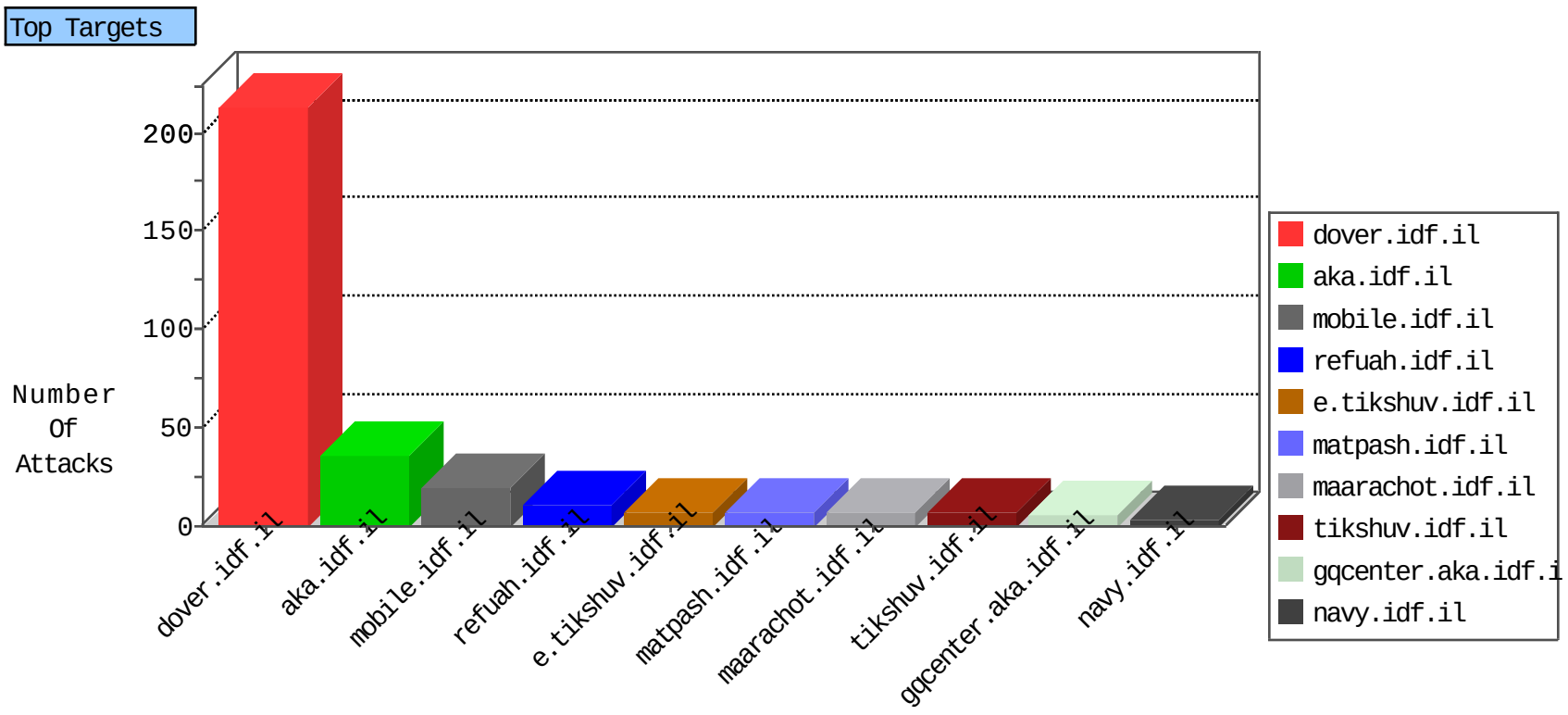
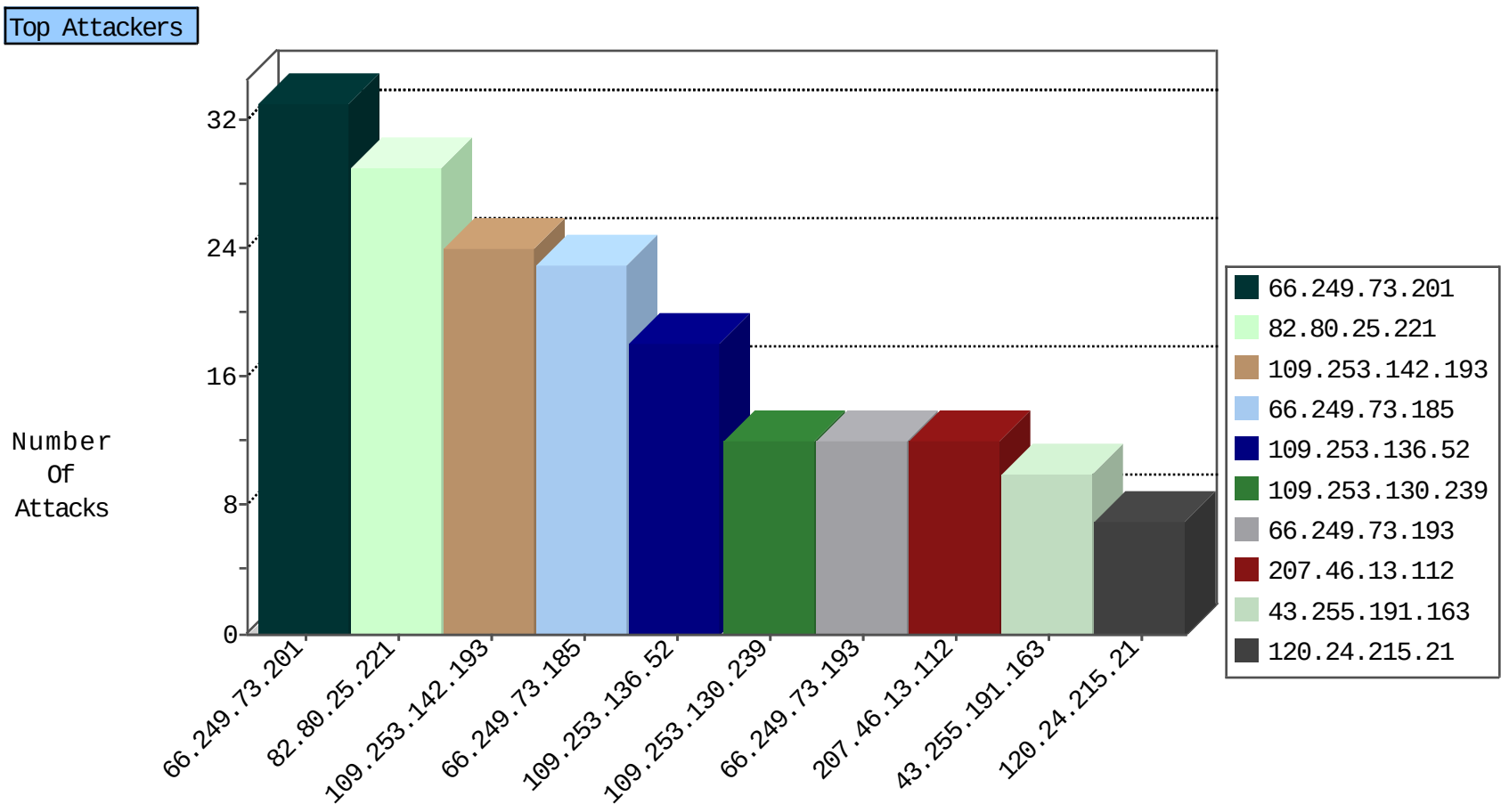
03-28-2015-11:03:07 to 03-28-2015-12:03:07

