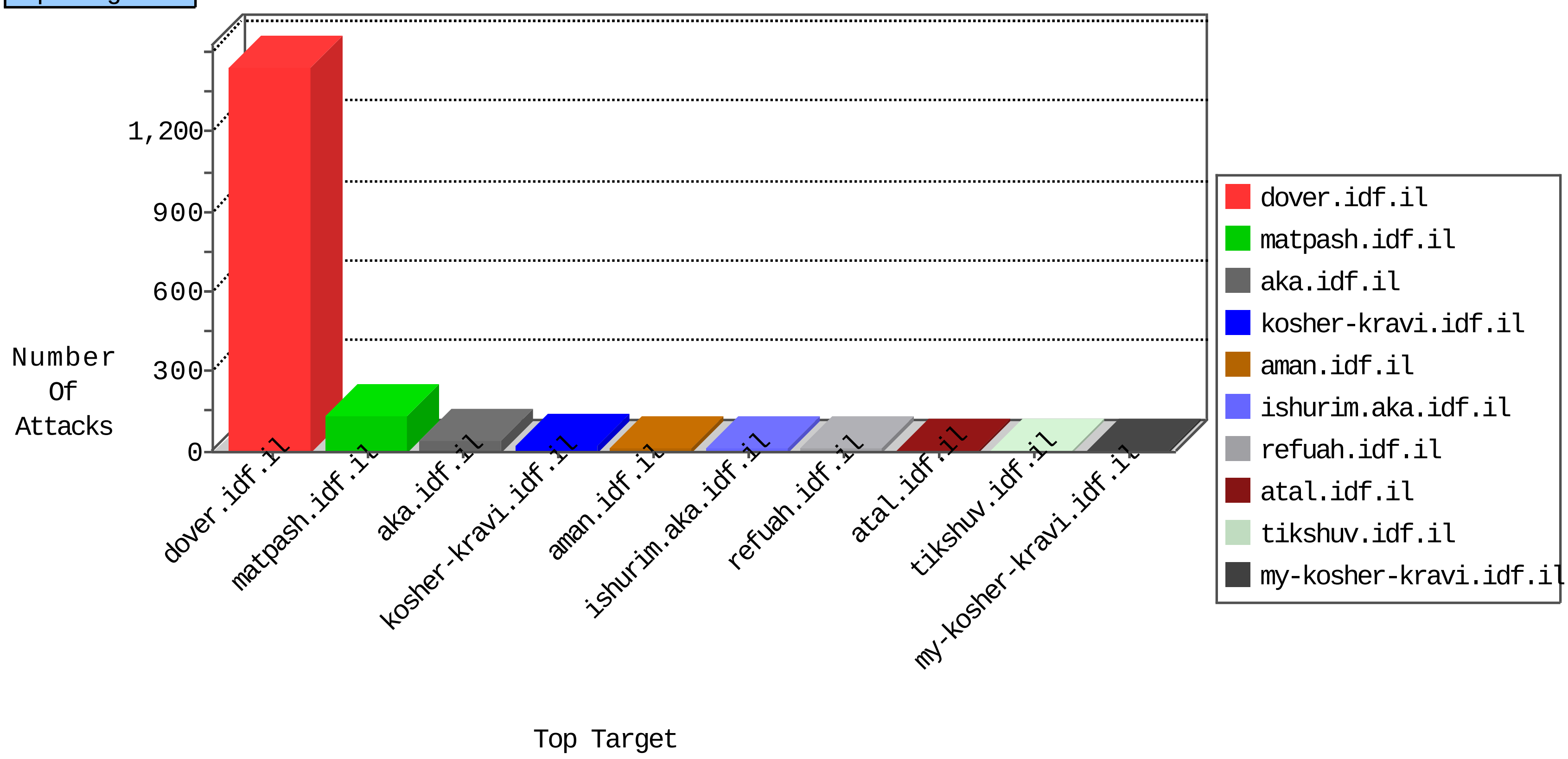
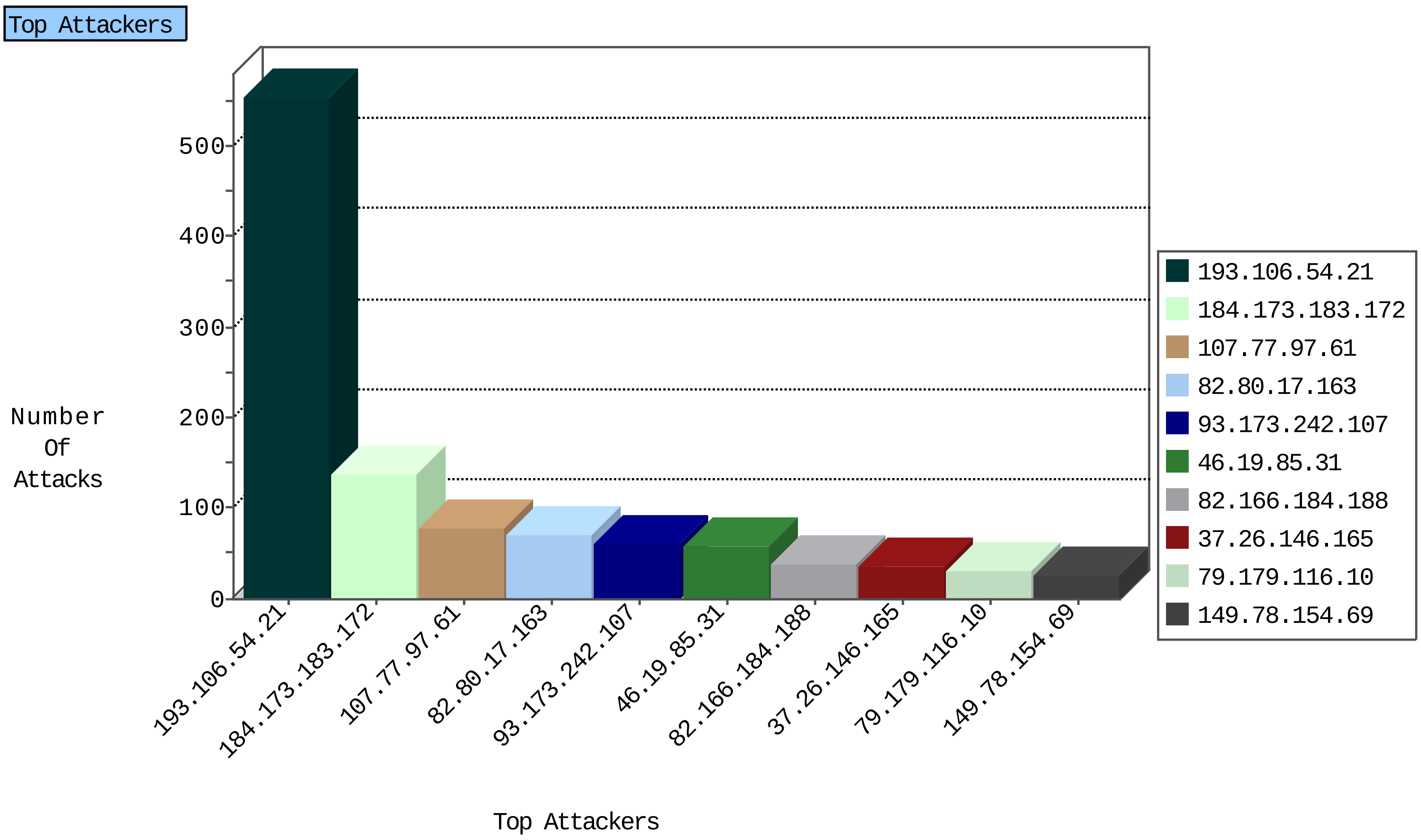
05-08-2015-09:03:07 to 05-08-2015-10:03:07

