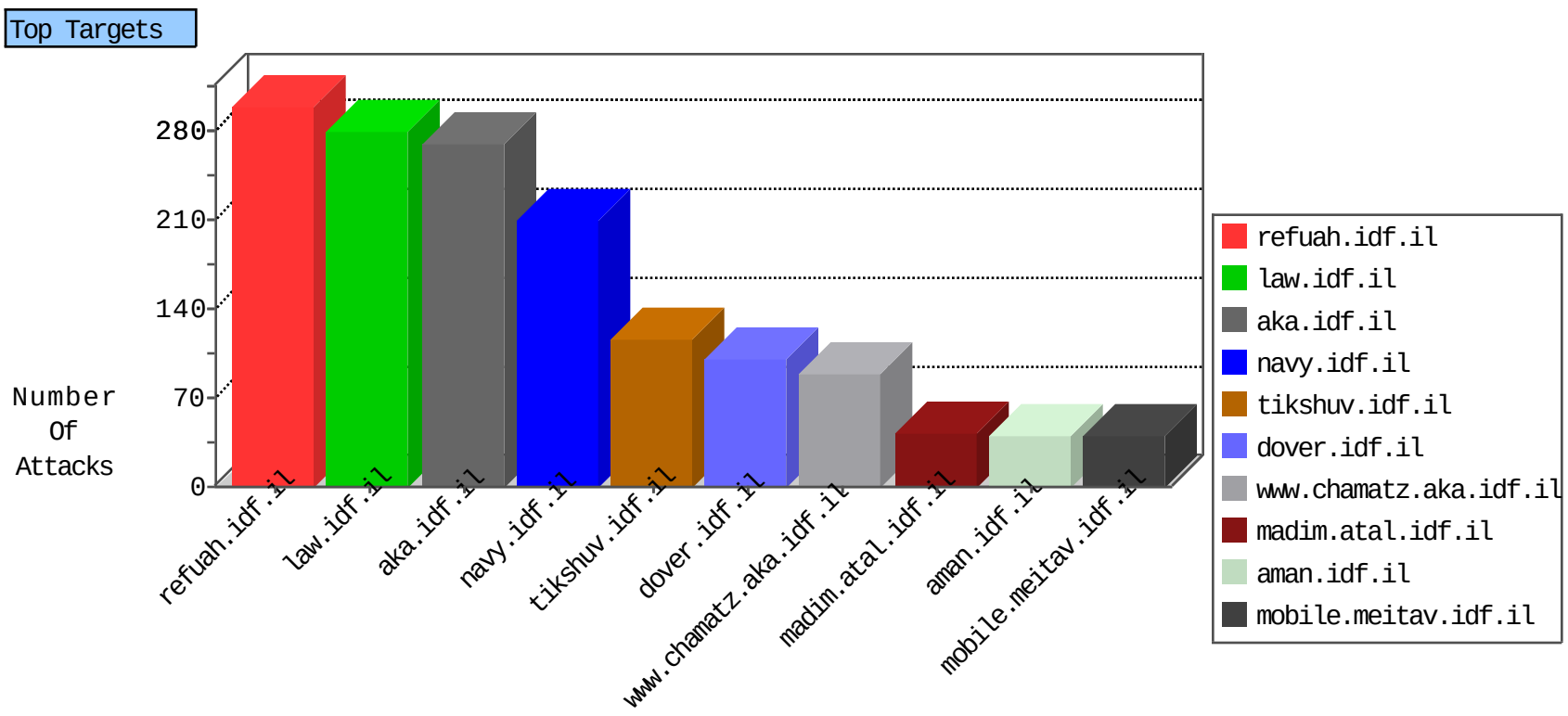
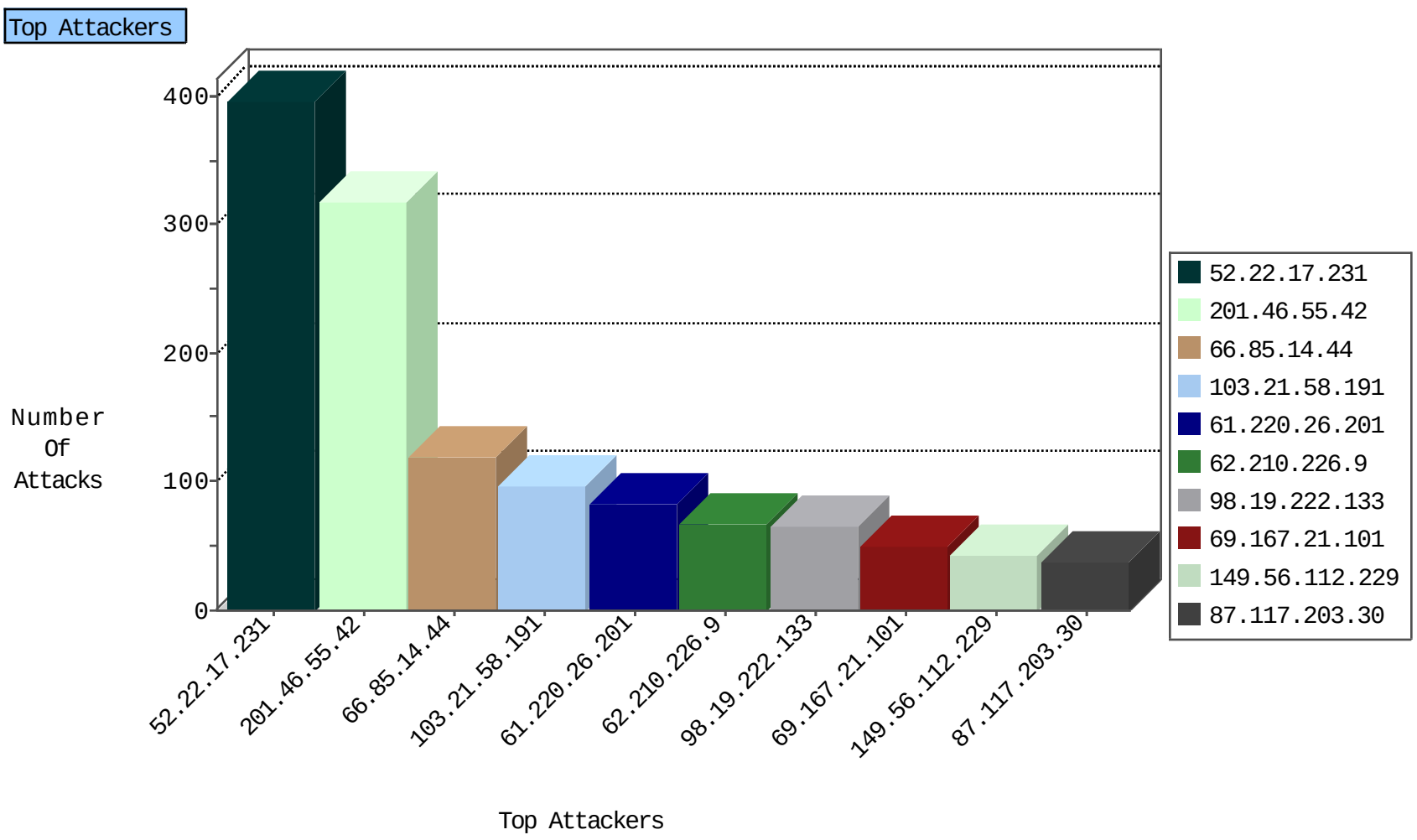
09-09-2016-03:04:04 to 09-09-2016-04:04:04

