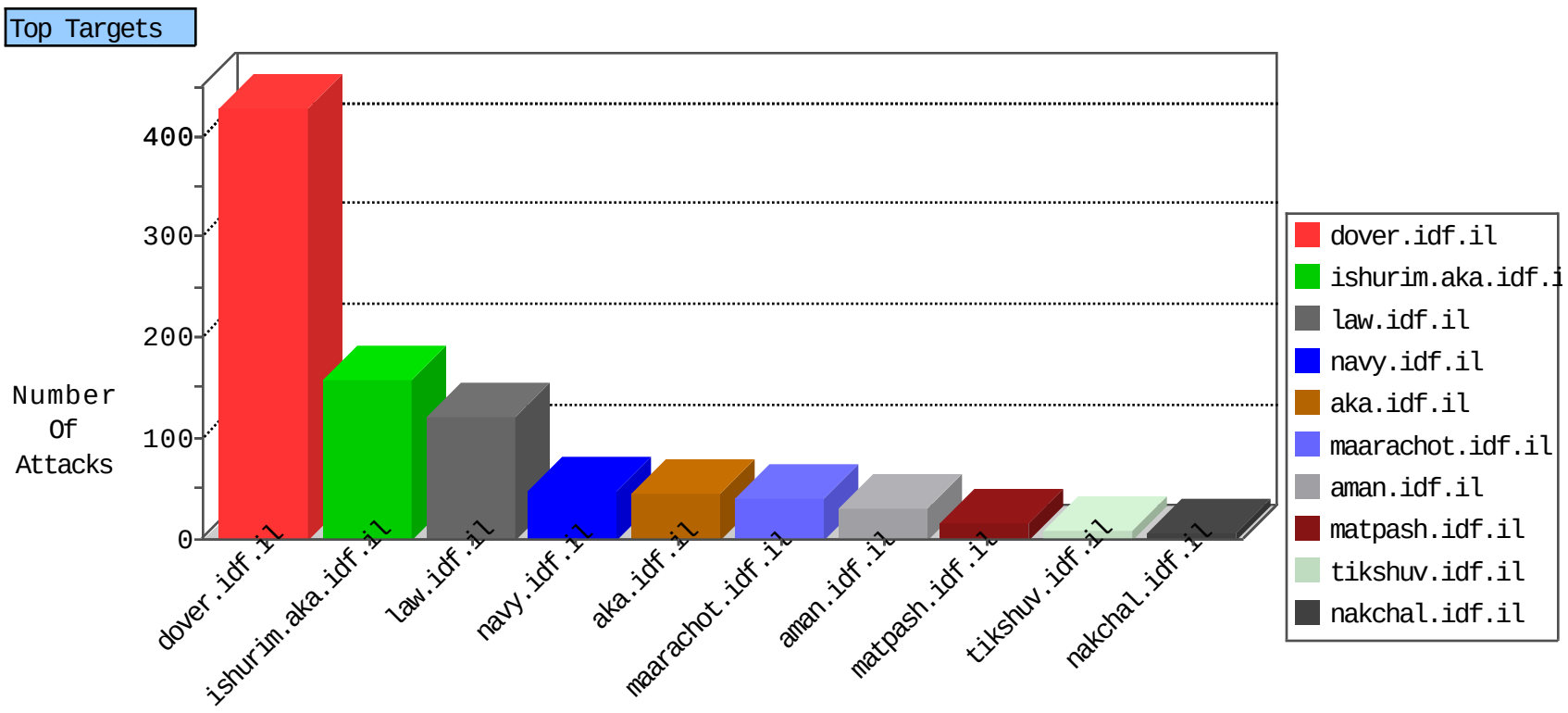
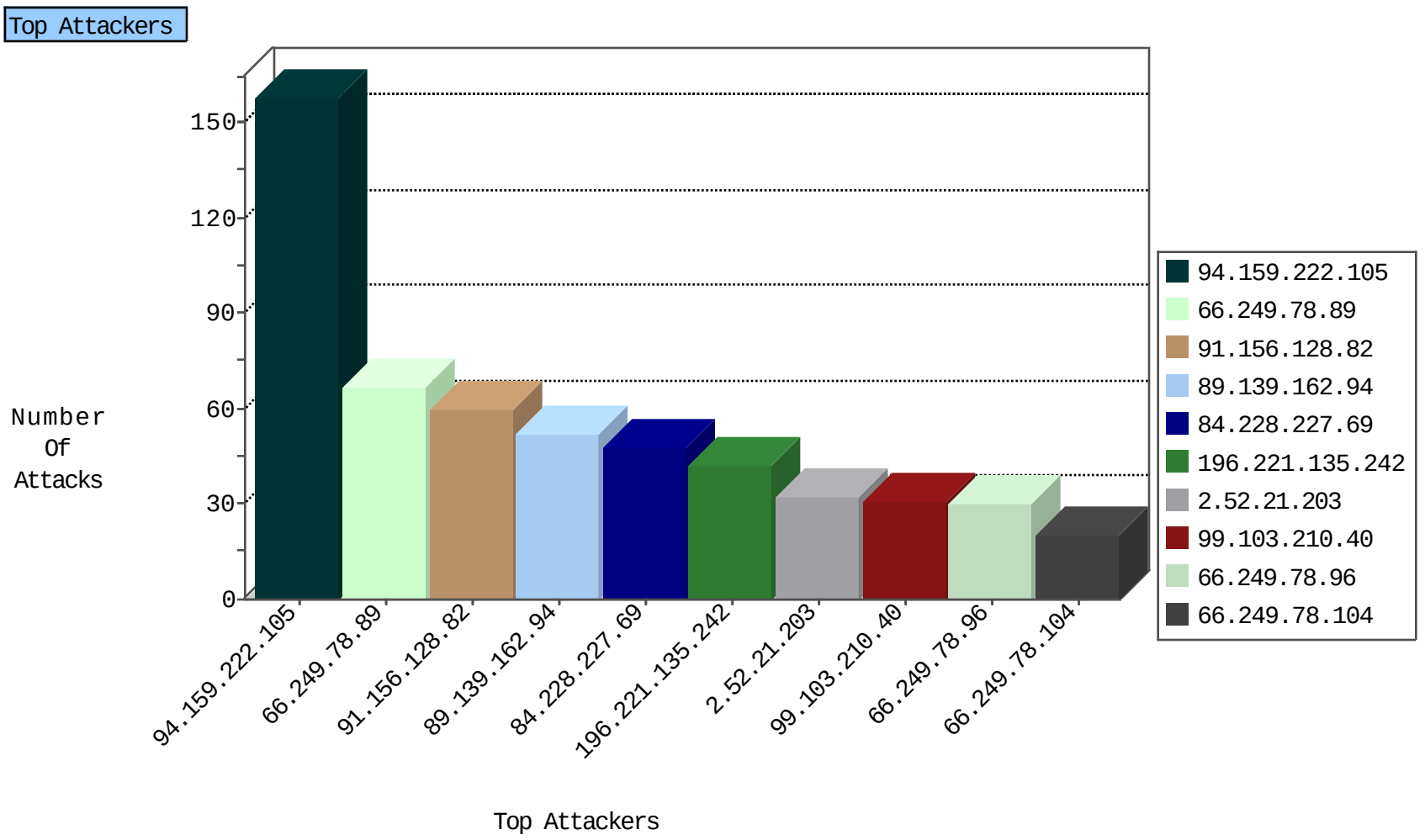
04-27-2015-00:03:03 to 04-27-2015-01:03:03

