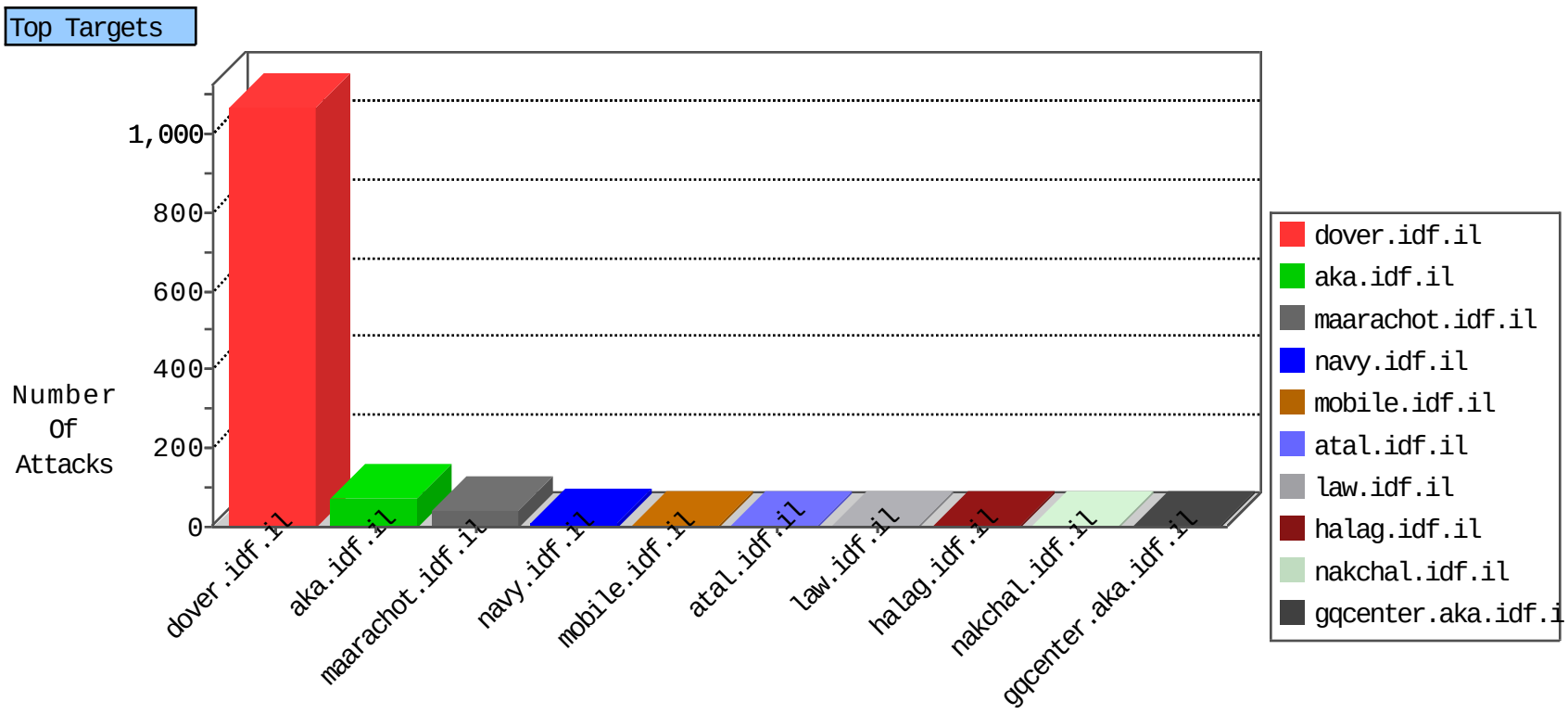
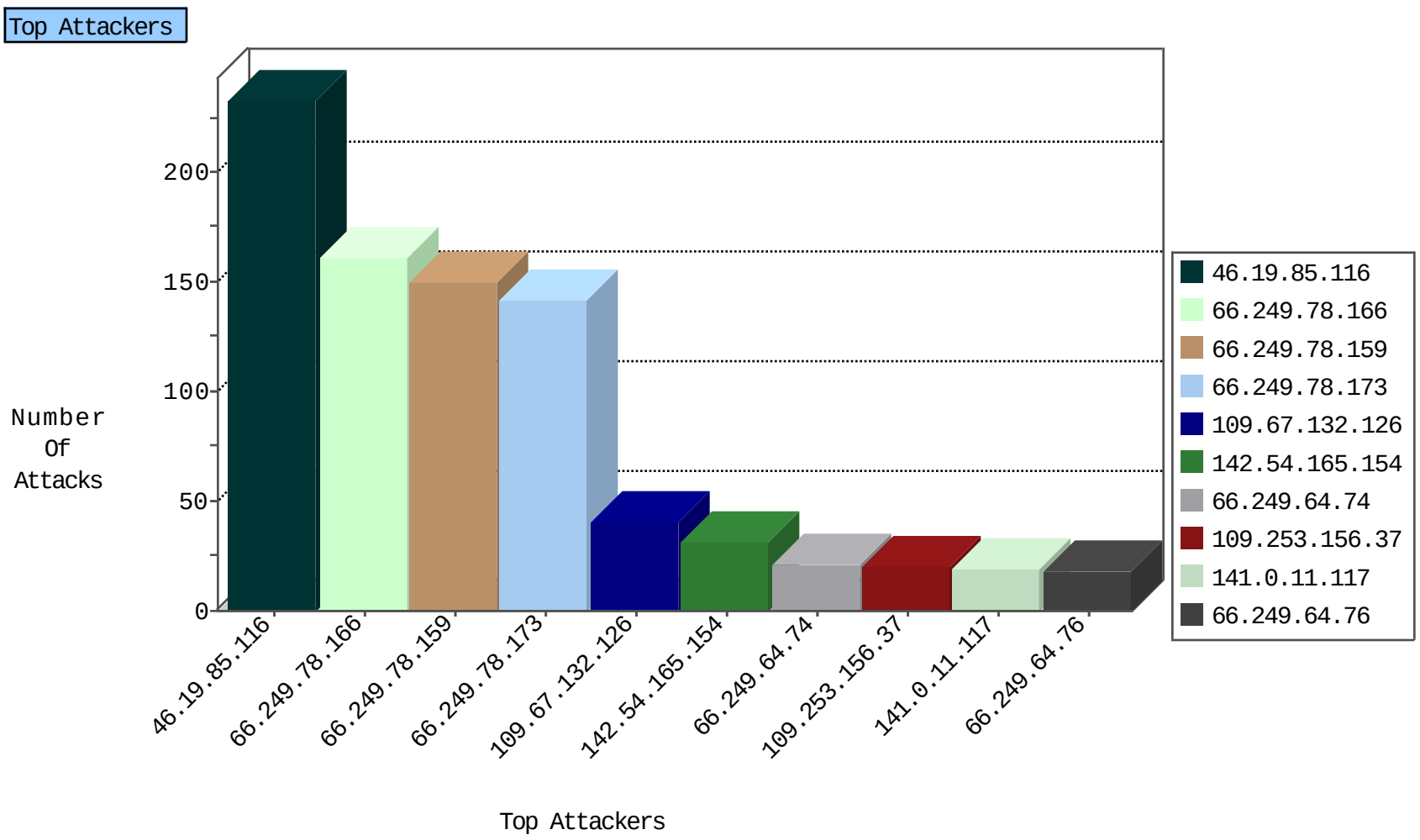
05-01-2015-06:03:05 to 05-01-2015-07:03:05

