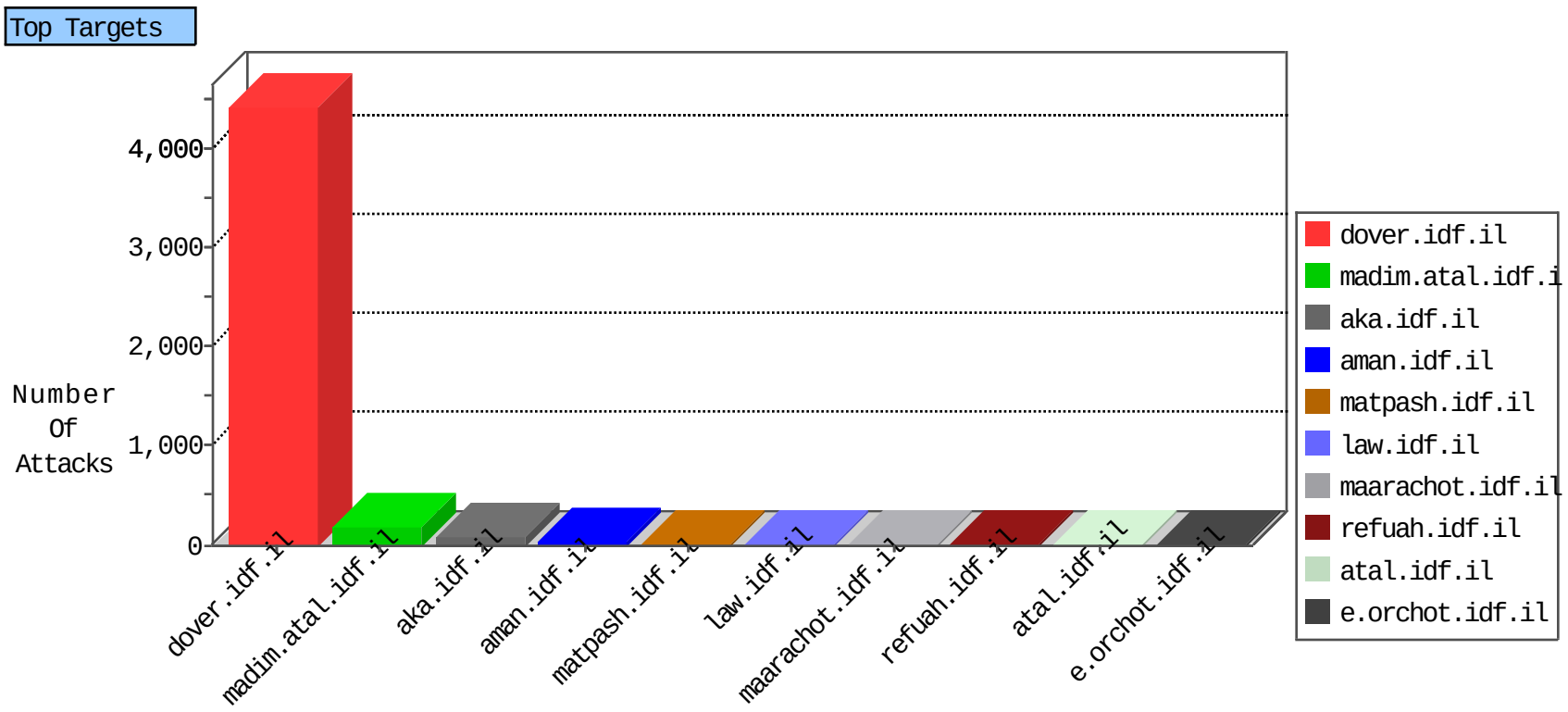
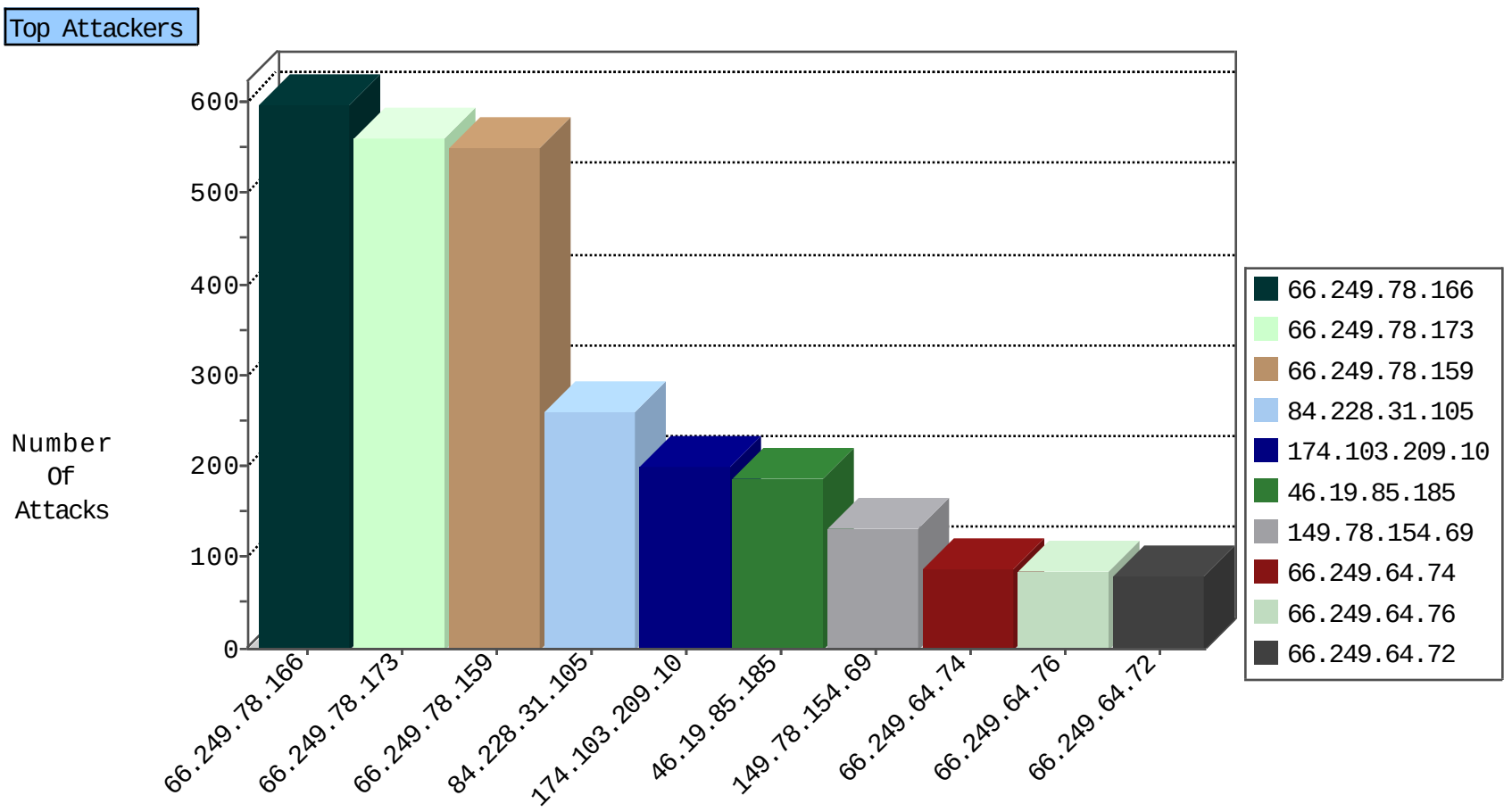
05-01-2015-21:03:01 to 05-01-2015-22:03:01

