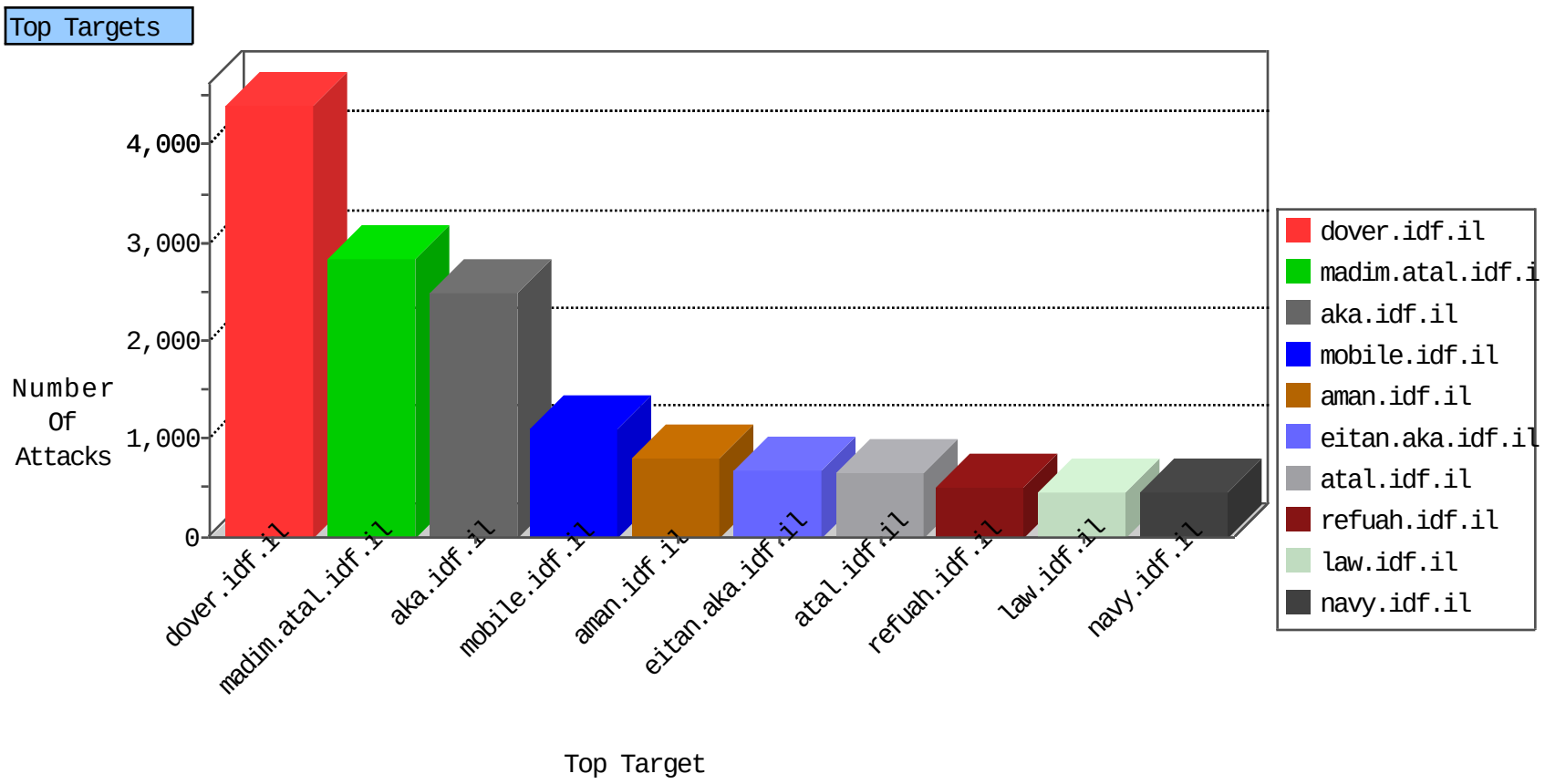
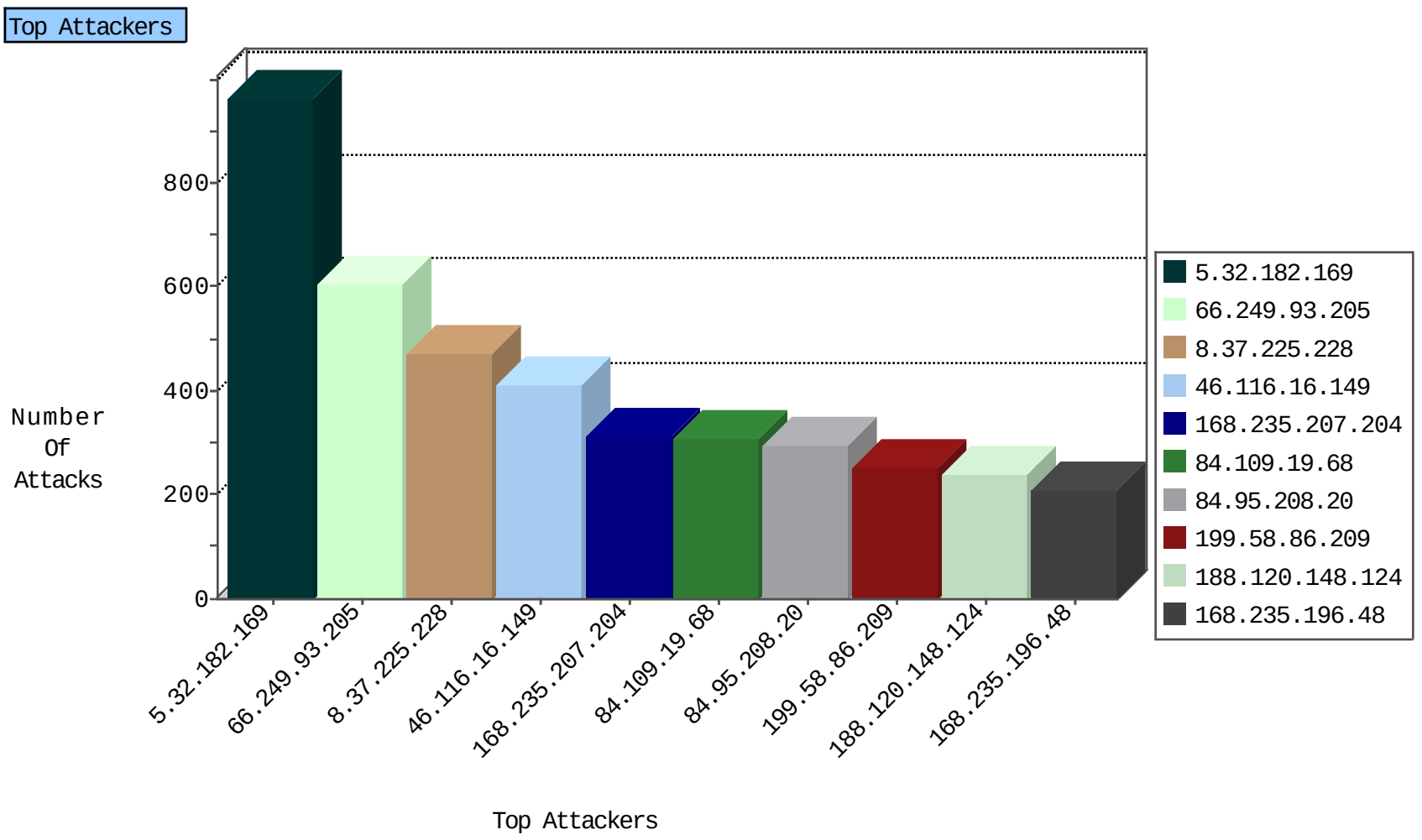
09-23-2016 to 09-24-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-23-2016 to 09-24-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.207.204	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	279
2.55.146.229	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
8.37.225.228	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	61
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	31
109.253.195.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
168.235.207.204	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
8.37.225.228	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
168.235.196.48	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	6
178.167.184.202	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
85.64.168.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Black List	drop	5
37.26.146.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
77.125.7.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
80.246.133.230	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
5.28.140.183	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
192.117.10.226	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.207.204	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
212.76.109.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
8.37.225.228	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
79.180.206.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.53.140.125	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
103.206.113.59	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
37.26.149.172	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	2
69.30.193.254	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
84.109.92.217	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
183.60.48.25	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	2
58.218.200.137	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
107.170.124.221	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
142.54.174.86	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	2
120.132.50.135	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Black List	drop	2
198.204.224.236	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
69.30.193.252	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
173.244.198.5	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
173.244.198.5	United States	147.237.76.30	himush.idf.il	Black List	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	2

