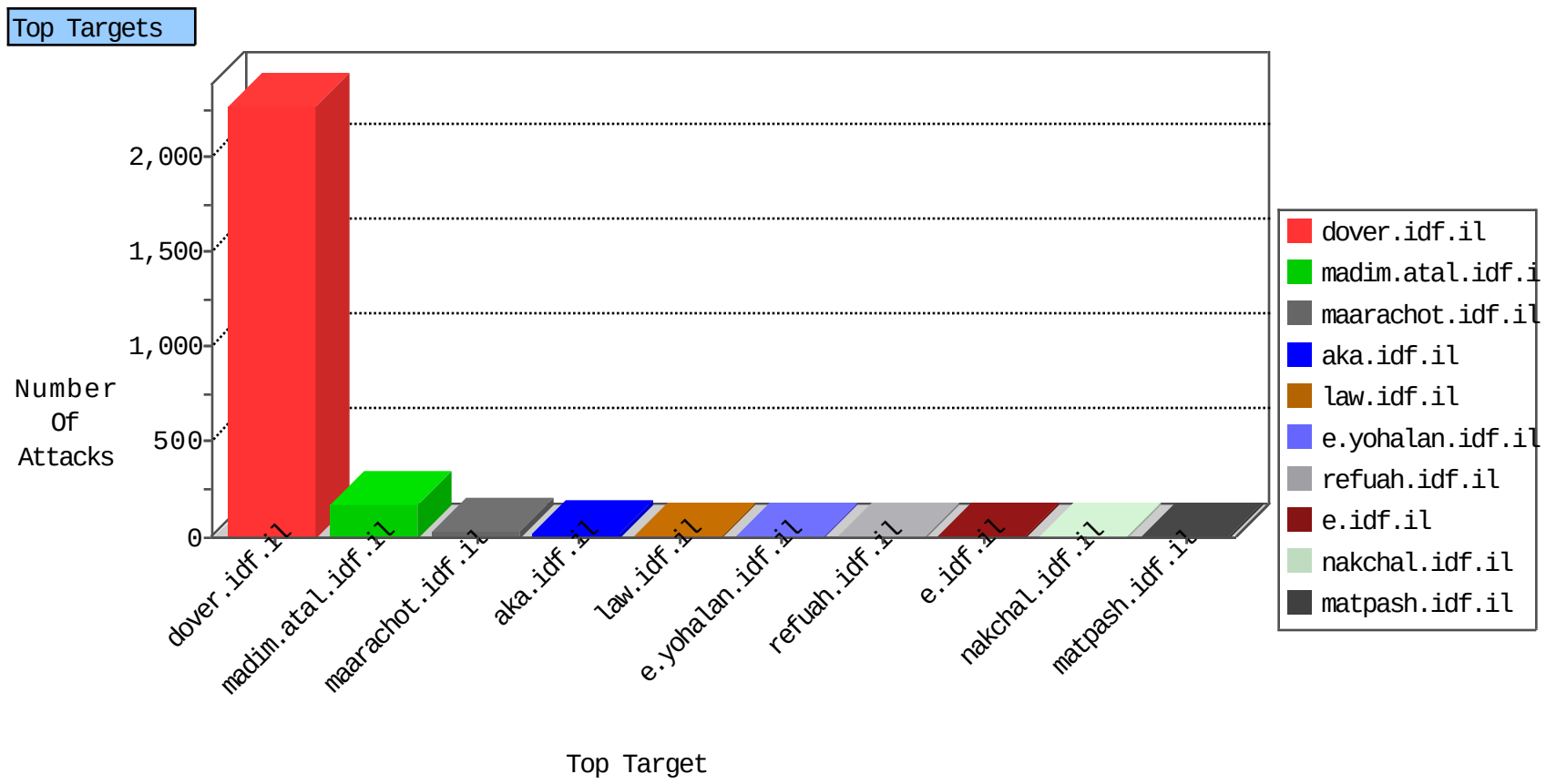
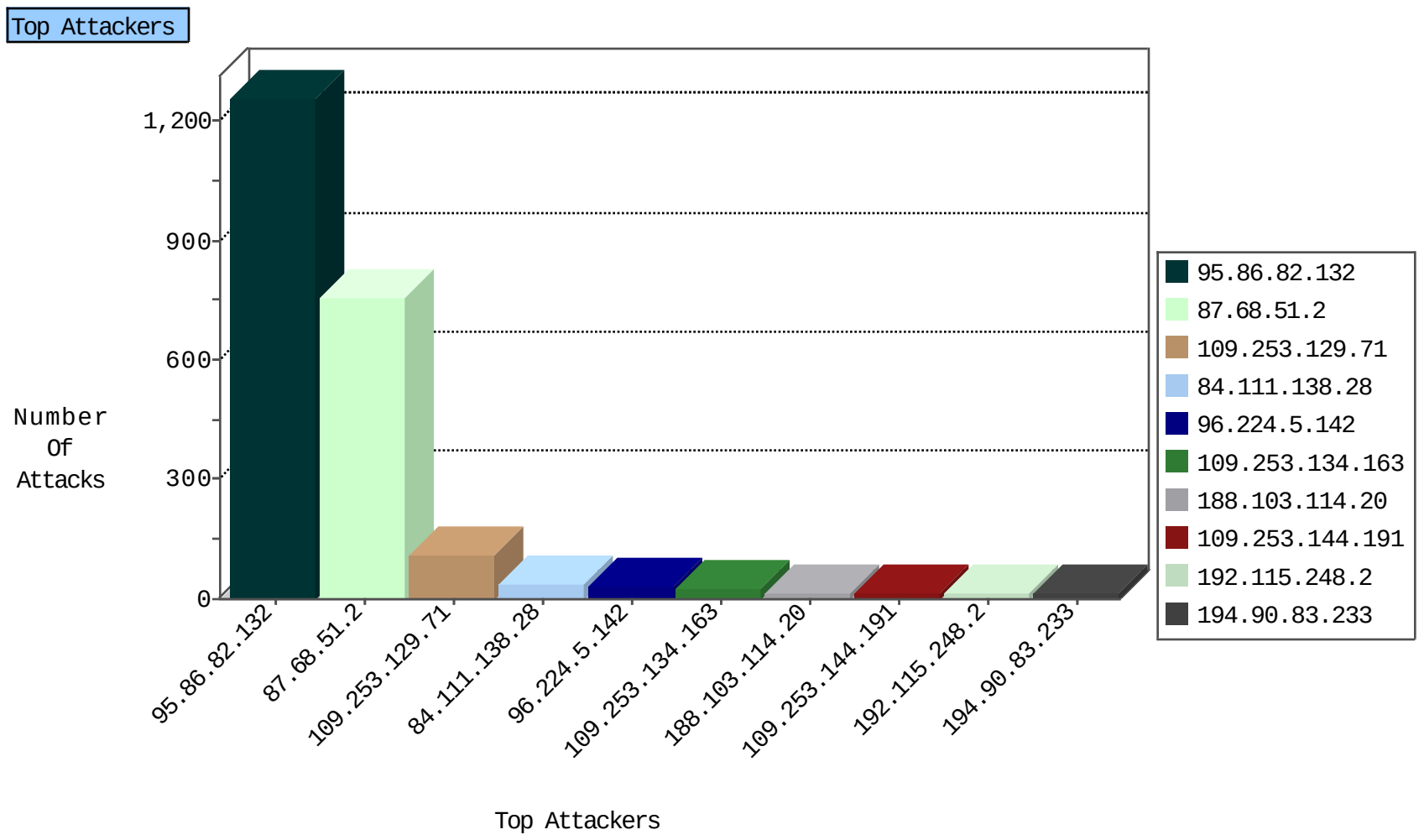
04-26-2015-06:03:00 to 04-26-2015-07:03:00

