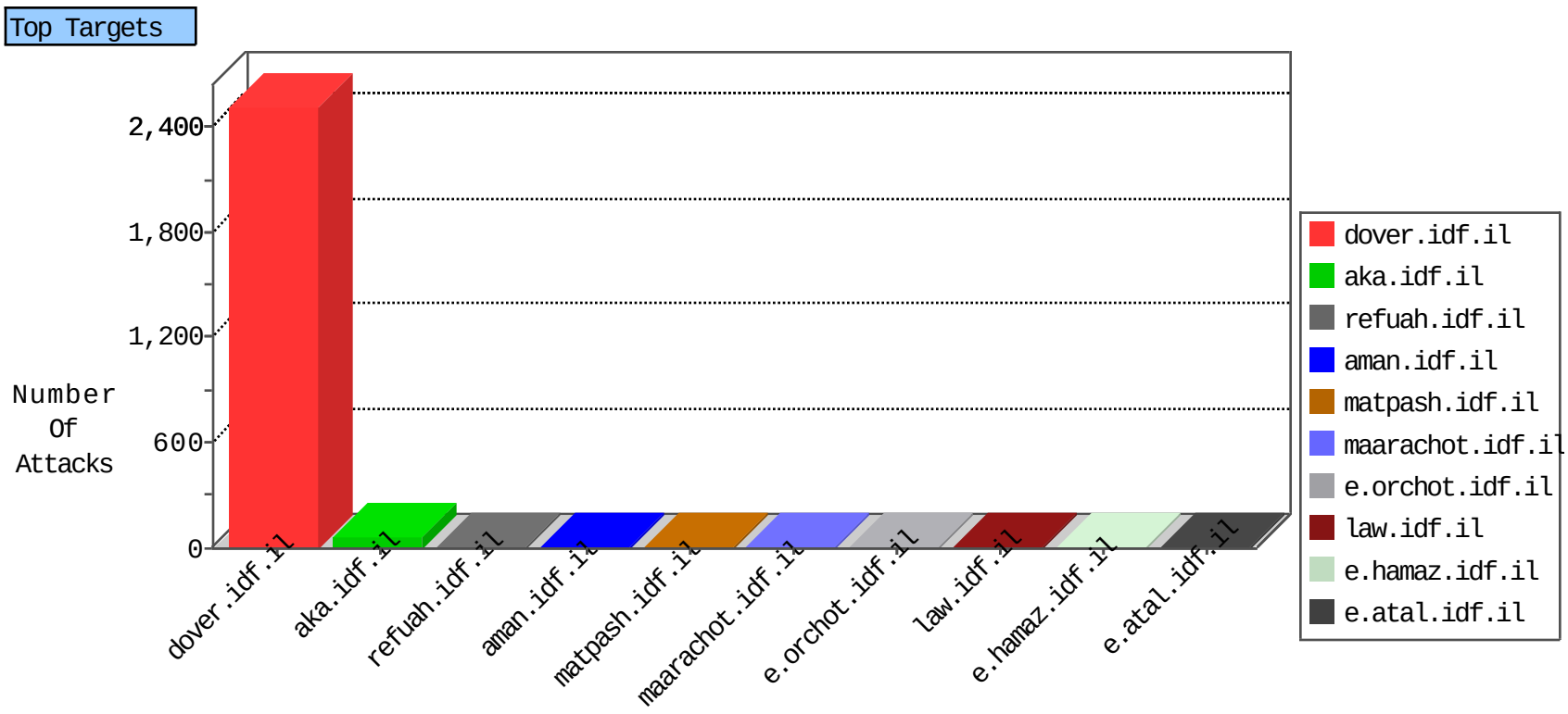
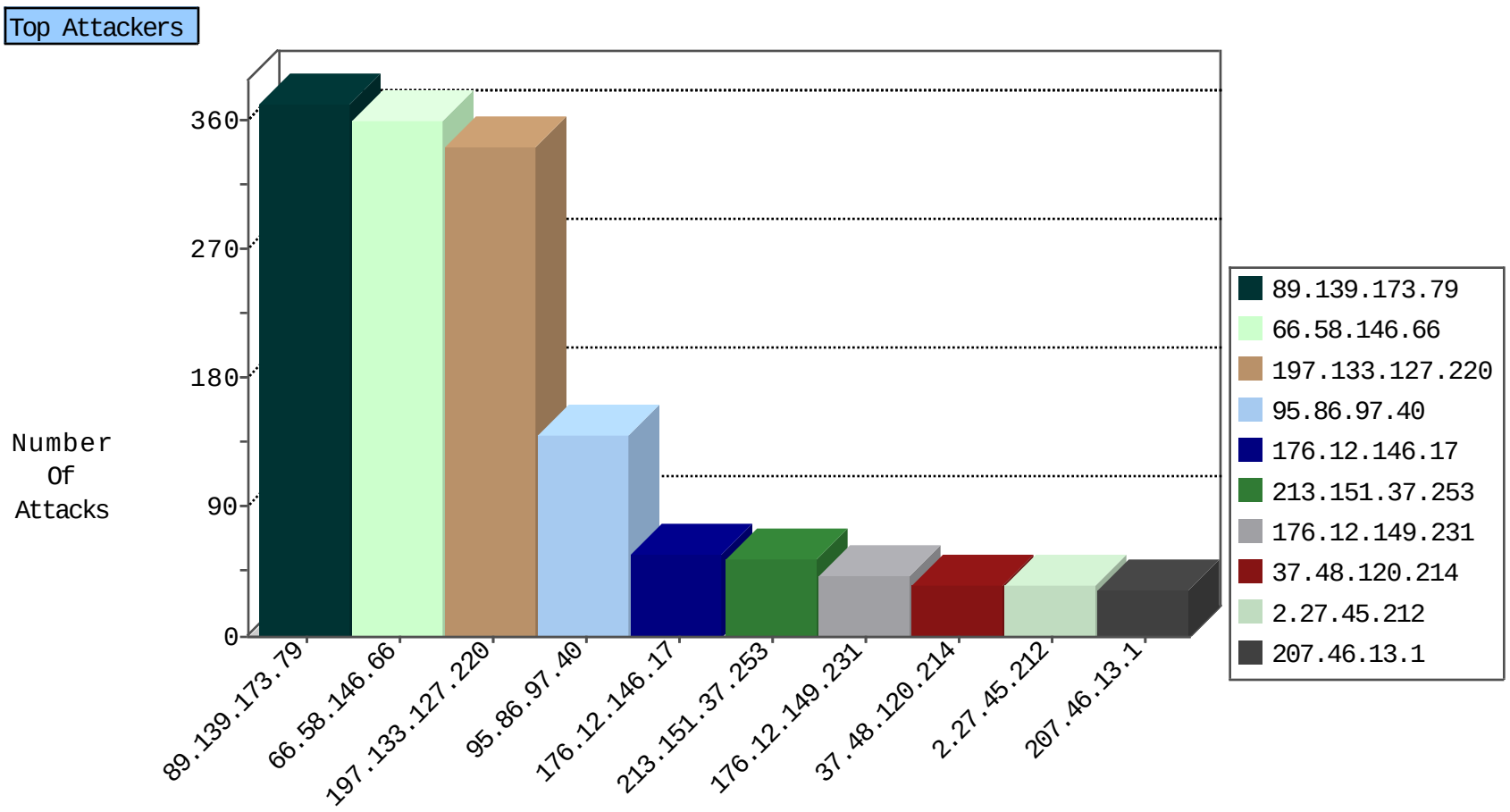
04-20-2015-01:03:02 to 04-20-2015-02:03:02

