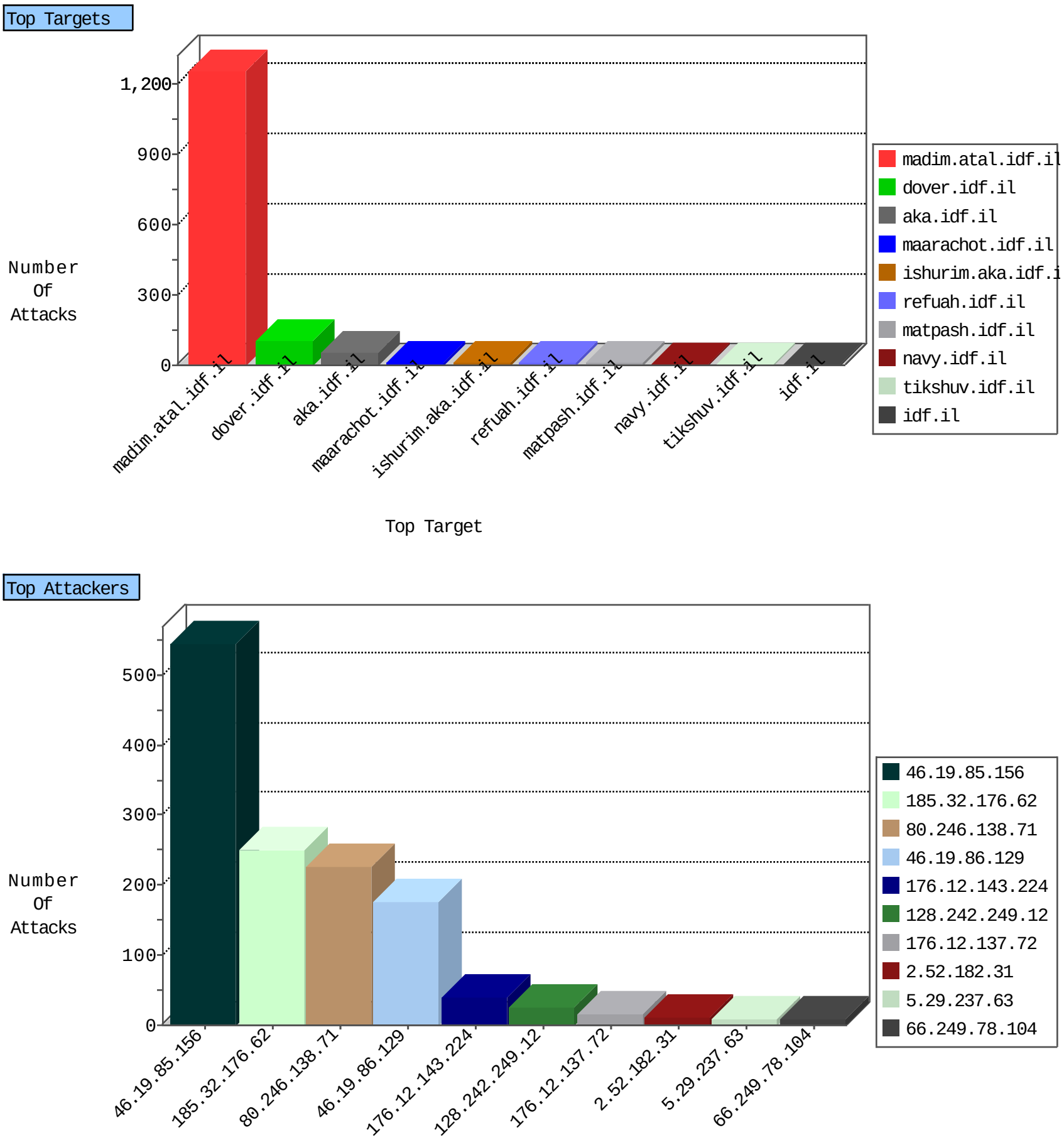
04-26-2015-08:03:05 to 04-26-2015-09:03:05

IDF Under Attack
04-26-2015-08:03:05



04-26-2015-08:03:05 to 04-26-2015-09:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1057
5.29.237.63	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
93.173.142.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
5.28.167.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
138.134.102.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
109.253.144.128	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
80.246.136.208	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.147.223	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
1.64.143.177	Hong Kong	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
172.245.109.82	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
46.19.86.186	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
118.236.87.106	Japan	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

04-26-2015-08:03:05 to 04-26-2015-09:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	26
93.120.27.62	Romania	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.98	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	147.237.72.167	ishurim.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
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1

04-26-2015-08:03:05 to 04-26-2015-09:03:05

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	2
66.249.81.144	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.161	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
209.88.198.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
43.255.191.161	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
14.139.127.124	India	147.237.0.34	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.62.125	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.132.118	Russian Federation	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.3.44	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
204.13.200.28	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.196	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
194.90.128.25	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.149.253	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
98.143.148.107	United States	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
82.80.196.44	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.162	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	1
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
218.77.79.43	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1

04-26-2015-08:03:05 to 04-26-2015-09:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.52.182.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
80.246.130.65	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.67.19.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
37.26.146.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
188.120.148.149	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
216.218.206.87	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
85.250.36.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
195.200.205.2	Israel	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	1
37.26.147.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
216.223.27.22	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
101.127.27.148	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
203.17.46.71	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
31.168.178.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.179.21.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
31.210.186.171	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
213.57.240.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	546
185.32.176.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	251
80.246.138.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	227
46.19.86.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	176
176.12.143.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
176.12.137.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
93.172.163.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
120.25.207.108	China	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 120.25.207.108	Block	3
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
149.78.99.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
84.228.178.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.10.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.117.152.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
2.54.175.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
37.60.40.96	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	2
176.12.151.218	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1029.stm	Block	1
46.19.86.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	1
24.7.42.65	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
77.125.75.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.203.226.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/ordnance/ordnance.stm	Block	1
41.189.43.98	Cote D'Ivoire	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
2.54.1.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.135.170	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.228.7.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
46.19.86.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
31.13.100.113	Ireland	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 31.13.100.113	Block	1
94.102.53.195	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/includes/templates/error.tpl	Block	1
79.180.123.34	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal/natziv.stm	Block	1
176.12.140.222	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	Distributed Suspicious Response Code	Block	1
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general.aspx	Block	1
41.189.43.98	Cote D'Ivoire	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
66.249.81.208	Israel	147.237.76.30	himush.idf.il	URL is Above Root Directory www.chimush.atal.idf.il/../favicon.ico	Block	1
157.55.39.170	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/undefined	Block	1
95.173.190.6	Turkey	147.237.77.235	sviva.idf.il	Illegal HTTP Version	Block	1
31.13.100.113	Ireland	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files	Block	1
80.246.133.32	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.95	Block	1
176.12.142.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/2004/february/0218-1.stm	Block	1
84.109.44.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1