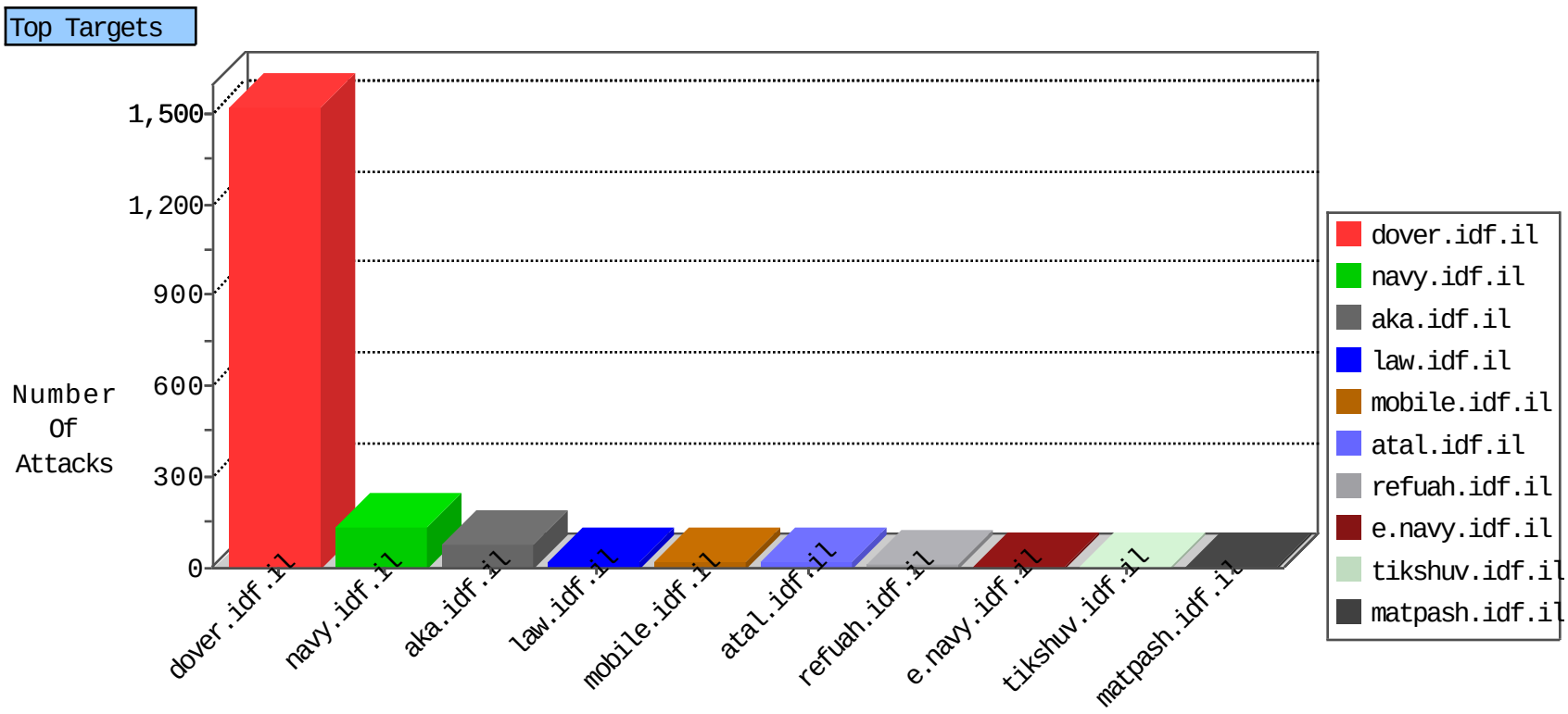
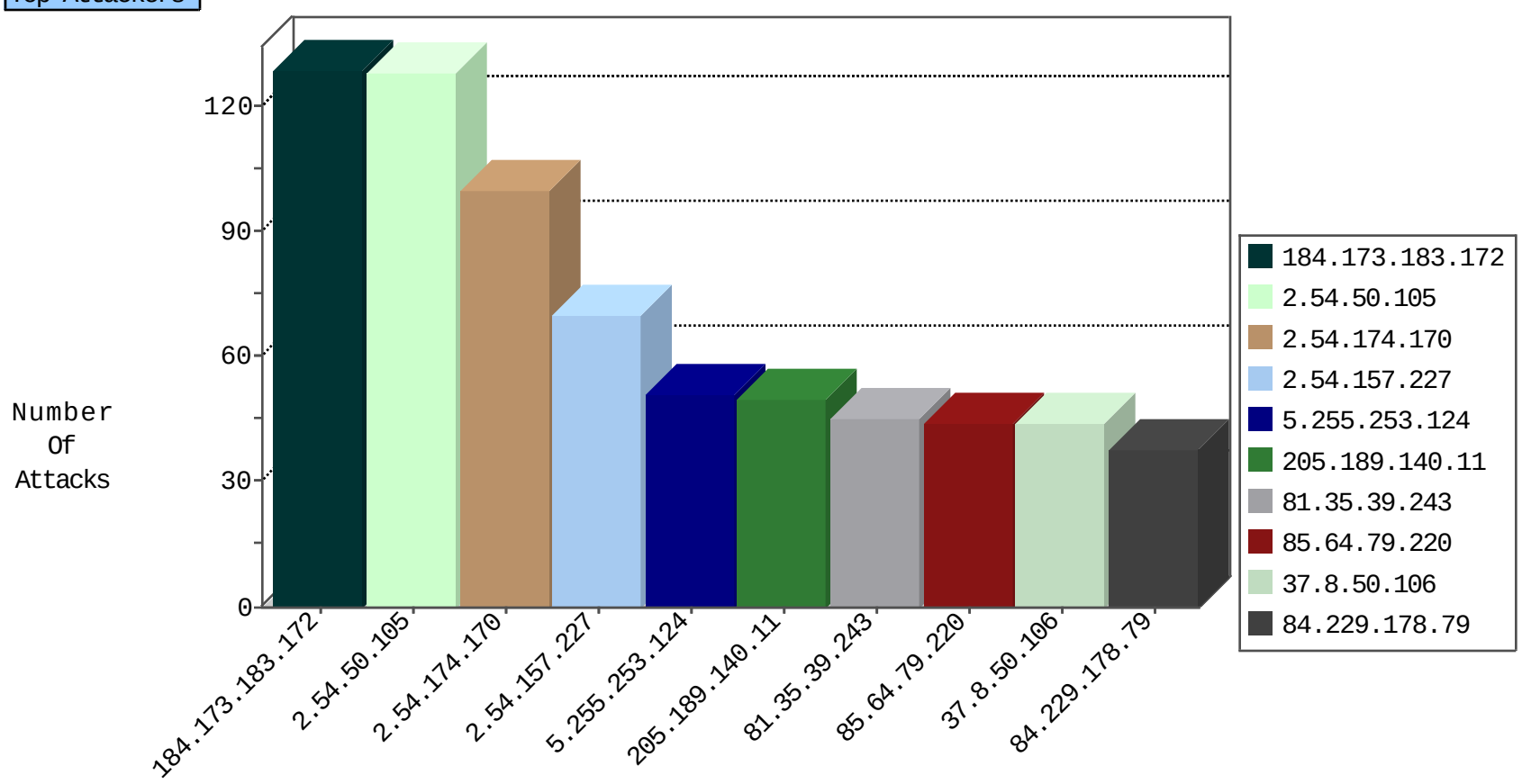
05-08-2015-20:03:02 to 05-08-2015-21:03:02

