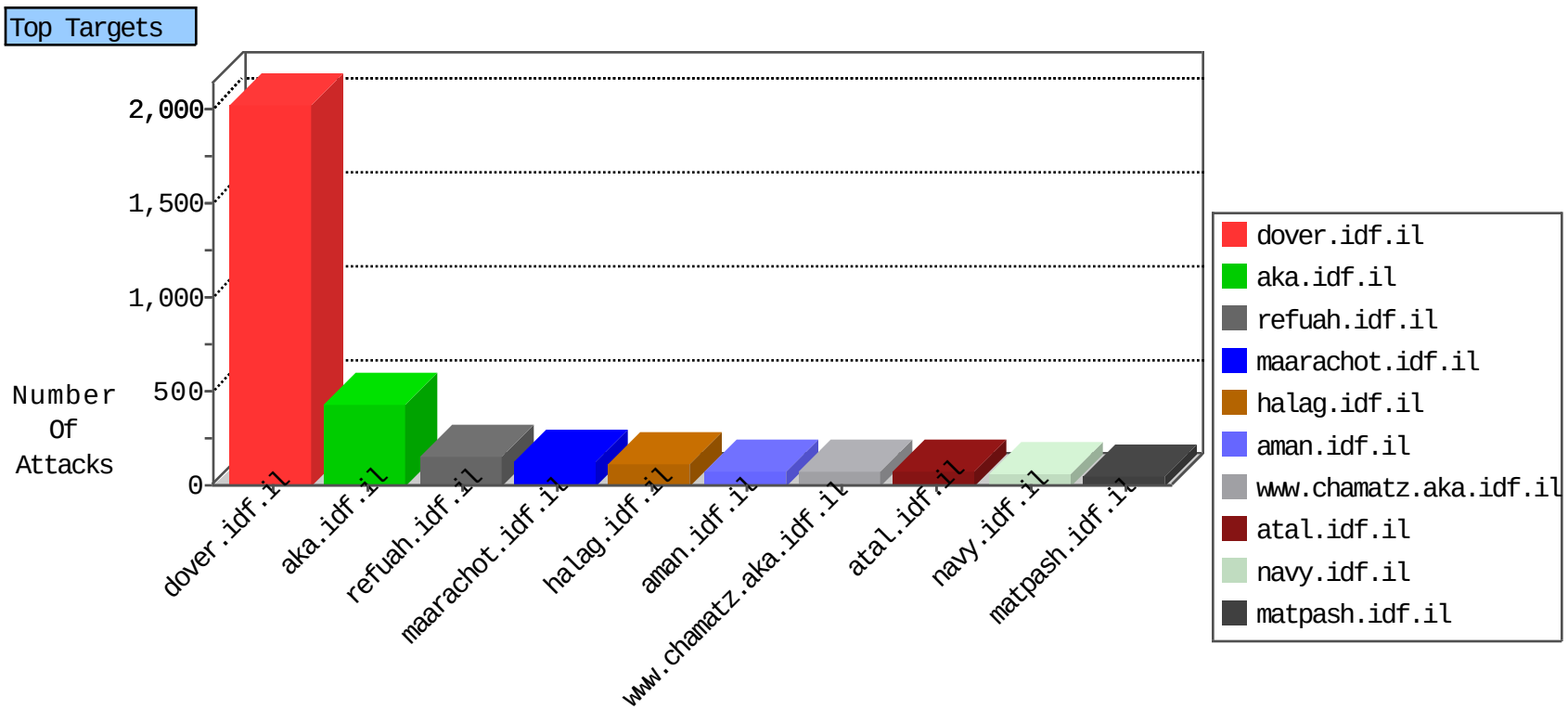
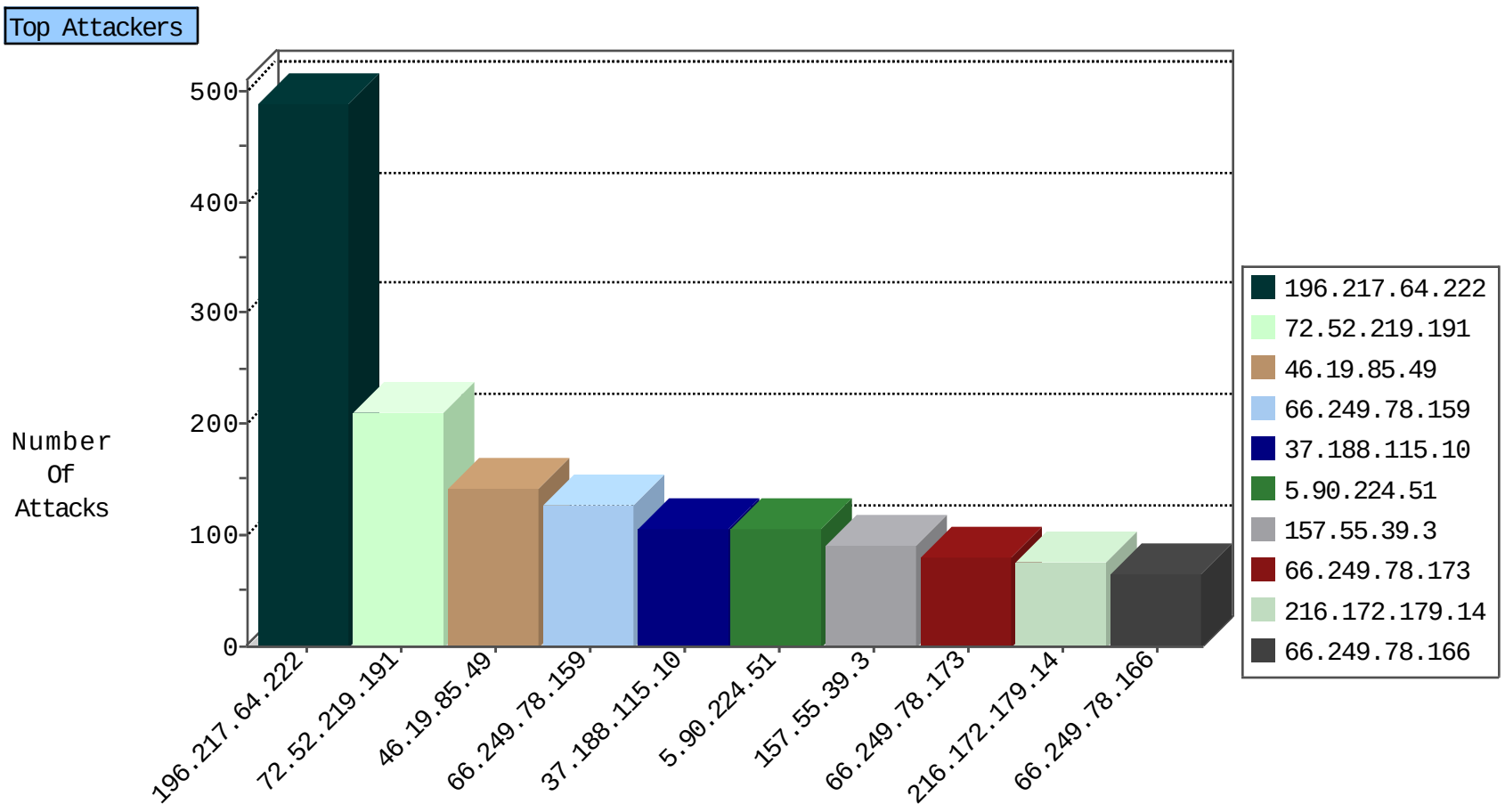
10-30-2015-23:04:00 to 10-31-2015-00:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-30-2015-23:04:00 to 10-31-2015-00:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4260
96.91.243.195	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2800
2.54.21.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2250
196.217.64.222	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1741
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	779
146.148.48.61	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	691
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	259
79.179.100.72	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	256
2.54.21.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
46.19.86.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
212.179.227.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20
109.66.119.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
31.210.186.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.19.85.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
213.57.202.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.170.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.248.187.14	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.137.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.15.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
84.94.181.145	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.199.57.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.158.203.148	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
109.66.133.68	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
31.210.186.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
218.250.9.192	Hong Kong	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
46.117.3.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
109.66.52.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
84.94.181.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-30-2015-23:04:00 to 10-31-2015-00:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
196.217.64.222	Morocco	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	2

10-30-2015-23:04:00 to 10-31-2015-00:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
196.217.64.222	147.237.77.216	Morocco	dover.idf.il	ET SCAN Metasploit WMAP GET len 0 and type	13
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
181.198.213.98	147.237.0.15	Ecuador	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.75.60	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
181.198.213.98	147.237.76.196	Ecuador	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
38.129.240.45	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
38.129.240.45	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
212.1.114.195	147.237.77.234	Ukraine	halag.idf.il	ET SCAN Potential SSH Scan	2
181.198.213.98	147.237.76.176	Ecuador	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
38.129.240.45	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
38.129.240.45	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
181.198.213.98	147.237.0.19	Ecuador	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.77.233	Ukraine	atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
38.129.240.45	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
181.198.213.98	147.237.76.44	Ecuador	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
181.198.213.98	147.237.8.24	Ecuador	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN Potential SSH Scan	1