IDF Under Attack
04-20-2015-01:03:02

Top Targets



Top Attackers



04-20-2015-01:03:02 to 04-20-2015-02:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3015
220.181.108.159	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	235
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	235
5.29.9.82	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	11
85.250.86.28	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
124.232.142.220	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
66.240.236.119	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

04-20-2015-01:03:02 to 04-20-2015-02:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	23
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
41.250.242.245	Morocco	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
94.247.203.205		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.22	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.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
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
74.57.149.154	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.166	aka.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
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1

04-20-2015-01:03:02 to 04-20-2015-02:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
46.19.85.157	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
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
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
94.159.239.183	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
12.139.34.20	United States	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
202.100.219.52	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
198.89.108.125	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 2048	1
117.135.163.104	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
210.14.158.75	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
12.139.34.20	United States	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
202.100.219.52	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
199.255.137.52	United States	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
117.135.163.104	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
12.139.34.20	United States	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
202.100.219.52	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

04-20-2015-01:03:02 to 04-20-2015-02:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.58.146.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	360
89.139.173.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	356
197.133.127.220	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	342
95.86.97.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	140
213.151.37.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
176.12.146.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
176.12.149.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
2.27.45.212	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
109.253.139.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
37.26.147.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
109.67.201.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
212.76.127.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
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
93.173.254.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
87.68.62.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.253.146.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
46.19.86.140	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
176.12.149.44	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.19.85.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
62.252.183.221	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
94.247.203.205		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
207.46.13.1	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
176.12.146.17	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
204.237.22.235	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
172.56.18.202	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.253.140.133	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.151.169	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.137.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
176.12.137.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
37.26.148.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.224.21.23	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
89.139.173.79	Israel	147.237.77.216	dover.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	10
109.64.62.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
95.86.70.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
5.109.170.23	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
85.65.100.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
87.69.79.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.19.85.157	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	8

04-20-2015-01:03:02 to 04-20-2015-02:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	3
149.78.241.86	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
87.68.214.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.48	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	2
79.179.120.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/6day.stm	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
207.46.13.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/netsar.stm	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.5	Block	1
76.4.163.202	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
192.116.98.196	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/present.stm	Block	1
89.139.173.79	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 89.139.173.79	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter docId&pageNum in aka.idf.il/tizmoret/faq/default.asp	None	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.120.54	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.179.120.54	Block	1
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
192.187.115.90	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
46.118.119.63	Ukraine	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
109.67.188.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/351-en/sb_item_lev2	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22716	Block	1
180.76.4.76	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
194.6.232.149	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
54.87.101.216	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
128.173.49.66	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /1133-20973-he/dover.aspx	Block	1
70.167.8.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/trajector/	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
183.15.238.217	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0105-2.stm	Block	1
84.109.188.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.35	Block	1
62.219.133.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.65.12	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1133-en/hamaz.aspx	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born.stm	Block	1

04-20-2015-01:03:02 to 04-20-2015-02:03:02