IDF Under Attack
05-08-2015-20:03:02

Top Targets



Top Attackers



05-08-2015-20:03:02 to 05-08-2015-21:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.159	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4209
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	938
79.164.129.146	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
124.232.142.220	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
31.210.186.131	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
81.111.230.218	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
198.23.132.226	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
111.202.66.66	China	147.237.76.42	refuah.idf.il	L4 Source or Dest Port Zero	drop	1

05-08-2015-20:03:02 to 05-08-2015-21:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	129
85.64.45.216	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.64.45.216	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
77.127.108.219	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.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
71.6.135.131	United States	147.237.76.38	e.e.meitav.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
84.94.223.182	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	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.64.45.216	Israel	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	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.27	e.madim.atal.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
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	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
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1

05-08-2015-20:03:02 to 05-08-2015-21:03:02

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
149.78.174.142	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.0.60	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
123.136.24.60	Bangladesh	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
123.136.24.60	Bangladesh	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
113.176.14.89	Vietnam	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
199.101.186.200	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
104.167.117.197		147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
94.131.14.10	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
188.138.9.51	Germany	147.237.72.217	e.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
144.0.0.60	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.0.60	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
123.136.24.60	Bangladesh	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
123.136.24.60	Bangladesh	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
113.176.14.89	Vietnam	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
218.241.153.80	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 4096	1
104.167.117.197		147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
199.101.186.200	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
104.167.117.197		147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
193.107.16.206	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
144.0.0.60	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1

05-08-2015-20:03:02 to 05-08-2015-21:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.50.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	128
2.54.174.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
2.54.157.227	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	70
205.189.140.11	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
85.64.79.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
37.8.50.106	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
81.35.39.243	Spain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
84.229.178.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
173.164.157.198	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
90.3.172.95	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
84.228.64.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
37.8.69.1	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
77.125.111.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
190.29.181.30	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
185.4.253.18	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
82.205.29.244	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
46.19.85.73	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
46.120.168.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
37.8.37.180	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
197.161.128.202	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
109.66.103.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
77.125.82.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
82.205.19.43	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
117.207.134.222	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
62.219.145.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
93.173.140.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
77.127.108.219	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	11
77.126.175.169	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.65.6.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
2.54.135.232	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	9
2.54.135.232	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
2.54.135.232	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	9
46.116.10.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
216.113.160.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
77.127.176.17	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
93.172.136.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
37.8.37.180	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
84.108.1.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
157.82.156.135	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
84.228.179.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
93.172.38.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
94.230.86.231	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6

05-08-2015-20:03:02 to 05-08-2015-21:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.67.66.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
79.181.183.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
84.228.234.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
190.29.181.30	Colombia	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.69.70	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
149.78.72.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.74.122.85	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1012-2.stm	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-16152-en	Block	1
93.173.140.26	Israel	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/chinuch/contact	Block	1
149.88.148.96	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.133.1	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
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/tizmoret/	None	1
174.129.237.157	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
94.230.92.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
77.127.108.219	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1136-he/atal.aspx	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1367-he/atal.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	1
84.228.80.140	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	Unauthorized URL Access to www.aka.idf.il/miluiml	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
180.76.6.61	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fatah/english/main_index.stm	Block	1
106.120.160.109	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/894-he/cogat.aspx	Block	1
79.179.134.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
157.55.39.124	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.64.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/search.asp	Block	1
85.250.150.73	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1

05-08-2015-20:03:02 to 05-08-2015-21:03:02