IDF Under Attack
03-28-2015-11:03:07

Top Targets



Top Attackers



03-28-2015-11:03:07 to 03-28-2015-12:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-28-2015-11:03:07 to 03-28-2015-12:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
52.0.4.72	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
77.127.220.98	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
87.69.246.162	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
46.19.85.236	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1

03-28-2015-11:03:07 to 03-28-2015-12:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
37.26.146.231	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
120.24.215.21	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
212.147.56.190	Switzerland	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	Cote D'Ivoire	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.67	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	Cote D'Ivoire	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

03-28-2015-11:03:07 to 03-28-2015-12:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.142.193	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
109.253.130.239	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
37.247.36.102	Netherlands	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	5
199.30.25.210	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.150.220	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
185.32.179.98	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
5.28.185.140	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.236	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
87.69.246.162	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
87.69.246.162	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.134	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
176.12.137.240	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.115	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
77.237.154.221	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
176.12.139.168	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.159	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.200	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.84	United States	147.237.76.148	gqcenter.aka.idf.il		drop	drop	1
109.163.234.4	Romania	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
192.116.128.90	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
78.108.63.44	Sweden	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
173.208.203.138	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
46.19.85.192	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.179	United States	147.237.0.35	akaws.idf.il		drop	drop	1
37.237.208.90	Iraq	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.47	United States	147.237.0.35	akaws.idf.il		drop	drop	1
212.179.61.122	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
85.64.216.111	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.147.98	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.201	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.101	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.86	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.108.236.251	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
176.12.137.74	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.180	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
37.237.208.90	Iraq	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.48	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
176.12.147.98	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
149.78.196.165	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.170	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.108.236.251	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.137.74	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.138.83.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined	Block	4
66.249.73.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	3
66.249.69.42	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	3
80.178.251.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	3
185.26.182.25	Europe	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
185.13.250.59	Ukraine	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 185.13.250.59	Block	2
79.181.161.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	2
46.19.86.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
185.13.250.59	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.13.250.59	Block	2
77.127.107.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	2
185.13.250.59	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/	Block	1
66.249.69.50	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.50	Block	1
5.29.237.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
103.28.37.61	Vietnam	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
80.246.133.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jenin/site/english/main	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=5c42c606kkkkkkk_5c42c606	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
87.68.60.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/trajector/	Block	1
78.46.92.68	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.69.50	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 11	Block	1
37.26.147.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.138.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.138.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.34	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/french/facts.stm	Block	1
185.13.250.59	Ukraine	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
87.68.61.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
78.108.63.44	Sweden	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
186.202.153.185	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.73.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133	Block	1
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an..	Block	1
84.109.4.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
212.143.119.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.69.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 12	Block	1
173.208.203.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/readme.asp	Block	1
84.111.112.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
74.208.16.113	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
2.54.185.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.230.204.77	Poland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
66.249.73.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/january/27.stm	Block	1
198.50.206.236	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
46.28.105.84	Czech Republic	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
178.248.250.125	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
85.250.15.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1