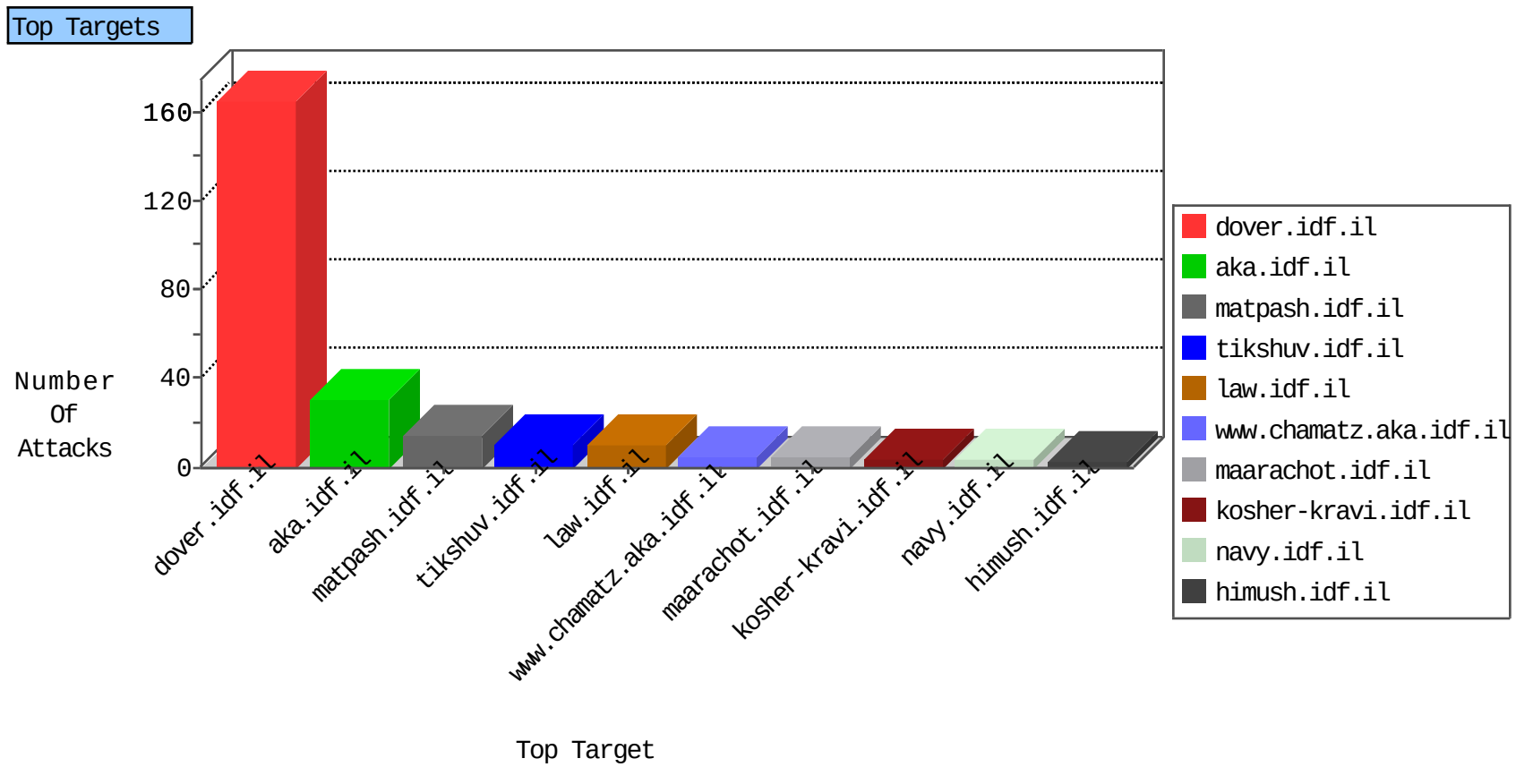
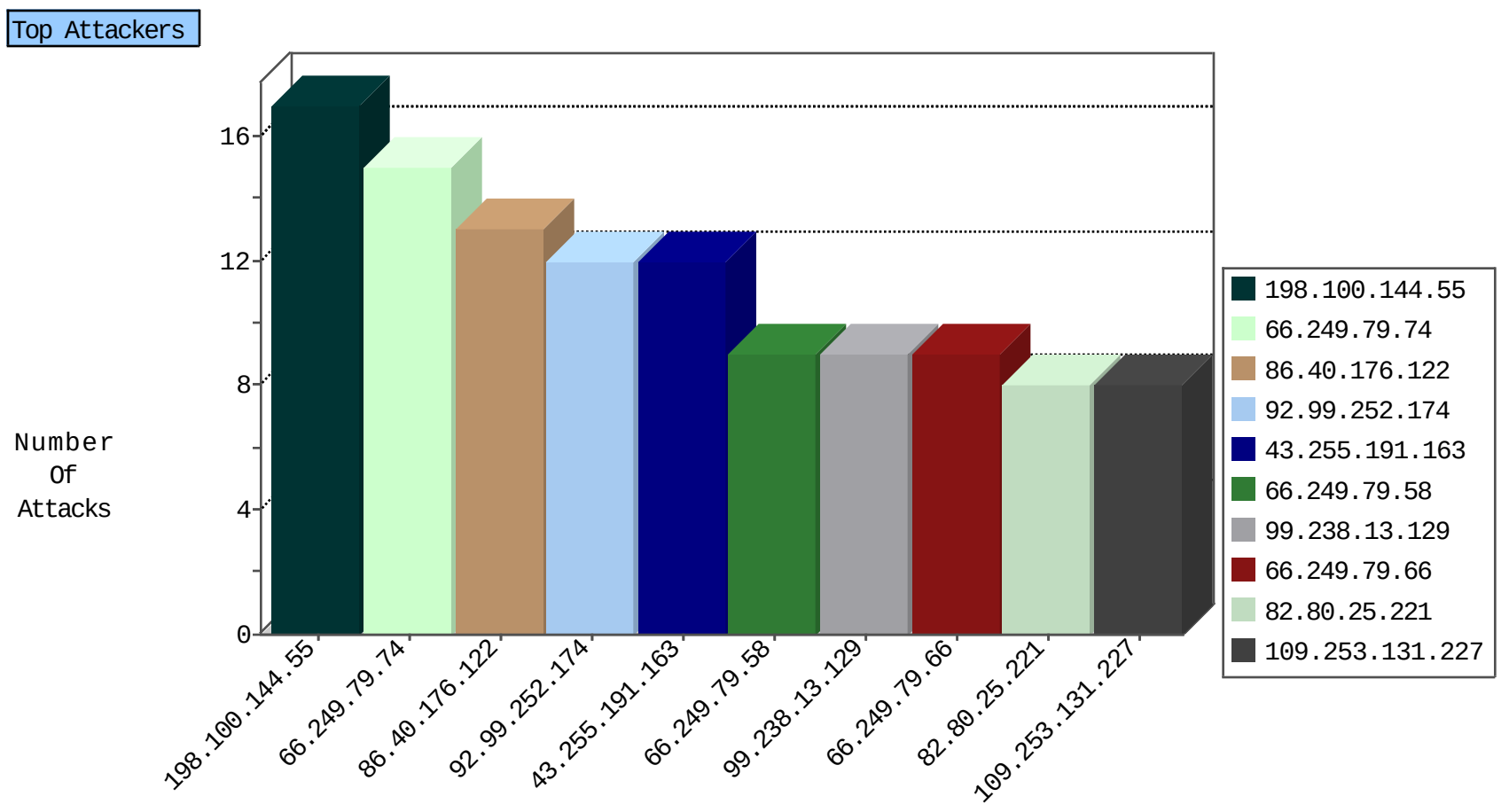
03-27-2015-03:03:02 to 03-27-2015-04:03:02