IDF Under Attack
05-08-2015-09:03:07

Top Targets



Top Attackers



05-08-2015-09:03:07 to 05-08-2015-10:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.109.165.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
124.232.142.220	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

05-08-2015-09:03:07 to 05-08-2015-10:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	138
84.109.81.212	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.201	e.atal.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
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.46	e.chinuch.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
85.25.43.94	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.76.177	ncore.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
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	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	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1

05-08-2015-09:03:07 to 05-08-2015-10:03:07

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
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
178.19.107.114	Poland	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.179.237.197	Poland	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
60.169.78.79	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
180.149.98.78	Mongolia	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
93.179.237.197	Poland	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
93.179.237.197	Poland	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
60.169.78.79	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
183.247.165.129	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1

05-08-2015-09:03:07 to 05-08-2015-10:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
193.106.54.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	555
107.77.97.61	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	78
93.173.242.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
46.19.85.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
82.166.184.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
37.26.146.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
82.80.17.163	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	32
79.179.116.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
68.180.228.224	United States	147.237.0.15	kosher-kravi.idf.il	SAM rule	drop	drop	21
82.80.17.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
5.22.130.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
82.80.17.163	Israel	147.237.77.216	dover.idf.il		drop	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
79.177.16.85	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
216.223.27.25	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
81.218.251.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
87.69.170.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.135	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
173.252.112.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
87.69.119.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
149.78.199.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
173.252.112.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
173.252.112.118	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
119.73.253.6	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
174.69.144.181	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
128.139.197.114	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
85.130.240.165	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
85.65.211.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.26.146.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
82.166.249.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
188.120.132.56	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
46.116.135.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
72.234.142.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.252.112.114	United States	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
82.166.20.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
195.10.194.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.126.5.21	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.67.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71861-he/maarachot.aspx	Block	1
176.10.99.208	Switzerland	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
85.250.25.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
198.12.152.27	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.113.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl50.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.67.78	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ie-index.stm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20277-he/kkkkkkk=8bb86253kkkkkkk_8bb86253	Block	1
88.208.252.224	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//scriptresource.axd	Block	1
207.46.13.137	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.243	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.144.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
180.76.6.45	China	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.192.110.162	Spain	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13780-he/dover.aspx	Block	1
208.97.177.187	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8736-he/atal.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/010.stm	Block	1
79.182.209.178	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
66.249.67.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1097-he/refuah.aspx	Block	1
193.46.84.114	Lithuania	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13187-he/dover.aspx ×″×ž×—×¤×¨×•×Ÿ ×″×—×“×©	Block	1
95.86.73.228	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/hasata/hasata.stm	Block	1
212.68.153.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.67.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
173.236.184.107	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1

05-08-2015-09:03:07 to 05-08-2015-10:03:07