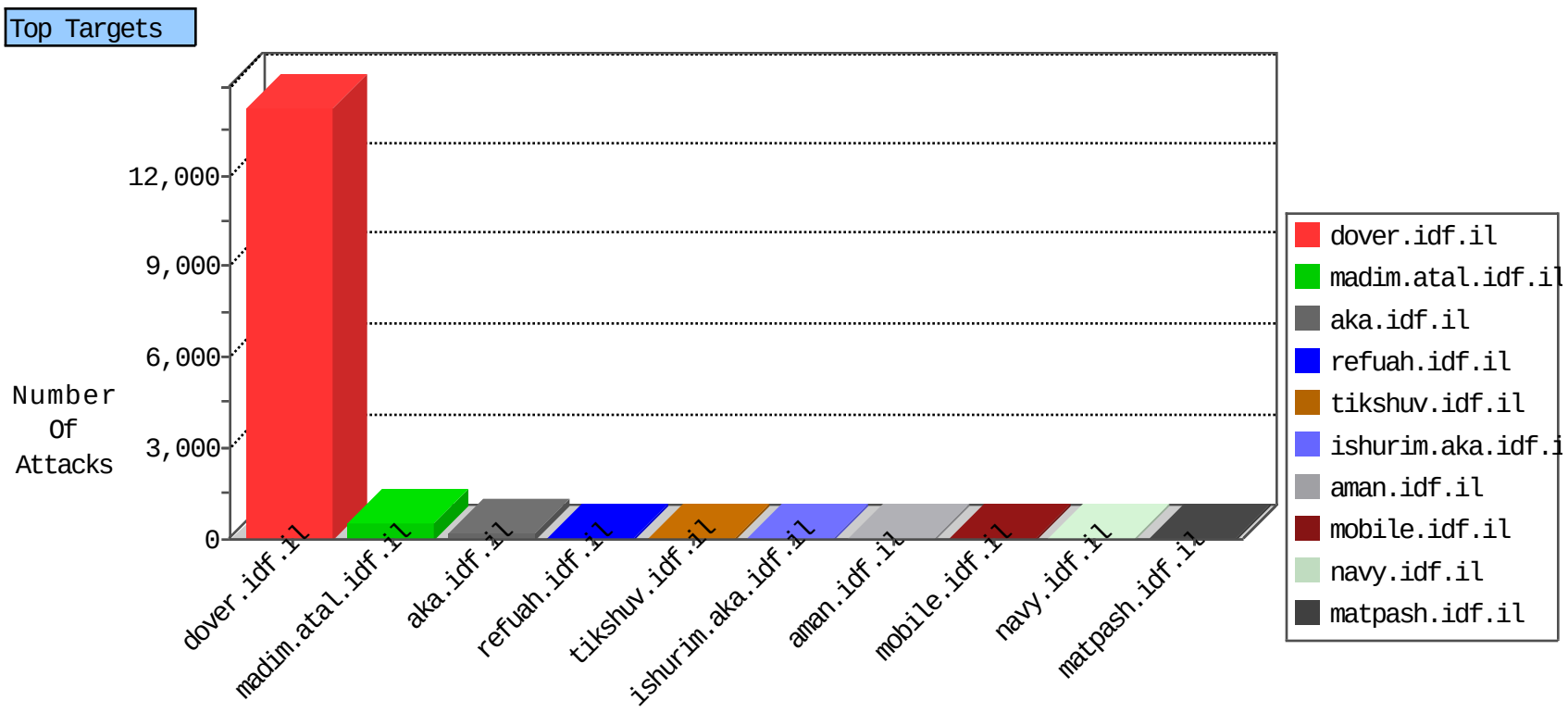
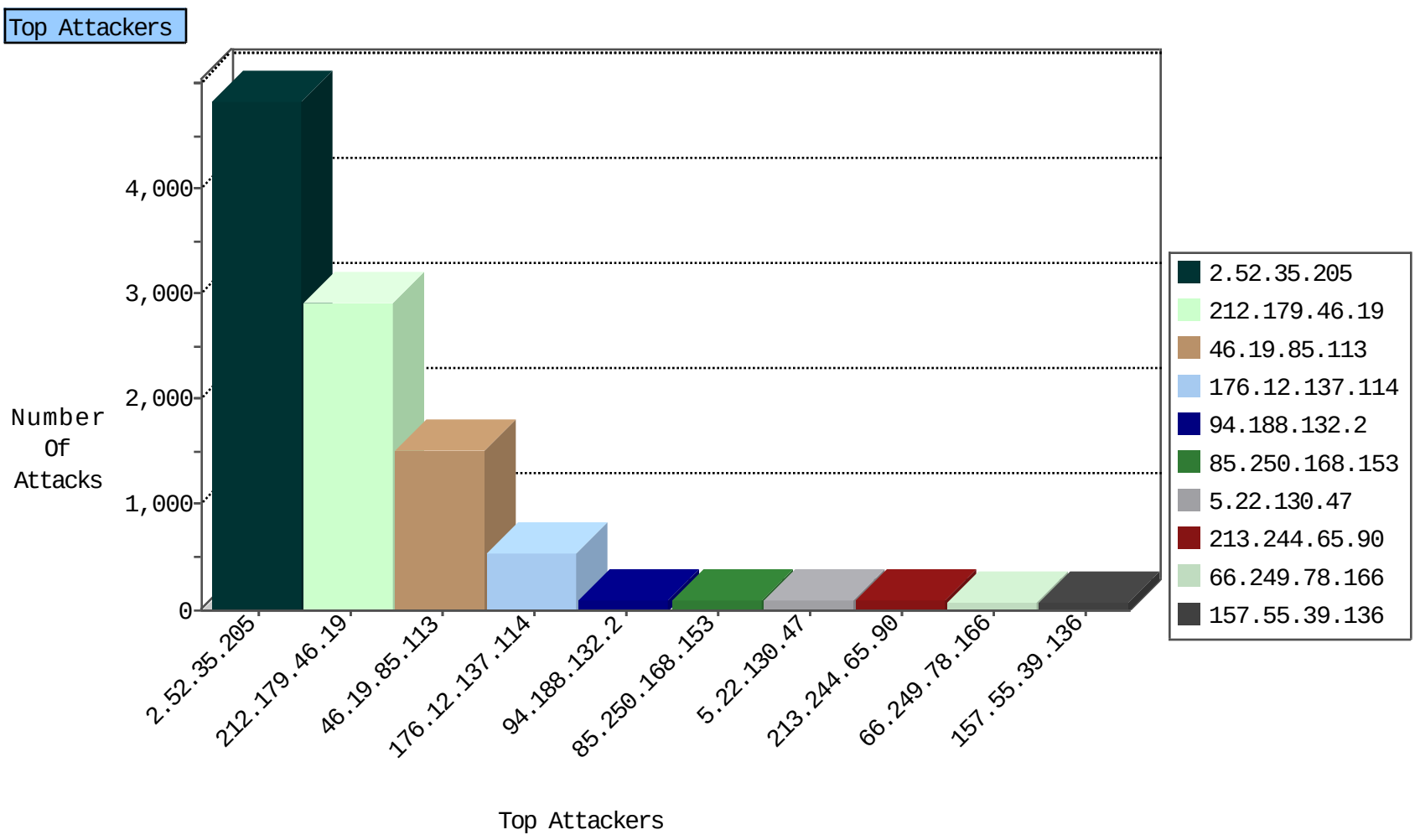
05-03-2015-17:03:04 to 05-03-2015-18:03:04