09-23-2016 to 09-24-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	238
91.121.86.136	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	126
51.254.97.22	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	101
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.42	refuah.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.86	navy.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.0.34	tikshuv.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.233	atal.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.74	law.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	84
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	44
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.170	maarachot.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.176	matpash.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.167	ishurim.aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.147	chinuch.aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.0.15	kosher-kravi.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.77.226	www.chamatz.aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.31	nakchal.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.200	eitan.aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.76.39	mobile.meitav.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
5.32.182.169	Macedonia, the Former Yugoslav Republic of	147.237.72.156	aman.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	42
75.56.235.20	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	24
209.15.196.170	Canada	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	24
213.180.89.124	Sweden	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
209.15.196.170	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
23.91.70.95	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
75.56.235.20	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
94.136.40.77	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
50.63.196.229	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
213.174.55.11	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
144.76.70.248	Germany	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
61.220.26.201	Taiwan	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	11
97.74.215.197	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
69.30.210.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	9
91.121.86.136	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	9
199.58.86.209	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
23.91.70.77	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.87.23.55	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
209.15.196.170	Canada	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
188.165.250.173	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.180.89.124	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.204	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.74	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
69.7.43.246	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.170	Canada	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
123.56.155.81	China	147.237.77.170	maarachot.idf.il	C1000016: HTTP: administrator in URI	Permit	6
91.151.208.90	United Kingdom	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.96.97.203	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
64.34.186.9	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
202.124.109.87	New Zealand	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6

