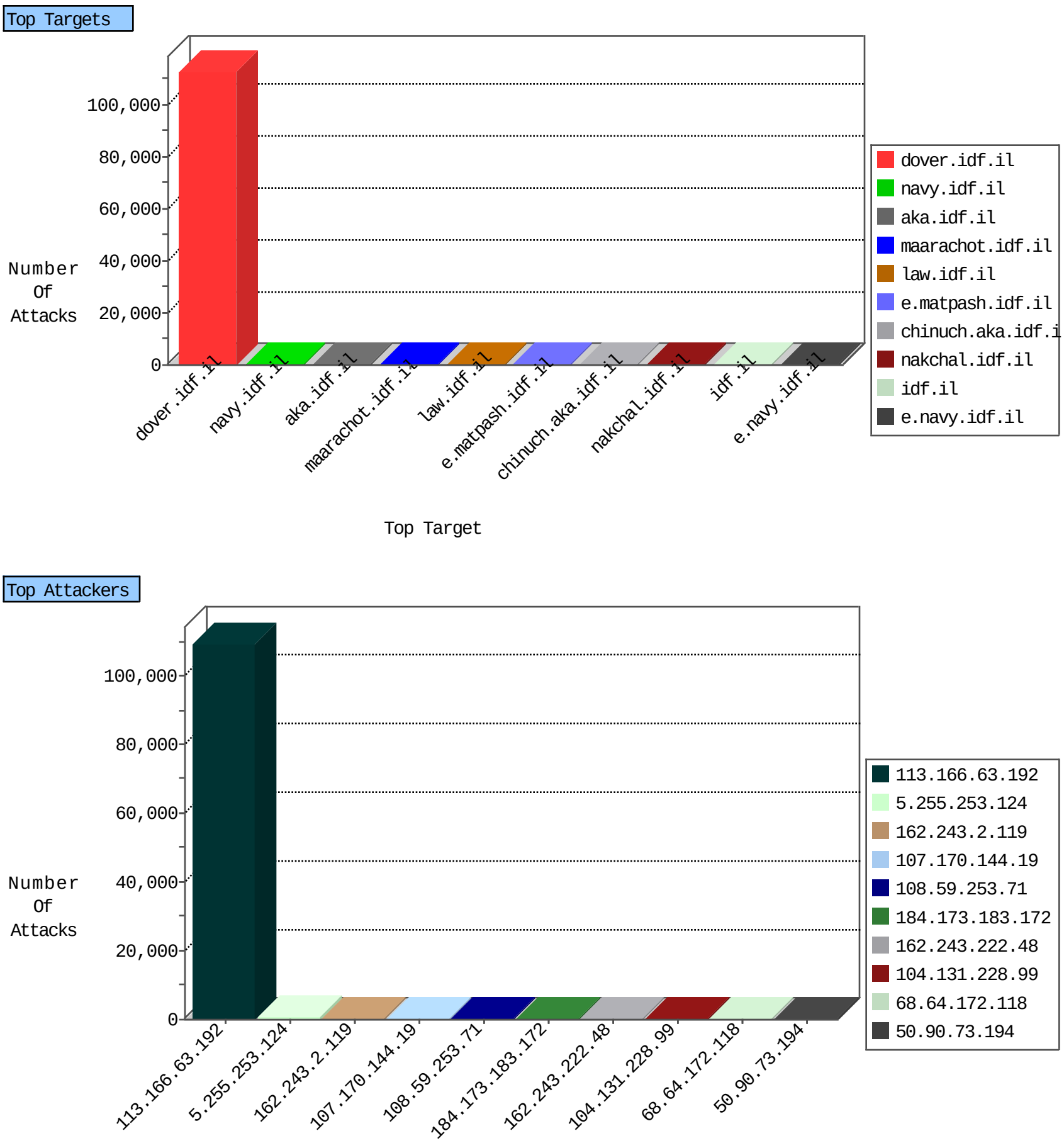
04-21-2015-03:03:10 to 04-21-2015-04:03:10

IDF Under Attack
04-21-2015-03:03:10



04-21-2015-03:03:10 to 04-21-2015-04:03:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4092
220.181.108.143	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	198
222.186.21.201	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
204.8.154.50	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
204.8.154.50	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

04-21-2015-03:03:10 to 04-21-2015-04:03:10

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	128
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	2
207.224.38.163	United States	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	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	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
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.31	nakchal.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	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.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

04-21-2015-03:03:10 to 04-21-2015-04:03:10

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	28
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
211.68.127.29	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
211.68.127.29	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
43.255.191.165	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
211.68.127.29	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.11	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.68.127.29	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.201	China	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.68.127.29	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
211.68.127.29	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
211.68.127.29	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.11	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.165	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.201	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.68.127.29	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.68.127.29	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1

04-21-2015-03:03:10 to 04-21-2015-04:03:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
113.166.63.192	Vietnam	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109273
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	678
162.243.2.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	410
107.170.144.19	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	395
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	144
162.243.222.48	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	128
104.131.228.99		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	122
68.64.172.118	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	102
50.90.73.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	77
166.137.244.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
153.107.97.169	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
173.208.169.226	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
65.129.179.108	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
70.199.103.229	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
140.139.231.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
85.72.40.4	Greece	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
109.66.61.219	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
66.249.79.58	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.102.6.210	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
66.102.6.202	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
31.116.149.50	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
192.68.112.171	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
69.175.127.10	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
216.244.83.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
88.198.25.217	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
188.40.112.210	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.102.6.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
73.184.196.81	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
66.249.79.66	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.79.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.138.99	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.139.14	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
200.25.211.193	Ecuador	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
220.255.1.106	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
220.255.1.128	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
207.224.38.163	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
212.174.166.140	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
82.193.98.24	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
89.252.2.14	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
70.27.133.117	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

04-21-2015-03:03:10 to 04-21-2015-04:03:10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.121.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	12
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	5
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	4
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	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
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16775-en/mmmmmmm=31c7cee2mmmmmmm_31c7cee2	Block	1
94.153.8.126	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
157.55.39.251	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/registrationwizard/register.aspx	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/rights/asp/faq.asp	None	1
180.76.6.52	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
95.90.229.211	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
157.55.39.252	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/doctrine/doctrine.stm	Block	1
66.249.64.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1312-he/refuah.aspx	Block	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0119-2.stm	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
176.12.138.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20387-he/dover.aspx	Block	1
66.249.65.11	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
157.55.39.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/signals.stm	Block	1
46.19.85.90	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
176.12.139.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/..aspx	Block	1

04-21-2015-03:03:10 to 04-21-2015-04:03:10