IDF Under Attack
05-01-2015-21:03:01

Top Targets



Top Attackers



05-01-2015-21:03:01 to 05-01-2015-22:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
37.142.131.93	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	213
220.181.108.107	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	81
173.199.65.20	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.60.77.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
37.142.234.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
104.156.228.198		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.216.57	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

05-01-2015-21:03:01 to 05-01-2015-22:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.202.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	2
68.14.225.28	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.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
93.120.27.62	Romania	147.237.77.170	maarachot.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	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
218.30.103.52	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
85.25.43.94	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
41.176.233.138	Egypt	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1

05-01-2015-21:03:01 to 05-01-2015-22:03:01

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	3
84.228.31.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.190.60	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.186.59.23	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
222.186.59.23	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
218.27.204.27	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
178.32.251.100	France	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.139.71	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.238.134.92	Poland	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.190.60	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.59.23	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.27.204.27	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.90.139.71	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
119.90.139.71	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -f -sS	1

05-01-2015-21:03:01 to 05-01-2015-22:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.228.31.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	260
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	250
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	229
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	215
174.103.209.10	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	199
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	131
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
89.139.13.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	71
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
2.52.37.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
5.29.93.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
213.57.88.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
80.246.133.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
62.219.21.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
109.253.135.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
173.199.65.20	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
188.117.96.99	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
46.120.52.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
176.12.143.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
207.46.13.8	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
84.94.17.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
72.2.103.175	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
104.156.228.198		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
114.113.138.211	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
107.77.83.26	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
70.210.17.155	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
46.19.85.213	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
188.58.106.9	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
157.55.39.47	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
185.23.127.85	Bahrain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
37.26.146.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
5.102.217.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.85.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
213.57.185.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
79.181.124.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	187
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	91
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	87
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	86
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	83
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	81
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	74
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	72
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	68
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	61
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	30
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	18
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	17
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	14
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	13
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	12
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	12
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	10
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 87.69.241.92	Block	8
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
77.126.30.188	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
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.176.8.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.181.57.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	2
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	2
185.53.44.41		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	2
176.12.139.157	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	2
114.121.161.123	Indonesia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.138	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
204.115.190.145	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.66	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	1
185.53.44.126		147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chamatz/klali/	None	1
185.53.44.74		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eurl.axd/85cb72ee4185cb41bf92a8916db47e4d/	Block	1
180.76.4.73	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
212.224.119.139	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/login	Block	1
185.53.44.202		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2000/december/12.stm	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.77.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.53.44.92		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.53.44.92	Block	1
185.53.44.61		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13339-en/dover.aspx forcerecrawl: 0	Block	1
66.249.78.96	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
109.253.143.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

05-01-2015-21:03:01 to 05-01-2015-22:03:01