181.198.213.98	147.237.0.33	Ecuador	idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.76.30	Ukraine	himush.idf.il	ET SCAN Potential SSH Scan	1
181.198.213.98	147.237.0.17	Ecuador	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
121.40.195.144	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
196.217.64.222	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
38.129.240.45	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
78.142.19.47	147.237.0.35	Bulgaria	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
38.129.240.45	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.1.114.195	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
38.129.240.45	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1

10-30-2015-23:04:00 to 10-31-2015-00:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
196.217.64.222	Morocco	147.237.77.216	dover.idf.i	drop		drop	344
46.19.85.49	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	143
196.217.64.222	Morocco	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	116
5.90.224.51	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	105
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
197.37.209.24	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
2.54.166.192	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
99.245.242.141	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
2.54.21.82	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
172.56.14.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
100.100.122.241		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
46.19.86.36	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
91.177.9.147	Belgium	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	16
46.120.229.31	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
46.19.86.24	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
213.57.129.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
40.77.167.37	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.52.208	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
100.100.36.58		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
100.100.2.95		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
100.100.2.95		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
100.100.82.160		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
100.100.106.246		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	10
66.249.78.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
213.57.202.27	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
92.90.26.44	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
141.0.14.187	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
40.77.167.33	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
79.176.196.165	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
149.161.132.176	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
41.43.158.92	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
66.249.67.65	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.46.39.196	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
79.182.68.110	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
37.26.146.146	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
46.120.13.246	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
31.210.186.168	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
46.19.85.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.78.159	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7

10-30-2015-23:04:00 to 10-31-2015-00:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.188.115.10	United Kingdom	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	45