IDF Under Attack
05-03-2015-17:03:04

Top Targets



Top Attackers



05-03-2015-17:03:04 to 05-03-2015-18:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
213.57.172.231	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5738
220.141.52.112	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2953
62.219.224.149	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
212.199.195.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.85.105	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
87.69.39.95	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
203.176.181.57	Indonesia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
10.0.0.3		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
31.154.7.160	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
77.127.173.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.12.136.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.26.146.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-03-2015-17:03:04 to 05-03-2015-18:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	11
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
84.228.6.142	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.67.55.4	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	2
79.177.102.129	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.197	e.himush.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
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
5.29.147.85	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
217.26.52.21	Switzerland	147.237.76.42	refuah.idf.il	C071: HTTP: Access to - install.php	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	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.45	e.eitan.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
46.19.85.202	Israel	147.237.0.19	madim.atal.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
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.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
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
87.69.39.95	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	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1

05-03-2015-17:03:04 to 05-03-2015-18:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
84.109.49.95	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
217.26.52.21	Switzerland	147.237.76.42	refuah.idf.il	LOCAL_RULES - Request with the string install.php in it	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
187.101.132.36	Brazil	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
87.69.61.92	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.130	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.130	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.54.112.133	Uzbekistan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.54.112.133	Uzbekistan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
213.10.0.53	Netherlands	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
74.217.148.77	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
193.104.115.2	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
62.219.13.180	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
182.72.109.162	India	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.61.139	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.173.33.251	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
85.65.45.6	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.130	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.54.112.133	Uzbekistan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.202	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
84.54.112.133	Uzbekistan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
2.52.148.229	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.204.144	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.67	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
154.121.251.22		147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
106.39.95.194	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

05-03-2015-17:03:04 to 05-03-2015-18:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.52.35.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4845
212.179.46.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2928
46.19.85.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1524
85.250.168.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	104
94.188.132.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	104
5.22.130.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	96
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
2.98.247.12	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	69
79.148.75.55	Spain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
212.179.23.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
2.54.143.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
46.19.85.50	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
149.78.216.15	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
212.235.77.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
212.179.61.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
46.19.86.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
46.19.86.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
62.219.135.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
207.241.237.107	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
31.168.132.62	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
195.212.93.2	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
80.246.140.136	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
46.116.234.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
2.52.180.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
203.141.115.89	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
46.19.86.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
157.55.39.139	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
84.228.14.50	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
84.42.175.90	Czech Republic	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
85.65.113.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
41.237.157.187	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
79.177.96.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
31.44.129.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
82.81.193.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
128.239.239.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
79.211.105.83	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
62.90.2.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
192.114.91.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
95.144.186.103	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.137.114	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.137.114	Block	532
84.109.49.95	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.109.49.95	Block	11
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	9
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	7
112.74.87.10	China	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 112.74.87.10	Block	4
5.255.253.93	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mod	Block	4
77.126.238.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
46.229.164.99	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.99	Block	4
84.109.49.95	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.109.49.95	Block	4
5.28.183.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.25.119.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
112.74.87.10	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.179.57.127	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	3
79.182.222.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.29.120.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.140.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.14.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.62.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.229.164.114	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	2
108.237.88.206	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/homefront3.stm	Block	2
5.29.22.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.168.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.64.57.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.68.8.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
64.124.203.75	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/ag/	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/forms	Block	1
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/valtam/asp/default.asp	None	1
176.10.104.227	Switzerland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 176.10.104.227	Block	1
2.52.56.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.61	Block	1
74.217.148.75	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bc/	Block	1
109.65.97.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/913-2792-he/patzar.aspx	Block	1
208.50.101.156	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bg/	Block	1
46.229.164.102	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	1
207.46.13.91	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//site/unselecatble.aspx	Block	1
84.109.49.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
79.179.124.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.235.30.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
112.74.87.10	China	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
89.138.83.35	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1