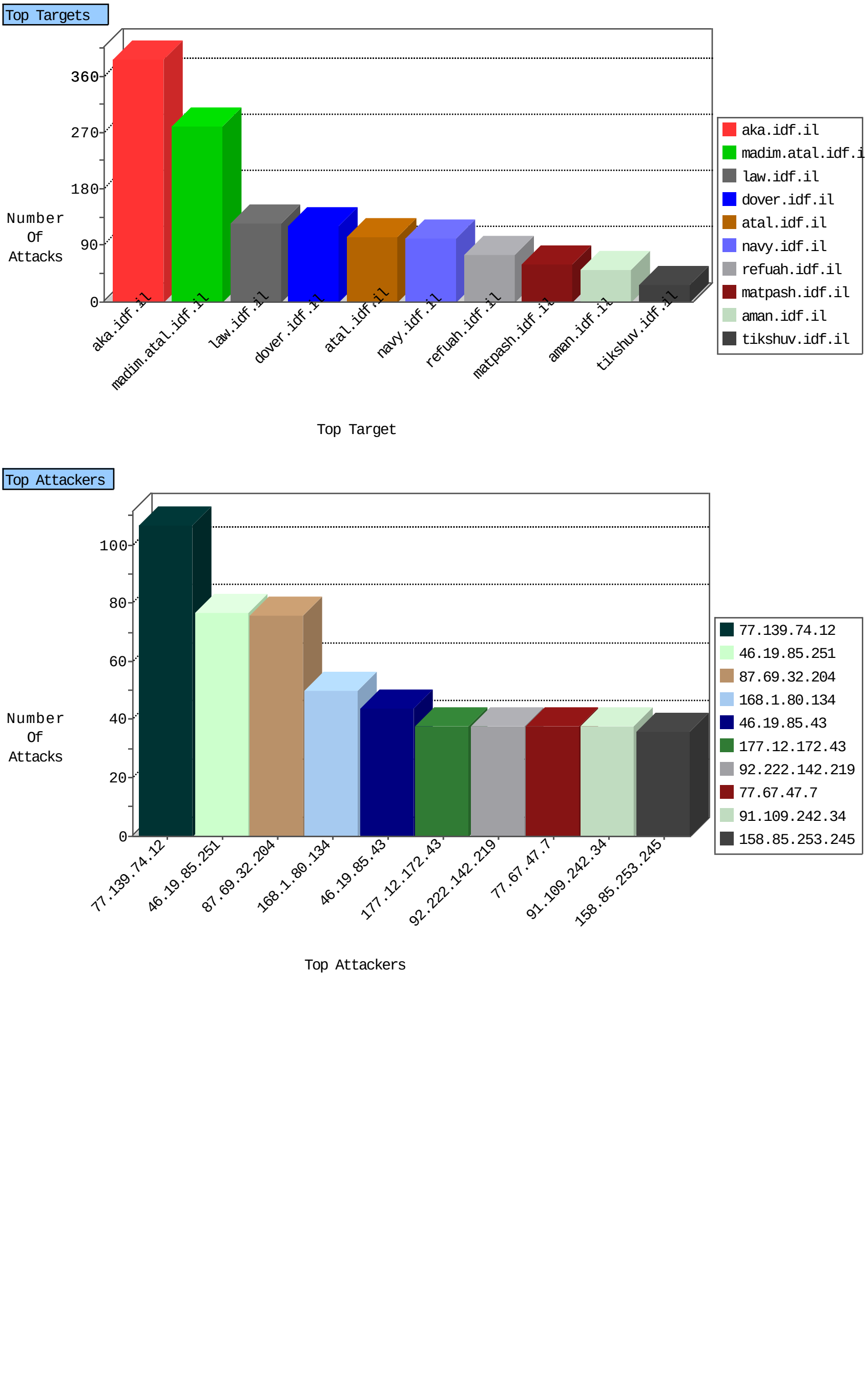
09-13-2016-20:04:03 to 09-13-2016-21:04:03

IDF Under Attack Daily Report



09-13-2016-20:04:03 to 09-13-2016-21:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
5.102.220.105	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
198.82.160.221	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
213.57.95.210	Israel	147.237.72.156	aman.idf.il	Black List	drop	1