IDF Under Attack
03-27-2015-03:03:02

Top Targets



Top Attackers



03-27-2015-03:03:02 to 03-27-2015-04:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
86.40.176.122	Ireland	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	13
92.99.252.174	United Arab Emirates	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	12
99.238.13.129	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	9
66.55.134.214	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
202.166.201.237	Nepal	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
157.55.39.137	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	4
188.29.165.220	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
73.47.16.127	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
157.55.39.227	United States	147.237.0.34	tikshuv.idf.il	unblock-sp-traf1	forward	2
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.73.140	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
199.30.24.75	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
188.165.15.148	France	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
73.199.113.21	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	unblock-sp-traf1	forward	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
162.212.1.172	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
157.55.39.102	United States	147.237.77.170	maarachot.idf.il	unblock-sp-traf1	forward	1
209.105.181.239	United States	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	1
202.166.201.237	Nepal	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
209.105.181.239	United States	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	1
202.166.201.237	Nepal	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	unblock-sp-traf1	forward	1
5.255.253.99	Russian Federation	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	1
217.69.133.222	Russian Federation	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
162.212.1.172	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
157.55.39.125	United States	147.237.77.170	maarachot.idf.il	unblock-sp-traf1	forward	1
212.106.95.176	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
205.203.135.1	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
66.249.81.206	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
66.249.67.1	United States	147.237.0.15	kosher-kravi.idf.il	unblock-sp-traf1	forward	1
162.212.1.172	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
37.140.141.6	Russian Federation	147.237.0.34	tikshuv.idf.il	unblock-sp-traf1	forward	1
73.132.127.42	United States	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
199.217.118.79	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
66.249.73.244	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
173.252.74.119	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
5.199.130.188	Germany	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	1
216.154.103.192	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
67.167.69.94	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
66.249.67.9	United States	147.237.0.15	kosher-kravi.idf.il	unblock-sp-traf1	forward	1
190.42.252.111	Peru	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
162.212.1.172	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

03-27-2015-03:03:02 to 03-27-2015-04:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
99.237.226.211	Canada	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.250.140.60	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
46.120.83.232	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.179.17.129	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
99.237.226.211	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-27-2015-03:03:02 to 03-27-2015-04:03:02

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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.163	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
125.16.240.130	India	147.237.72.14	dover.idf.il(old)	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
91.238.134.92	Poland	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
82.165.143.210	Germany	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
211.154.83.77	China	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.67	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
27.50.132.61	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
208.124.237.146	Canada	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	ET DROP Dshield Block Listed Source	1
43.255.191.163	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
91.123.201.179	Sweden	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
211.154.83.77	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
27.50.132.61	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
211.154.83.77	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
208.124.237.146	Canada	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1

03-27-2015-03:03:02 to 03-27-2015-04:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
198.100.144.55	Canada	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	14
109.253.131.227	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
85.130.226.9	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
85.130.226.9	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
198.100.144.55	Canada	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
77.237.138.51	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
188.138.17.205	France	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
209.105.181.239	United States	147.237.77.74	law.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
2.54.139.114	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
198.100.144.55	Canada	147.237.77.176	matpash.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
94.159.229.188	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
70.39.187.108	Satellite Provide	147.237.77.233	atal.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1

03-27-2015-03:03:02 to 03-27-2015-04:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	3
85.250.140.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
87.69.104.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	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
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	1
52.4.29.226	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=695fbd35kkkkkkk_695fbd35	Block	1
66.249.79.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.72.238.241	Block	1
94.242.252.41	Luxembourg	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/webmaster-msg_google_costs_too_much_money_for_websites_and_too_much_of_your_members_privacy	Block	1
52.4.131.75	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
209.105.181.239	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
180.76.5.77	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
108.30.54.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.67.136	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8870-he/refuah.aspx	Block	1
209.105.181.239	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
188.138.17.205	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
77.237.138.51	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
149.88.90.108	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.58	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
217.69.133.220	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/news	Block	1
188.165.15.22	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1498-he/atal.aspx ÐžÐ± Ñ?Ñ‚Ð¾Ñ Ð¶Ðµ Ð² Ñ?Ð²Ð¾Ð¸Ñ… Ð¸Ñ?Ñ?Ð»ÐµÐ´Ð¾Ð²Ð°Ð½Ð¸ÑÑ… Ð³Ð¾Ð²Ð¾Ñ€Ð¸Ñ‚ Ð±Ñ‹Ð»Ð¸ Ð¾Ð±Ð½Ð°Ñ€ÑƒÐ¶ÐµÐ½Ñ‹ Ð¾Ð³Ñ€Ð¾Ð¼Ð½Ñ‹Ðµ Ð¾Ð±ÑŠÐµÐ¼Ñ‹ Ñ‚Ð°Ñ€Ñ‹Ð¸	Block	1
46.237.207.196	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
198.100.144.55	Canada	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1

03-27-2015-03:03:02 to 03-27-2015-04:03:02