IDF Under Attack Daily Report





09-09-2016-03:04:04 to 09-09-2016-04:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
120.132.50.135	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	4
61.203.100.168	Japan	147.237.76.196	e.sviva.idf.il	Black List	drop	1
216.26.141.6	United States	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
89.248.167.131	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
216.26.141.7	United States	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-09-2016-03:04:04 to 09-09-2016-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.220.26.201	Taiwan	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	24
98.19.222.133	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	18
213.174.55.11	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
177.185.194.45	Brazil	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
87.117.203.30	United Kingdom	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
103.21.58.191	India	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
216.26.128.28	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
61.220.26.201	Taiwan	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
61.220.26.201	Taiwan	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
137.117.8.203	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	10
177.185.194.45	Brazil	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
5.196.22.55	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.172.106.100	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
103.21.58.191	India	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.117.203.30	United Kingdom	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.119	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
96.251.45.13	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
62.210.226.9	France	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
187.188.169.247	Mexico	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
103.21.58.191	India	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.26.128.28	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.130	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
97.74.215.165	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
62.210.226.9	France	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
178.18.194.186	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
97.88.198.223	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
62.210.226.9	France	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
166.62.42.29	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.19	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
193.28.95.4	Italy	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.109.242.34	United Kingdom	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
137.117.80.189	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
137.117.80.189	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
51.254.97.192	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
191.236.151.40	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
67.199.10.25	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
137.117.80.189	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
137.117.9.62	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
137.117.11.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
191.236.150.197	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
137.117.80.189	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
137.117.80.189	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
123.126.68.124	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
91.109.242.34	United Kingdom	147.237.77.216	dover.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-09-2016-03:04:04 to 09-09-2016-04:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
103.21.58.191	147.237.76.42	India	refuah.idf.il	SQL Injection - Select From	72
62.210.226.9	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	49
98.19.222.133	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	47
61.220.26.201	147.237.76.42	Taiwan	refuah.idf.il	SQL Injection - Select From	34
216.26.128.28	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	20
87.117.203.30	147.237.0.34	United Kingdom	tikshuv.idf.il	SQL Injection - Select From	20
177.185.194.45	147.237.77.226	Brazil	www.chamatz.aka.idf.il	SQL Injection - Select From	19
23.91.70.119	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
97.88.198.223	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	18
96.251.45.13	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
177.185.194.130	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
137.117.8.203	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
184.172.106.100	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
137.117.80.189	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	12
91.219.122.2	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	12
137.117.80.189	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	11
178.18.194.186	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	8
166.62.42.29	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
187.188.169.247	147.237.72.166	Mexico	aka.idf.il	SQL Injection - Select From	8
184.168.46.19	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
5.196.22.55	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	8
97.74.215.165	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
91.109.242.34	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	8
193.28.95.4	147.237.72.166	Italy	aka.idf.il	SQL Injection - Select From	6
67.199.10.25	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
191.236.151.40	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
168.1.128.51	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
77.252.26.51	147.237.76.176	Poland	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
168.1.128.51	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
137.117.9.62	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	1
168.1.128.51	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.31	Cote D'Ivoire	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
168.1.128.51	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.31	Cote D'Ivoire	nakchal.idf.il	ET SCAN NMAP -f -sS	1
168.1.128.51	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
168.1.128.51	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
168.1.128.51	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
168.1.128.51	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
77.252.26.51	147.237.76.176	Poland	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
168.1.128.51	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
137.117.11.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	1
168.1.128.51	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
45.79.103.178	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
211.141.78.56	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
168.1.128.51	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.31	Cote D'Ivoire	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
168.1.128.51	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
168.1.128.51	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
191.236.150.197	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	1
94.102.48.195	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1

09-09-2016-03:04:04 to 09-09-2016-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	28
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	25
52.22.17.231	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
52.22.17.231	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
52.22.17.231	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
185.26.180.33	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
52.22.17.231	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
52.22.17.231	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
52.22.17.231	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
52.22.17.231	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
52.22.17.231	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
52.22.17.231	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
52.22.17.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
52.22.17.231	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
52.22.17.231	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
52.22.17.231	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
83.168.250.50	Sweden	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
52.22.17.231	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.22.17.231	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.22.17.231	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.22.17.231	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.22.17.231	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.22.17.231	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.22.17.231	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.22.17.231	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
66.85.14.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.22.17.231	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
66.85.14.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
201.46.55.42	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13

09-09-2016-03:04:04 to 09-09-2016-04:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.9.142.113	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 121.9.142.113	Block	17
121.9.142.113	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	4
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
66.249.76.42	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/7/1557.jpg	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1482-he/atal.aspx	Block	1
68.180.229.190	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
121.9.142.113	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.asp	Block	1
66.249.66.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/6/1066.pdf	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/m/main/giyus/userdetails/updateuserdetails.aspx	Block	1
98.218.140.83	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/	Block	1
66.249.66.116	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/8/1548.jpg	Block	1

09-09-2016-03:04:04 to 09-09-2016-04:04:04