09-13-2016-20:04:03 to 09-13-2016-21:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.1.80.134	Australia	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
77.67.47.7	France	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
92.222.142.219	France	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
177.12.172.43	Brazil	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
91.109.242.34	United Kingdom	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
92.222.142.219	France	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
24.222.4.86	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.12.172.43	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.242.112.45	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
185.21.133.159	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.109.242.34	United Kingdom	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
202.124.109.87	New Zealand	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.1.80.134	Australia	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
64.87.23.55	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.81	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.42	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.1.80.134	Australia	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
77.67.47.7	France	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.104.215	United States	147.237.77.74	law.idf.il	C1000016: HTTP: administrator in URI	Permit	6
23.91.70.95	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.109.242.34	United Kingdom	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
216.119.125.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
184.168.104.215	United States	147.237.77.74	law.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

09-13-2016-20:04:03 to 09-13-2016-21:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
168.1.80.134	147.237.77.176	Australia	matpash.idf.il	SQL Injection - Select From	26
177.12.172.43	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	20
92.222.142.219	147.237.76.86	France	navy.idf.il	SQL Injection - Select From	20
91.109.242.34	147.237.76.86	United Kingdom	navy.idf.il	SQL Injection - Select From	20
77.67.47.7	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	20
24.222.4.86	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	18
216.119.125.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
87.242.112.45	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	8
64.87.23.55	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
185.21.133.159	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
50.77.136.81	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
23.91.70.42	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
202.124.109.87	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	8
184.168.27.81	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	8
23.91.70.95	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
106.51.226.59	147.237.8.45	India	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
202.79.60.94	147.237.77.233	Nepal	atal.idf.il	ET SCAN NMAP -sS window 4096	1
202.79.60.94	147.237.77.233	Nepal	atal.idf.il	ET SCAN NMAP -f -sS	1
52.166.249.197	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
178.20.188.164	147.237.76.86	Jordan	navy.idf.il	ET SCAN NMAP -sS window 4096	1
178.20.188.164	147.237.76.86	Jordan	navy.idf.il	ET SCAN NMAP -f -sS	1
106.51.226.59	147.237.8.45	India	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
202.79.60.94	147.237.77.233	Nepal	atal.idf.il	ET SCAN NMAP -sS window 2048	1
52.166.249.197	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
188.0.236.165	147.237.76.200	Moldova, Republic of	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.10.97	147.237.72.166	Israel	aka.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
178.20.188.164	147.237.76.86	Jordan	navy.idf.il	ET SCAN NMAP -sS window 2048	1

09-13-2016-20:04:03 to 09-13-2016-21:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.69.32.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
87.69.32.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
158.85.253.245	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
79.177.25.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
46.19.85.43	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.126.43.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
85.64.40.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
77.126.43.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.67.118.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
109.66.143.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
84.95.61.246	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.43	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.67.158.165	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
217.132.156.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
217.132.178.89	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
84.94.82.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.26.147.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
176.13.15.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.127	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
46.19.86.35	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.176.133	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
74.208.218.66	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.230.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	6
109.64.100.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
158.85.253.245	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
87.68.59.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.230.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
158.85.253.245	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
184.168.27.118	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
87.68.59.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.181.130.226	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.0.115	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.22.134.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.241.225.212	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	4
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
212.35.165.222	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.246.230	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.177.222.57	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
84.94.82.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
46.19.85.155	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-13-2016-20:04:03 to 09-13-2016-21:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.74.12	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
109.253.156.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
89.138.114.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
89.139.190.155	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	21
89.138.185.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	12
77.139.3.39	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.3.39	Block	4
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.184.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
141.226.218.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.3.39	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
80.246.136.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.195.50.85	Ireland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	2
77.138.8.86	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
2.53.30.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
83.137.1.203	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
46.19.86.219	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
37.142.10.97	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.10.97	Block	1
2.53.36.199	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.25.70	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
157.55.39.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/vb/sendmessage.php	Block	1
66.249.73.182	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
109.66.49.174	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
84.108.0.129	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.55.36.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.45.13	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	1
213.57.98.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.156.8	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.219	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
89.139.157.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.10.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/_vti_bin/owssvr.dll	Block	1
2.53.170.89	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.179.168.19	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
66.249.93.13	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	Block	1
109.66.167.33	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
87.70.55.43	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
213.57.143.99	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.191	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
2.53.178.84	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.181.130.226	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
77.126.66.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
173.62.166.31	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
46.19.86.219	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
109.67.118.243	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
89.138.114.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Parameter Type Violation on madim.atal.idf.il/mobile/1088-he/meretz.aspx parameter ctl00$ContentPlaceHolder1$txtMobile	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
217.132.44.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
2.53.8.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
144.76.120.23	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1

09-13-2016-20:04:03 to 09-13-2016-21:04:03