IDF Under Attack
04-26-2015-06:03:00

Top Targets



Top Attackers



04-26-2015-06:03:00 to 04-26-2015-07:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	120
192.115.248.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
77.126.212.156	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-26-2015-06:03:00 to 04-26-2015-07:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	2
66.240.236.119	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	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	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.200	eitan.aka.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
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1

04-26-2015-06:03:00 to 04-26-2015-07:03:00

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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.72.217	e.idf.il	ET SCAN NMAP -f -sS	1
222.186.21.195	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
203.150.228.208	Thailand	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
203.150.228.208	Thailand	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
140.210.1.248	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
140.210.1.248	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.21.195	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
207.46.13.114	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
203.150.228.208	Thailand	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
140.210.1.248	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2015-06:03:00 to 04-26-2015-07:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.82.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1259
87.68.51.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	756
84.111.138.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
96.224.5.142	United States	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	28
188.103.114.20	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.86.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
192.115.248.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.90	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.253.129.71	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.186.228.67	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
104.63.14.59		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.67.143.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.121.247.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
87.68.214.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.26	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.108.116.208	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
79.178.234.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.80.51.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.27	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.183.166.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.63.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.108.68.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.116.240.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.230.74.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.120.151.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.108.116.208	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
64.53.11.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.108.116.208	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.253.134.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.130.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
31.186.228.68	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
88.198.25.217	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.67.53.205	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1

04-26-2015-06:03:00 to 04-26-2015-07:03:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.129.71	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.129.71	Block	104
109.253.134.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
109.253.144.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
109.253.157.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
109.253.137.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
109.253.131.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
37.142.237.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2003/november/06.stm	Block	1
188.138.17.205	France	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.67.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
109.253.129.71	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/armored4.stm	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/procedure.asp	Block	1
2.54.0.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
74.82.47.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
216.223.27.22	United States	147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/../images/shared/home.png	Block	1
66.249.67.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2001/february/india_new.stm	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chamatz/home/d...sp	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in aka.idf.il/shalishut/site/gallery.aspx	None	1
85.65.53.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.67.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.112	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1
66.249.81.227	Israel	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../favicon.ico	Block	1
179.52.116.129	Dominican Republic	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/894-en/matpash.aspx	Block	1
46.19.85.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
125.209.235.185	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
96.224.5.142	United States	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
157.55.39.127	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
180.76.4.185	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kenesatuda	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter 0559c450 in www.aka.idf.il/main/home/default.aspx	None	1
109.67.53.205	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1

04-26-2015-06:03:00 to 04-26-2015-07:03:00