IDF Under Attack
05-01-2015-06:03:05

Top Targets



Top Attackers



05-01-2015-06:03:05 to 05-01-2015-07:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.66	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3802
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
183.61.165.209	China	147.237.77.19	law-forum.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
87.68.11.45	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

05-01-2015-06:03:05 to 05-01-2015-07:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.46.39.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.234	halag.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
66.240.236.119	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.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
66.240.236.119	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1

05-01-2015-06:03:05 to 05-01-2015-07:03:05

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
122.154.130.180	Thailand	147.237.76.86	navy.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
122.154.130.180	Thailand	147.237.76.86	navy.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie	3
66.249.64.64	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.160.224.128	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
119.93.1.73	Philippines	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
119.90.139.77	China	147.237.77.234	halag.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 4096	1
91.224.132.118	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
61.160.224.128	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
58.20.54.249	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.139.77	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
117.135.163.104	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.20		147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

05-01-2015-06:03:05 to 05-01-2015-07:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
109.67.132.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
109.253.156.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
141.0.11.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.75.13	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
185.46.212.71	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.136.80	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
87.68.11.45	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
87.68.11.45	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
220.255.1.145	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.3	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.176	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.66.33.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.253.133.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.103	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.116.134.101	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	3
79.182.3.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
2.135.75.120	Kazakstan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
84.108.138.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.160.248.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.25.121.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
220.255.1.162	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.68.11.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
220.255.1.128	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.177.109.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	86
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	70
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	56
142.54.165.154	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 142.54.165.154	Block	27
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	27
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	8
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	6
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	4
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	4
182.39.198.86	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	4
142.54.165.154	United States	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 142.54.165.154	Block	3
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.10.104.227	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.10.104.227	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
78.47.67.232	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
94.153.9.66	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.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
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19653-he/dover.aspx	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.108.39.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
185.53.44.80		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
180.76.4.28	China	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
185.53.44.125		147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
122.154.130.180	Thailand	147.237.76.86	navy.idf.il	Access to: /cgi-sys/entropysearch.cgi	Block	1
46.116.134.101	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
185.53.44.61		147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/faq/	None	1
77.125.213.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19771-he/idfgdover.aspx	Block	1
176.10.104.227	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.100.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.53.44.85		147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/chinuch/kurs/	None	1
2.135.75.120	Kazakstan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
185.53.44.138		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eurl.axd/c34fd35da7f0e9459e6c17c560f3e2fd/	Block	1
122.154.130.180	Thailand	147.237.76.86	navy.idf.il	Multiple URL worm attacks from 122.154.130.180	Block	1
66.220.146.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//qr/	Block	1
185.53.44.63		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
176.12.146.165	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
87.68.241.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1

05-01-2015-06:03:05 to 05-01-2015-07:03:05