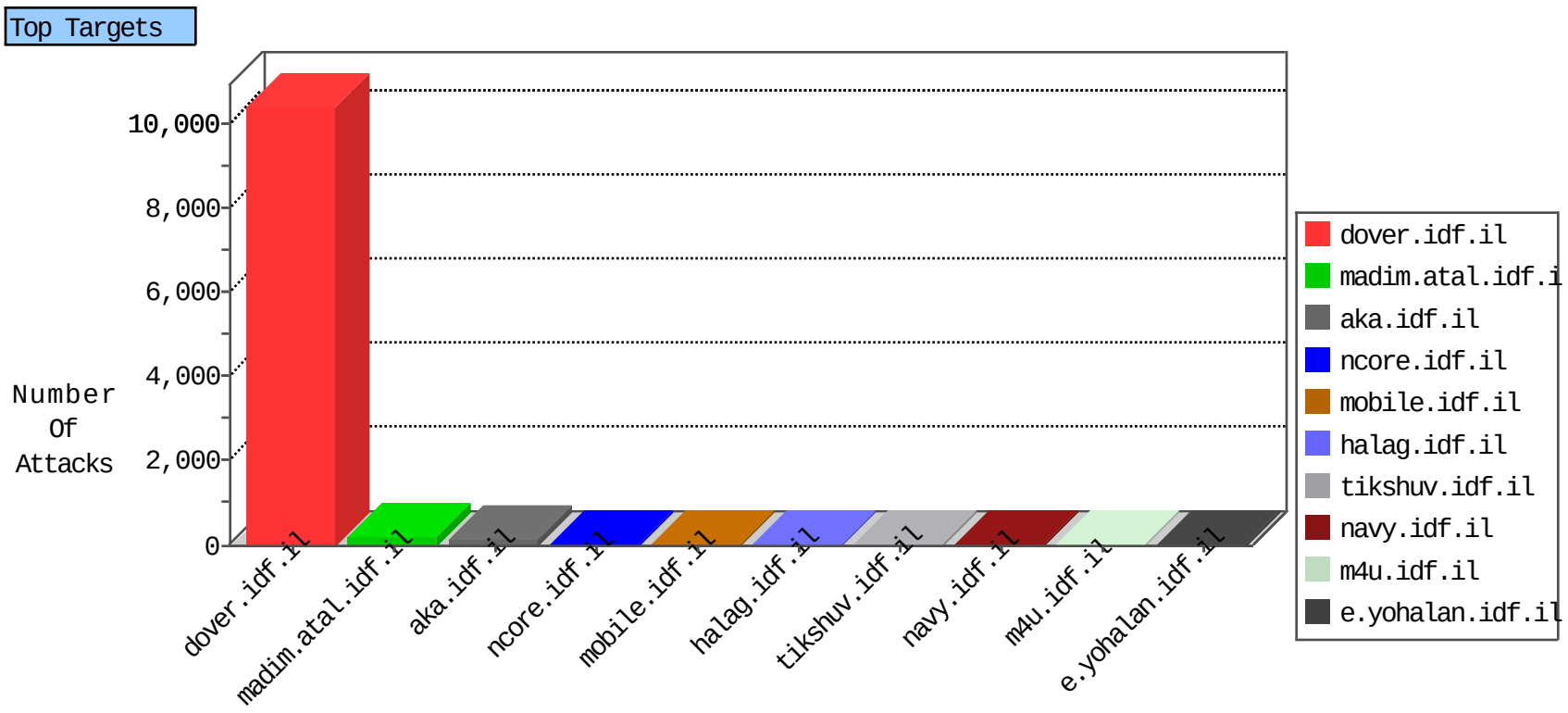
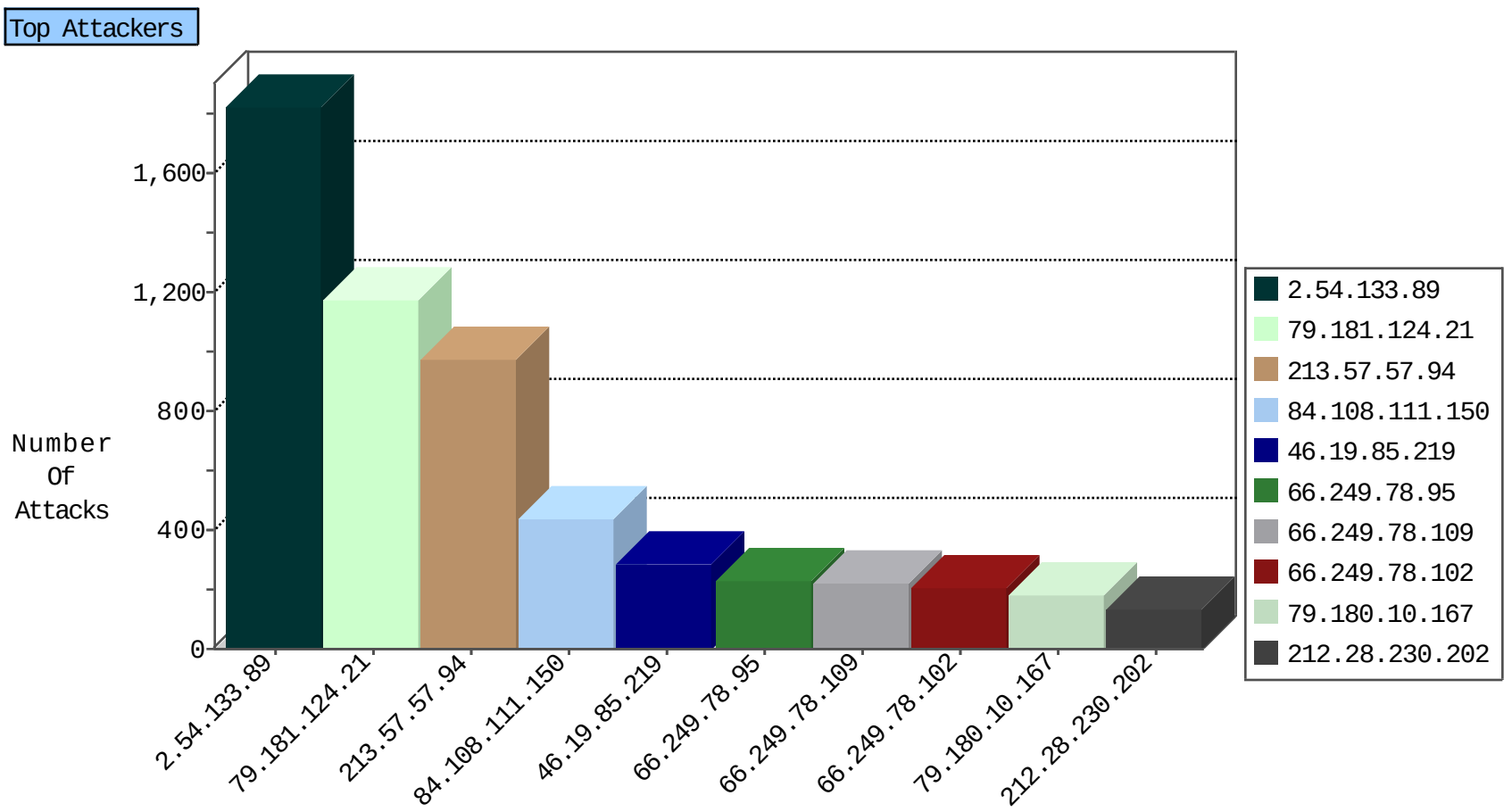
04-28-2015-07:03:04 to 04-28-2015-08:03:04