09-23-2016 to 09-24-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.205	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	604
75.56.235.20	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	108
66.249.73.180	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	68
209.15.196.170	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	40
209.15.196.170	147.237.77.216	Canada	dover.idf.il	SQL Injection - Select From	20
184.168.46.74	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
64.87.23.55	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	20
144.76.70.248	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	20
213.180.89.124	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	20
23.91.70.95	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
1.39.39.115	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	20
50.77.136.81	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	19
97.74.215.197	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	19
50.63.196.229	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	19
202.124.109.87	147.237.76.86	New Zealand	navy.idf.il	SQL Injection - Select From	19
195.76.149.15	147.237.77.233	Spain	atal.idf.il	SQL Injection - Select From	18
177.185.194.130	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
177.185.194.80	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
94.136.40.77	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	14
213.174.55.11	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	14
61.220.26.201	147.237.77.233	Taiwan	atal.idf.il	SQL Injection - Select From	13
23.96.97.203	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
173.198.251.2	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
69.7.43.246	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
50.63.197.9	147.237.72.166	United States	aka.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
202.124.109.87	147.237.76.42	New Zealand	refuah.idf.il	SQL Injection - Select From	8
91.151.208.90	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	8
208.52.175.27	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
168.1.80.134	147.237.77.233	Australia	atal.idf.il	SQL Injection - Select From	8
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
64.34.186.9	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
50.63.197.204	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
23.91.70.95	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
184.168.193.48	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
23.91.70.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
23.96.97.235	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
46.183.223.228	147.237.8.46	Latvia	e.chinuch.idf.il	ET SCAN Potential SSH Scan	3
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
114.95.101.31	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
82.166.92.132	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
114.95.101.31	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
185.60.88.25	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	2
128.232.110.28	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
211.197.201.106	147.237.76.39	Korea, Republic of	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
66.249.73.163	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
115.208.231.65	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
59.67.64.13	147.237.77.227	China	e.hamaz.idf.il	GPL SCAN nmap TCP	2

09-23-2016 to 09-24-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.116.16.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	412
8.37.225.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	371
192.241.170.19	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	142
87.69.119.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	112
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
168.235.207.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
168.235.207.204	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	99
213.71.171.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
168.235.196.48	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	94
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	91
13.8.125.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
84.109.4.76	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	80
8.37.225.228	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	67
223.24.41.53	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
46.117.83.50	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	62
168.235.196.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
2.53.51.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.53.42.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
5.102.242.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
109.67.222.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
79.177.231.36	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
84.108.79.234	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
168.235.196.48	United States	147.237.77.216	dover.idf.il	SYN Attack		monitor	50
77.127.22.57	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	46
77.127.22.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
27.55.12.92	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
223.24.19.235	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	39
62.0.236.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
109.67.101.145	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	36
156.111.216.113	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
156.111.216.113	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
188.120.154.65	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
37.26.149.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
2.55.13.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	32
85.130.227.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
2.55.13.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	32
2.55.13.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
85.130.227.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	31
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.139.251.236	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
85.130.227.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
110.77.203.165	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.178.204.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
77.127.22.57	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26

09-23-2016 to 09-24-2016

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.19.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	310
188.120.148.124	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	238
109.67.122.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	185
109.253.129.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	177
2.55.146.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
46.19.86.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
2.55.8.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
2.55.182.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
109.67.157.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	94
87.71.34.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	82
2.53.7.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
109.253.159.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
77.124.1.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.53.162.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
77.125.55.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
218.87.49.237	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.87.49.237	Block	37
2.53.31.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
217.132.171.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
5.29.231.35	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/templates/catalog/catalog.aspx	Block	31
80.246.138.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
77.125.68.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	23
176.13.23.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
42.123.65.19	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 42.123.65.19	Block	17
49.80.88.105	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 49.80.88.105	Block	16
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	13
77.138.174.95	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaireend.aspx	Block	13
77.139.90.231	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.9.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
2.55.156.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
77.139.240.46	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.159.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.146.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	8
109.253.157.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.94.167.80	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
109.66.155.167	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 109.66.155.167	Block	7
109.66.155.167	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	7
218.87.49.237	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
46.121.92.183	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.121.92.183	Block	6

09-23-2016 to 09-24-2016