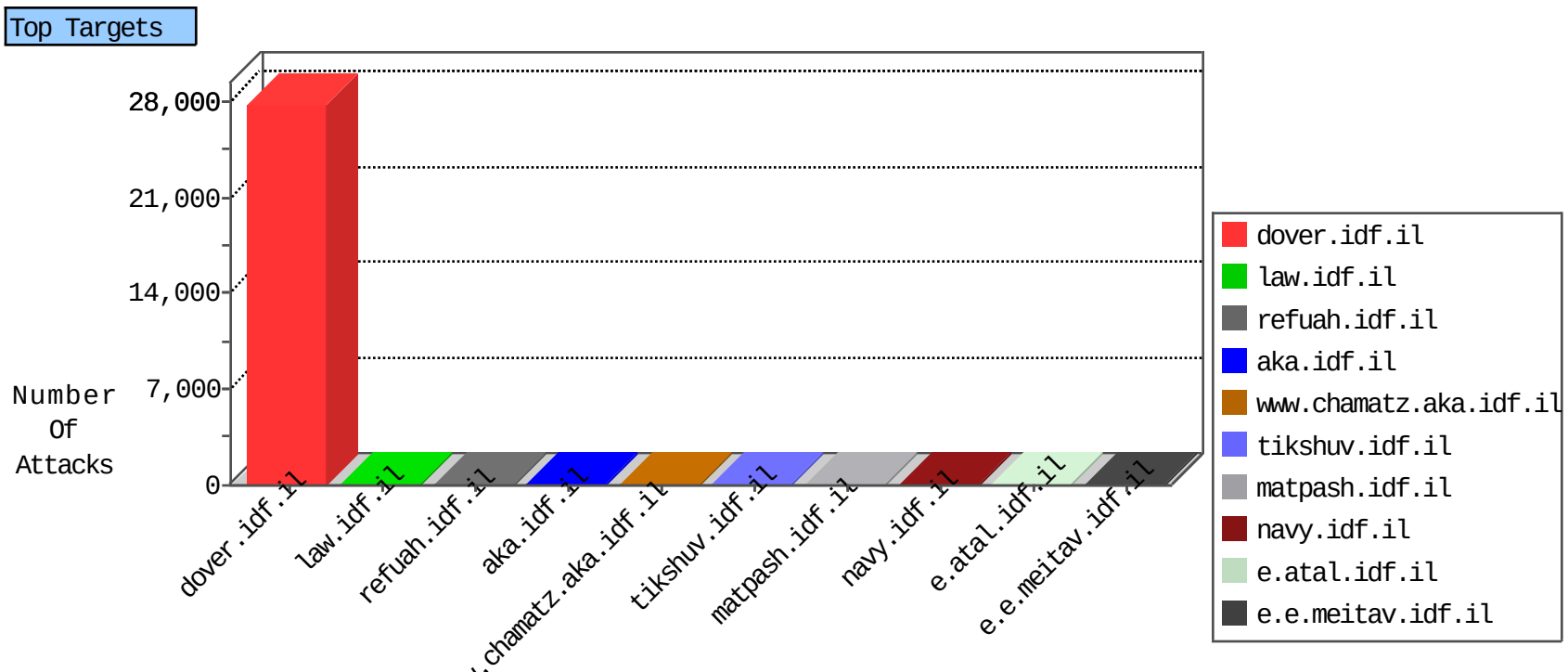
08-26-2016-04:04:04 to 08-26-2016-05:04:04