IDF Under Attack
04-27-2015-00:03:03

Top Targets



Top Attackers



04-27-2015-00:03:03 to 04-27-2015-01:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	11328
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7834
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1941
94.159.222.105	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1769
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1062
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	994
109.64.232.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	965
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	671
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	450
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	56
46.116.118.191	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
82.102.141.248	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	3
82.102.141.248	Israel	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
66.249.78.160	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
79.183.160.175	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	2
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
2.52.32.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.3.202.58	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.148.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
134.196.137.228	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
62.210.244.54	France	147.237.77.226	www.chamatz.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
41.67.84.159	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.3.202.58	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

04-27-2015-00:03:03 to 04-27-2015-01:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	1
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1

04-27-2015-00:03:03 to 04-27-2015-01:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
84.228.227.69	Israel	147.237.76.86	navy.idf.il	GPL SCAN nmap TCP	32
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
81.218.77.162	Israel	147.237.0.34	tikshuv.idf.il	GPL SCAN nmap TCP	2
81.218.77.162	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
66.249.69.85	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
5.29.17.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
1.34.90.227	Taiwan	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.117.197		147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
203.150.228.208	Thailand	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
193.107.17.72	Russian Federation	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
176.100.87.224	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.100.87.224	Russian Federation	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
176.100.87.224	Russian Federation	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
50.7.217.50	Czech Republic	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
157.55.39.247	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
1.93.25.36	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
1.34.90.227	Taiwan	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.117.197		147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
104.167.117.197		147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
193.107.17.72	Russian Federation	147.237.72.14	dover.idf.il(old)	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.100.87.224	Russian Federation	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.100.87.224	Russian Federation	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
176.100.87.224	Russian Federation	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
1.34.90.227	Taiwan	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -f -sS	1

04-27-2015-00:03:03 to 04-27-2015-01:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
91.156.128.82	Finland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
89.139.162.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
196.221.135.242	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
2.52.21.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
77.163.193.92	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.228.227.69	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
84.228.227.69	Israel	147.237.76.86	navy.idf.il	Invalid sequence number	Bad TCP sequence	monitor	8
46.120.42.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
87.68.83.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
89.149.89.209	Moldova, Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
178.62.126.246	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
24.149.94.229	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
77.174.212.143	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.176.17.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
179.158.174.143	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.151.42.39	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.241.198.78	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.193.51.84	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.69.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
67.194.229.137	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.210.178.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.67.84.159	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.67.84.159	Egypt	147.237.77.216	dover.idf.il	Invalid checksum. Packet dropped.	Streaming Engine: TCP Invalid Checksum	drop	3
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
62.210.75.243	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.183.31.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.68.46.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
197.134.127.209	Egypt	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
109.253.130.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.60.145.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.189.50.213	Cote D'Ivoire	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	1
192.114.91.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
173.252.74.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.65.119.27	Israel	147.237.77.216	dover.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
99.103.210.40	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	26
80.179.22.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
99.103.210.40	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/maslul.aspx?catid=61166&docid=73982&usg=alkjrhgfjw7t88xep0zdxf3jdx0hgomwkq	Block	5
176.12.137.182	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/links/links.aspx	Block	3
37.142.139.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
149.78.199.236	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
66.249.69.69	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.69.69	Block	2
86.164.123.216	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/merkava3-p	Block	2
88.198.48.46	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	2
105.235.130.130	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
91.200.12.74	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11845-en/dover.aspx/trackback/	Block	1
2.54.60.0	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-20309-he/dover.aspx	Block	1
105.235.130.130	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login-php	Block	1
37.26.147.236	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers from 37.26.147.236	Block	1
82.102.136.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19374-he/kkkkkkk=273876f7kkkkkkk_273876f7	Block	1
46.121.89.211	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.65.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
5.29.17.124	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/	Block	1
66.249.78.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.138.70	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//templates/links/links.aspx	Block	1
109.207.193.249	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/russian/0511.stm	Block	1
66.249.78.96	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
180.76.4.101	China	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
66.249.64.91	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.199.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1222-2.stm	Block	1
176.12.147.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.69.85	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.69.85	Block	1
37.142.252.68	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
157.55.39.244	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176//	Block	1
66.249.67.84	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/935	Block	1
5.255.253.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
79.177.174.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
176.12.148.149	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.85	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/mobile/	Block	1
46.19.86.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
149.88.69.234	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
89.138.193.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/913-3933-he/patzar.aspx	Block	1
176.12.136.51	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//templates/links/links.aspx	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
37.26.147.236	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers Referer	Block	1
176.12.150.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-27-2015-00:03:03 to 04-27-2015-01:03:03