IDF Under Attack
04-28-2015-07:03:04

Top Targets



Top Attackers



04-28-2015-07:03:04 to 04-28-2015-08:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	221
109.253.143.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
220.181.108.76	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	27
79.179.168.120	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.180.107.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
61.4.196.74	Korea, Republic of	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	5
37.26.147.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
37.26.147.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.176.147.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
179.8.165.28	Chile	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
61.160.213.180	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
109.67.110.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.8	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.253.110.223	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.12.136.152	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.181.124.21	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.49.248	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
37.26.148.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.133.40	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.142.220	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.32.179.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.240.236.119	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
176.12.136.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.52.36.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.176.65.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-28-2015-07:03:04 to 04-28-2015-08:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.235	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.252	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.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
71.6.167.142	United States	147.237.76.147	chinuch.aka.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
85.25.103.50	Germany	147.237.76.200	eitan.aka.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
198.20.69.98	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
149.78.146.230	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.34	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
192.118.48.248	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-28-2015-07:03:04 to 04-28-2015-08:03:04

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	4
66.249.64.64	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
2.54.139.137	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.26.147.140	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
178.19.107.114	Poland	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
111.203.22.56	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -f -sS	1
91.224.132.118	Russian Federation	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
59.175.148.68	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
59.175.148.68	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
217.194.206.108	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.117.143.250	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.120.117	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.1.131	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
111.203.22.56	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
109.253.158.90	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.109	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
59.175.148.68	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
59.175.148.68	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.179.23.22	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.45	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-28-2015-07:03:04 to 04-28-2015-08:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.133.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1819
79.181.124.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1172
213.57.57.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	972
84.108.111.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	435
46.19.85.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	283
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	132
31.154.3.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	124
66.249.78.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
2.52.35.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	119
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	105
66.249.78.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	101
66.249.78.102	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
66.249.78.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	91
109.253.38.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	89
66.249.78.109	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	83
41.35.52.90	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
37.26.146.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
2.54.162.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
79.181.125.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
82.80.128.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
109.253.147.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
84.111.140.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
2.52.36.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
176.241.84.171	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
176.12.142.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
109.253.139.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
176.12.136.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
176.12.150.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
176.12.150.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
93.173.242.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
176.12.148.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
79.180.102.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
176.12.140.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
46.19.85.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
69.35.176.189	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
176.12.136.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
108.0.14.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
176.12.151.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
176.12.136.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
176.12.146.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
46.19.85.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
176.12.139.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.148.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
46.19.85.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.148.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29

04-28-2015-07:03:04 to 04-28-2015-08:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.180.10.167	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.10.167	Block	181
95.86.66.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.186.121.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
52.6.31.228	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 52.6.31.228	Block	2
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//templates/sendtofriend/sendtofriend.aspx	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
157.55.39.73	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
85.250.63.219	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	1
176.12.142.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/010.stm	Block	1
68.180.228.237	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12206-he/dover.aspx	Block	1
212.117.143.250	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.134.218.126	Hungary	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	1
37.26.147.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
176.12.150.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/1269-he/navy.aspx	Block	1
213.57.137.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.136.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.138.66.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/m/	Block	1
37.237.216.34	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
176.12.150.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.12.137.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.43.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
94.159.214.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
184.105.247.195	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmiluim/templates/www.behazdaa.org.il	Block	1
80.179.89.84	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
176.12.141.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.47.10	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
95.86.66.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.79.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12518-he/dover.aspx	Block	1

04-28-2015-07:03:04 to 04-28-2015-08:03:04