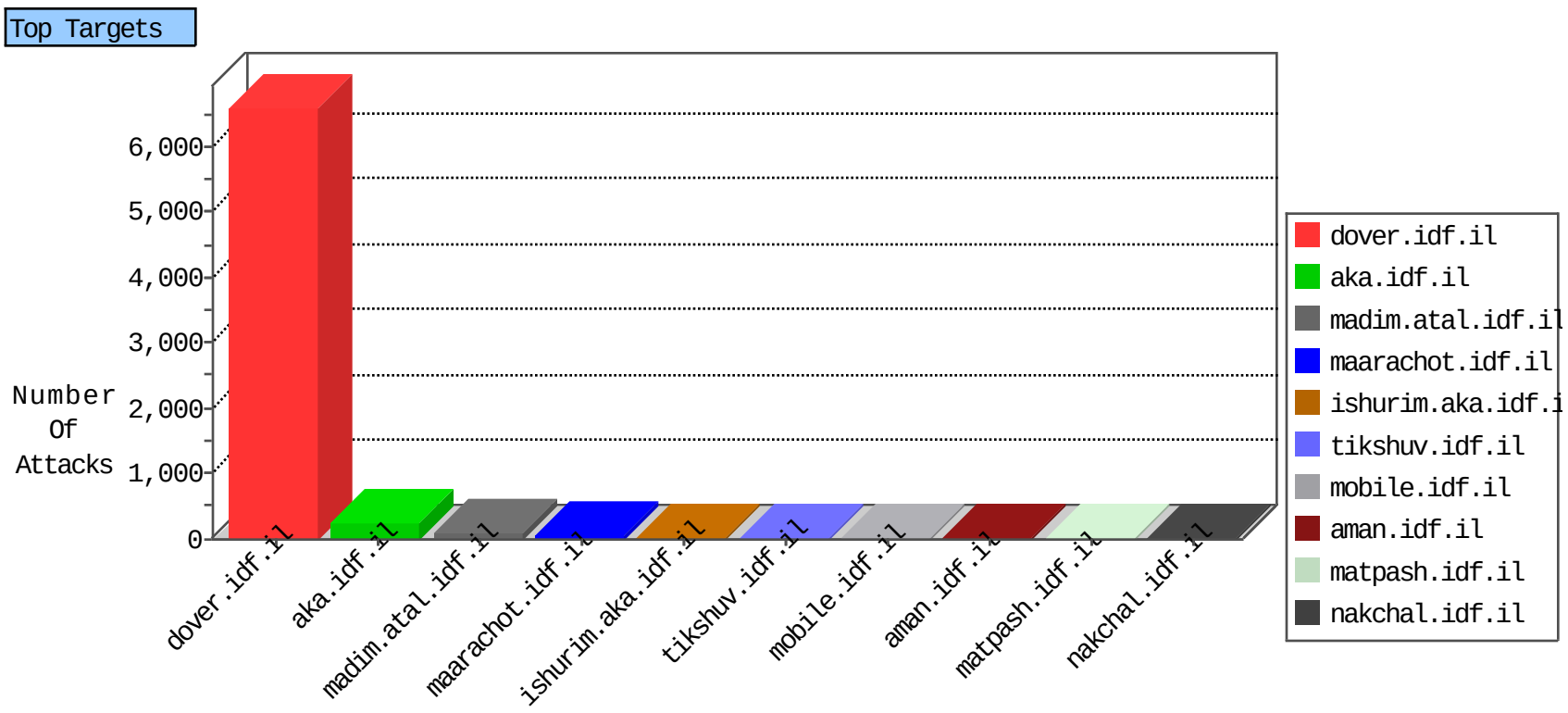
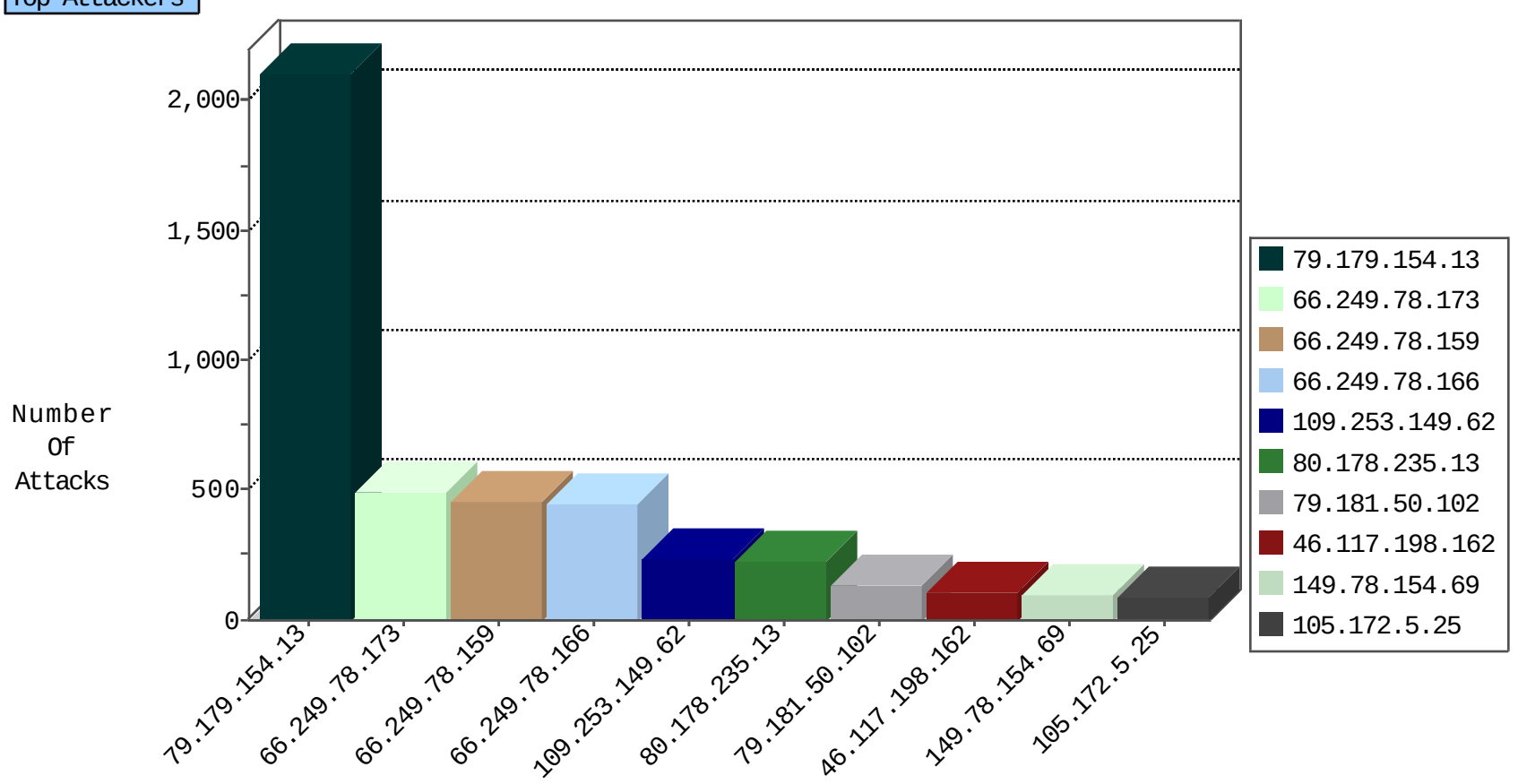
05-01-2015-16:03:06 to 05-01-2015-17:03:06