197.38.213.220	Egypt	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/maslul.aspxÂ¿catid=60570&docid=72235	Block	45
72.52.219.191	United States	147.237.77.234	halag.idf.il	PHP Attempt	Block	45
198.1.101.123	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	45
72.52.219.191	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	45
212.179.227.147	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	30
79.170.40.38	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.170.40.38	Block	30
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	30
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	30
37.188.115.10	United Kingdom	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 37.188.115.10	Block	30
72.52.219.191	United States	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 72.52.219.191	Block	30
72.52.219.191	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 72.52.219.191	Block	30
216.172.179.14	United States	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	30
72.52.219.191	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/index.php	Block	15
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	15
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	15
46.19.86.30	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	15
216.172.179.14	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/index.php	Block	15
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17455.jpg	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10641-he/dover.aspx	Block	15
66.249.69.84	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-5512-he	Block	15
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/skira/default.asp	None	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
72.52.219.191	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/index.php	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	15
66.249.75.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/0/770.pdf	Block	15
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter siteid in aka.idf.il/sites/klali/default.asp	None	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.19.86.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
207.46.13.100	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	15
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
72.52.219.191	United States	147.237.77.234	halag.idf.il	Admin Blocking	Block	15
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/926-he/refuah.aspx	Block	15
216.172.179.14	United States	147.237.77.226	www.chamatz.aka.idf.il	Admin Blocking	Block	15
157.55.39.245	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chinuch/miktzoa/default.asp	None	15
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	15
79.170.40.38	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	15
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19916-he/idfgdover.aspx	Block	15
46.116.150.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	15
72.52.219.191	United States	147.237.77.170	maarachot.idf.il	Admin Blocking	Block	15
5.22.130.68	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	15
207.46.13.100	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9070-he/atal.aspx	Block	15
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/sites/home/default.asp	None	15
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	15
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8905-he/refuah.aspx	Block	15
37.188.115.10	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/index.php	Block	15

10-30-2015-23:04:00 to 10-31-2015-00:04:00