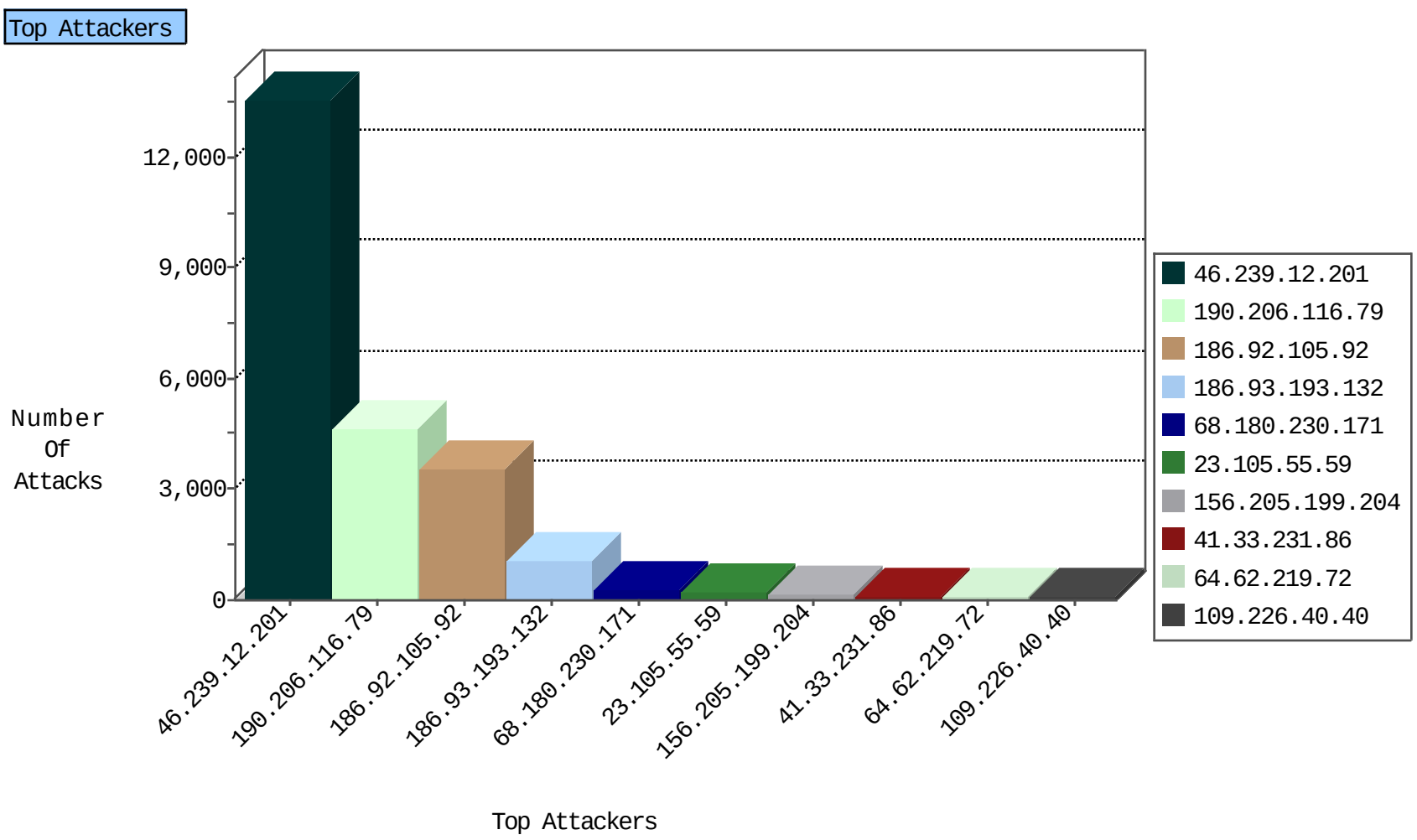
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-26-2016-04:04:04 to 08-26-2016-05:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1603770
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	264415
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	109719
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4991
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1889
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1679
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1675
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1330
186.93.193.132	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	616
186.93.193.132	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	377
23.105.55.59	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	193
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	184
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	102
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	96
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	93
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	79
186.93.193.132	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	74
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	71
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	68
64.62.219.74	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	64
64.62.219.72	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	64
66.249.69.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	61
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	60
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	47
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	46
64.62.219.148	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	46
64.62.219.76	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	43
64.62.219.80	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	37
64.62.219.72	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	35
108.59.253.71	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	35
64.62.219.85	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	35
64.62.219.74	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	33
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	31
64.62.219.77	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	31
64.62.219.158	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	31
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	30
64.62.219.84	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
64.62.219.154	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
64.62.219.165	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
64.62.219.79	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
64.62.219.153	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
64.62.219.157	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
84.108.182.191	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
64.62.219.84	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
64.62.219.79	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	26
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
64.62.219.77	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24

08-26-2016-04:04:04 to 08-26-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.95	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
71.171.93.66	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
216.119.125.173	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	9
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
177.185.194.45	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
38.110.11.92	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.171	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
71.171.93.66	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
209.15.196.171	Canada	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
23.91.70.95	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.58	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
71.171.93.66	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.76.149.15	Spain	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
89.44.144.244	Romania	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.154.235.88	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.17.114.79	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
23.96.97.233	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	2
216.119.125.57	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
216.119.125.173	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-26-2016-04:04:04 to 08-26-2016-05:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
71.171.93.66	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	26
23.91.70.95	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	20
87.242.112.35	147.237.76.42	Russian Federation	refuah.idf.il	SQL Injection - Select From	20
195.76.149.15	147.237.72.166	Spain	aka.idf.il	SQL Injection - Select From	18
177.185.194.45	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	14
209.15.196.171	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	14
216.119.125.173	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	10
184.168.46.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
38.110.11.92	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
209.17.114.79	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
195.154.235.88	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	8
184.168.152.58	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
89.44.144.244	147.237.72.166	Romania	aka.idf.il	SQL Injection - Select From	8
23.96.97.233	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	7
216.119.125.57	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
42.116.29.68	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
88.249.106.23	147.237.72.217	Turkey	e.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
68.190.208.191	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
163.172.169.150	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.72.217	Sweden	e.idf.il	ET SCAN NMAP -sS window 1024	1
42.116.29.68	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.169.150	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
68.190.208.191	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.169.150	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
68.190.208.191	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
163.172.169.150	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
157.122.97.182	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1

08-26-2016-04:04:04 to 08-26-2016-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13072
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	529
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
141.0.14.75	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
141.0.15.35	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	8
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	7
59.120.255.127	Taiwan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
40.77.169.97	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
83.168.250.50	Sweden	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
185.29.9.249	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.96	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop		drop	3
84.94.47.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.96	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.91.8	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	2
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
66.249.65.50	Israel	147.237.0.33	idf.il	drop		drop	1
183.129.160.229	China	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
79.180.100.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.167.66	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.198	e.yohalan.idf.il	drop	SAM rule	drop	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.67	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1

08-26-2016-04:04:04 to 08-26-2016-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
180.76.15.7	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
40.77.169.102	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.76.15.31	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
77.237.146.28	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
157.55.39.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
157.55.39.229	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1

08-26-2016-04:04:04 to 08-26-2016-05:04:04