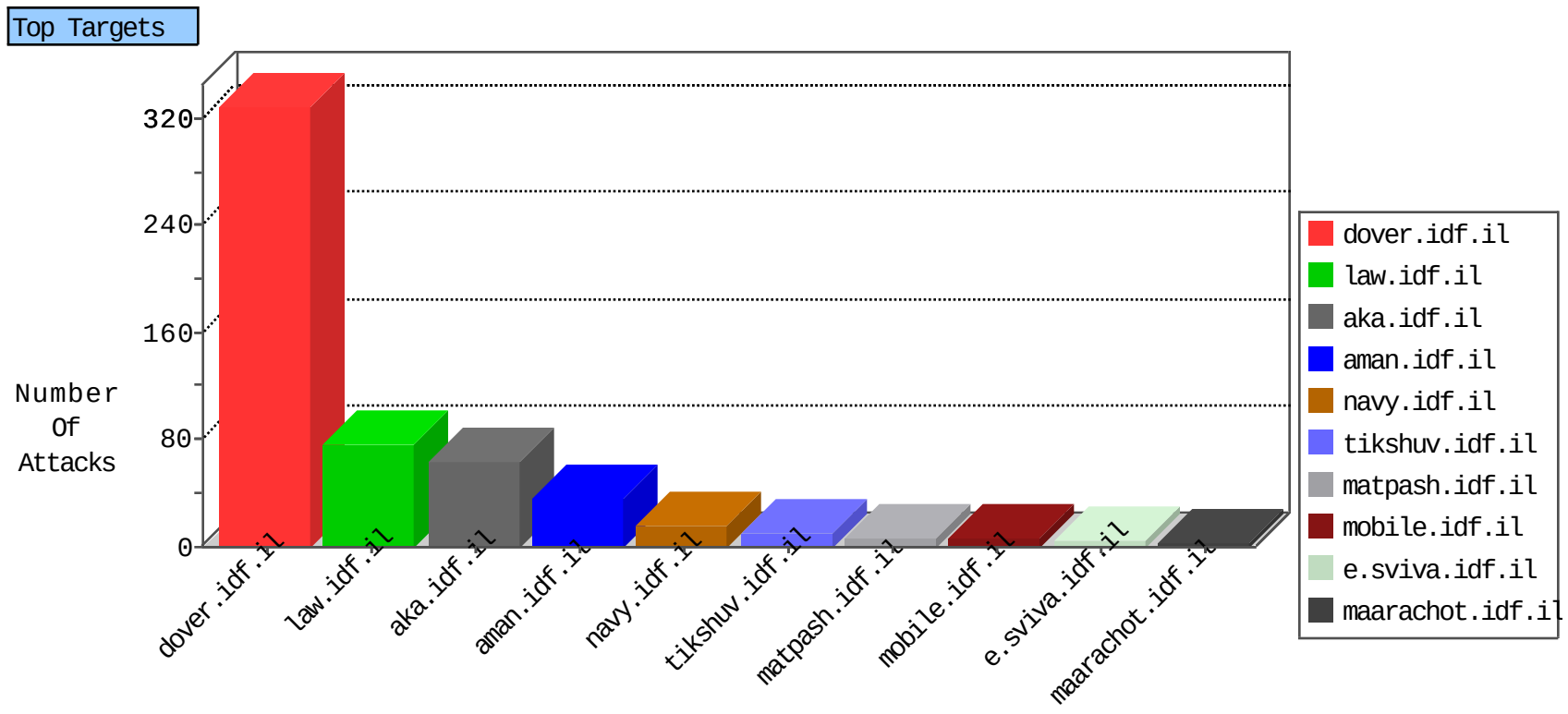
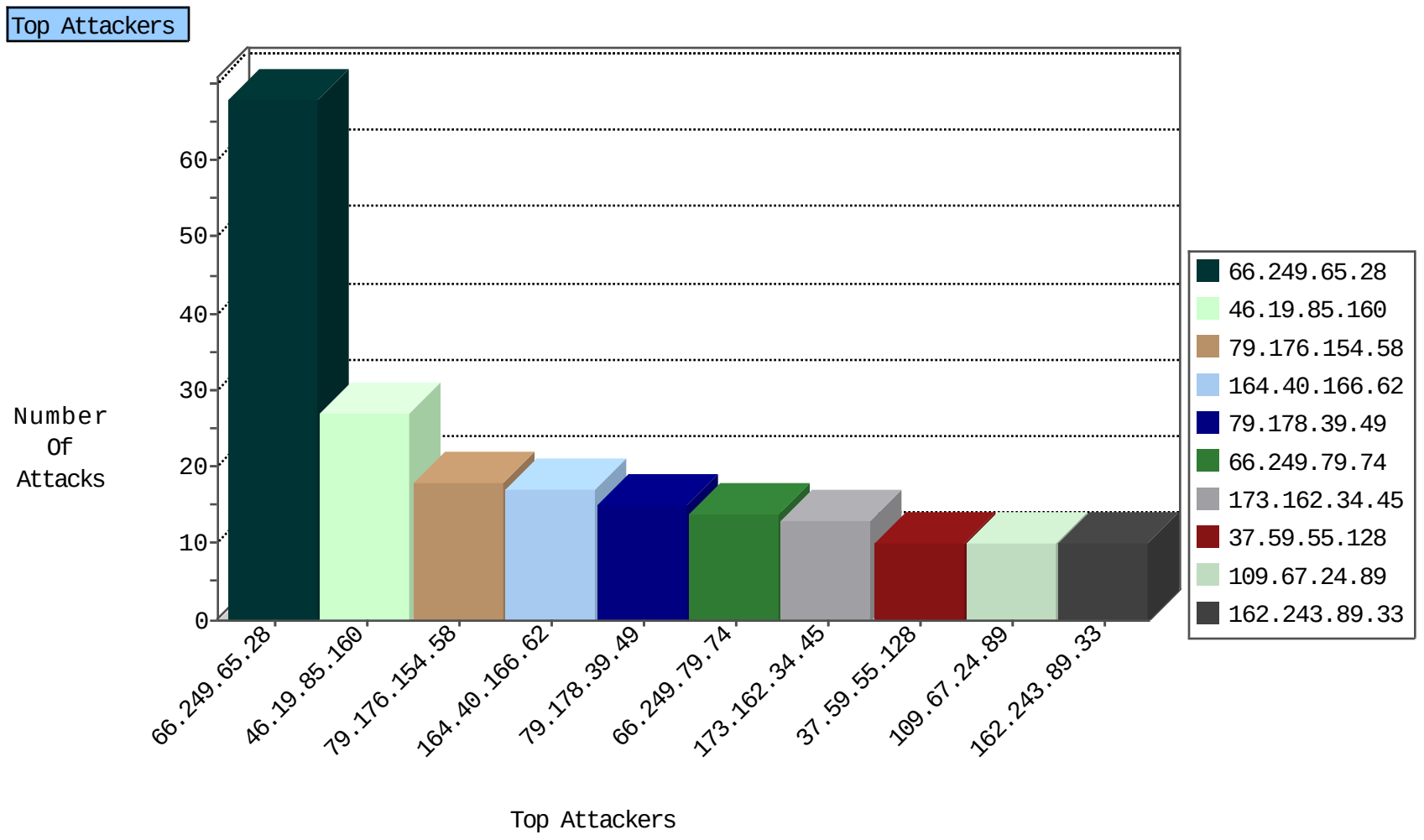
04-24-2015-15:03:09 to 04-24-2015-16:03:09