IDF Under Attack
05-01-2015-16:03:06

Top Targets



Top Attackers



05-01-2015-16:03:06 to 05-01-2015-17:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.182.97.80	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
93.172.190.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
87.68.37.52	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
84.108.111.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	3
192.3.190.242	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
2.52.139.150	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-01-2015-16:03:06 to 05-01-2015-17:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.126.52.173	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
66.240.236.119	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
84.95.58.237	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.217	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
81.167.237.53	Norway	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.220	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.24	e.lifestyle.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	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.68	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.0.34	tikshuv.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
84.111.24.239	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.24	e.lifestyle.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	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.177	ncore.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	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1

05-01-2015-16:03:06 to 05-01-2015-17:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.39	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	74
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	7
109.67.52.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.173.40.83	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.172.207	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.150.163	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.121.136.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.131.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.173.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
193.107.16.206	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
157.55.39.190	United States	147.237.0.34	tikshuv.idf.il	SERVER-IIS asp-dot attempt	1
61.160.224.130	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.217.200.158	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.217.200.158	Korea, Republic of	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
221.229.166.4	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
208.68.232.136	United States	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	Russian Federation	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
178.32.251.100	France	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
112.217.200.158	Korea, Republic of	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.217.200.158	Korea, Republic of	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
209.66.70.253	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
78.95.0.155	United Kingdom	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

05-01-2015-16:03:06 to 05-01-2015-17:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.179.154.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2107
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	364
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	313
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	280
109.253.149.62	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	235
80.178.235.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	228
79.181.50.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	134
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	94
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	88
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	88
105.172.5.25	Angola	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	84
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	84
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	76
212.179.46.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	74
84.228.147.91	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	66
199.85.73.12	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
109.64.157.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
164.138.121.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
84.109.234.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
68.108.160.130	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
79.181.17.117	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
66.249.75.117	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
87.68.210.209	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.75.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
72.55.122.222	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
212.116.177.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
46.19.85.148	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
129.64.200.171	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
46.120.79.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
79.178.133.232	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
5.22.130.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
207.46.13.8	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
84.228.50.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
109.65.174.169	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
2.54.11.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
185.32.177.103	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
84.229.11.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
109.65.177.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
176.12.137.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16

05-01-2015-16:03:06 to 05-01-2015-17:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.117.198.162	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.117.198.162	Block	109
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	12
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	5
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	4
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	3
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	3
207.46.13.78	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.78	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
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	2
5.29.162.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
85.64.164.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
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	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
185.32.177.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.106.190.66	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
31.168.72.173	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
93.173.17.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.53.44.53		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0101-7.stm	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.117	Block	1
185.53.44.91		147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/kamlar/klali/	None	1
79.183.54.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	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_imgtop.asp	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/gallery	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1117-7673-he/nakhal.aspx	Block	1
207.46.13.20	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.20	Block	1
2.54.153.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
82.145.210.173	Europe	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0817-1.stm	Block	1
66.249.64.144	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/15022011masaiyot.aspx	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	1

05-01-2015-16:03:06 to 05-01-2015-17:03:06