IDF Under Attack
04-24-2015-15:03:09

Top Targets



Top Attackers



04-24-2015-15:03:09 to 04-24-2015-16:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
173.162.34.45	United States	147.237.72.156	aman.idf.il	TCP Scan (vertical)	drop	335
79.178.39.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
213.57.96.82	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
192.168.14.198		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
192.168.2.106		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
201.234.230.209	Venezuela	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
89.139.162.91	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.61.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.168.1.101		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
199.180.114.241	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
201.234.230.209	Venezuela	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.230.28.30	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.32.177.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
195.37.190.86	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

04-24-2015-15:03:09 to 04-24-2015-16:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.85	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	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
49.148.90.178	Philippines	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	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
79.176.0.29	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
37.142.201.144	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
80.230.28.30	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-15:03:09 to 04-24-2015-16:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	68
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
85.250.17.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.37.226	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
89.138.95.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
120.82.95.83	China	147.237.8.27	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.186.16.225	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.210.205.2	Saudi Arabia	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
213.210.205.2	Saudi Arabia	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.197.48.113	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	1
113.21.226.56	New Zealand	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

04-24-2015-15:03:09 to 04-24-2015-16:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
79.176.154.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
164.40.166.62	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
109.67.24.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
85.65.169.216	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.166.84.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.183.61.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
95.86.117.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
85.250.46.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
71.166.55.57	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.29.202.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.146.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.22.130.53	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
37.201.194.186	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
86.108.25.96	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
37.247.36.86	Netherlands	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	3
98.14.101.225	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.172.88.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
38.111.147.86	United States	147.237.0.34	tikshuv.idf.il		drop	drop	2
80.179.96.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
149.78.235.223	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.68.214.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
185.32.177.35	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
79.181.136.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.116.52.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.176.11.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.69.32.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
185.32.177.35	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
37.142.184.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
94.159.209.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
201.234.230.209	Venezuela	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
5.29.125.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
89.138.95.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
201.234.230.209	Venezuela	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
84.95.22.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.149.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.178.15.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
89.139.162.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
74.6.254.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.68.46.203	Israel	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
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	12
162.243.89.33	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.89.33	Block	9
5.29.184.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
93.173.190.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	6
79.183.202.19	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
173.162.34.45	United States	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
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
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	4
93.173.170.189	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
66.249.73.222	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/	Block	3
37.59.55.128	France	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 37.59.55.128	Block	3
37.59.55.128	France	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 37.59.55.128	Block	3
162.243.198.188	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.198.188	Block	3
213.57.51.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.121.194.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
85.250.233.215	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.138.215.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
213.6.232.200	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.6.232.200	Block	2
82.80.16.90	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
93.173.170.189	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 93.173.170.189	Block	2
213.6.232.200	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/undefined	Block	2
84.94.62.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
37.59.55.128	France	147.237.72.166	aka.idf.il	Illegal HTTP Version + encodeURI(url) + ' HTTP/1.1	Block	1
192.111.149.138	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
66.249.81.245	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/894-he/himush.aspx	Block	1
46.19.85.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
85.65.229.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
188.138.17.205	France	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
79.177.29.100	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/default.stm	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.241.92	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sitemap.aspx	Block	1
84.108.67.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
162.243.89.33	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.93.146	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.himush.atal.idf.il//894-he/himush.aspx	Block	1
66.249.73.230	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//mobile/	Block	1
31.168.195.70	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	1
79.183.202.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//newsite/english/main.stm	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³×ŸÂ¿Â½	Block	1
66.249.65.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
84.111.158.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Malformed URL	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
95.173.171.236	Turkey	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
66.249.73.238	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//mobile/	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-24-2015-15:03:09 to 04-24-2015-16:03:09