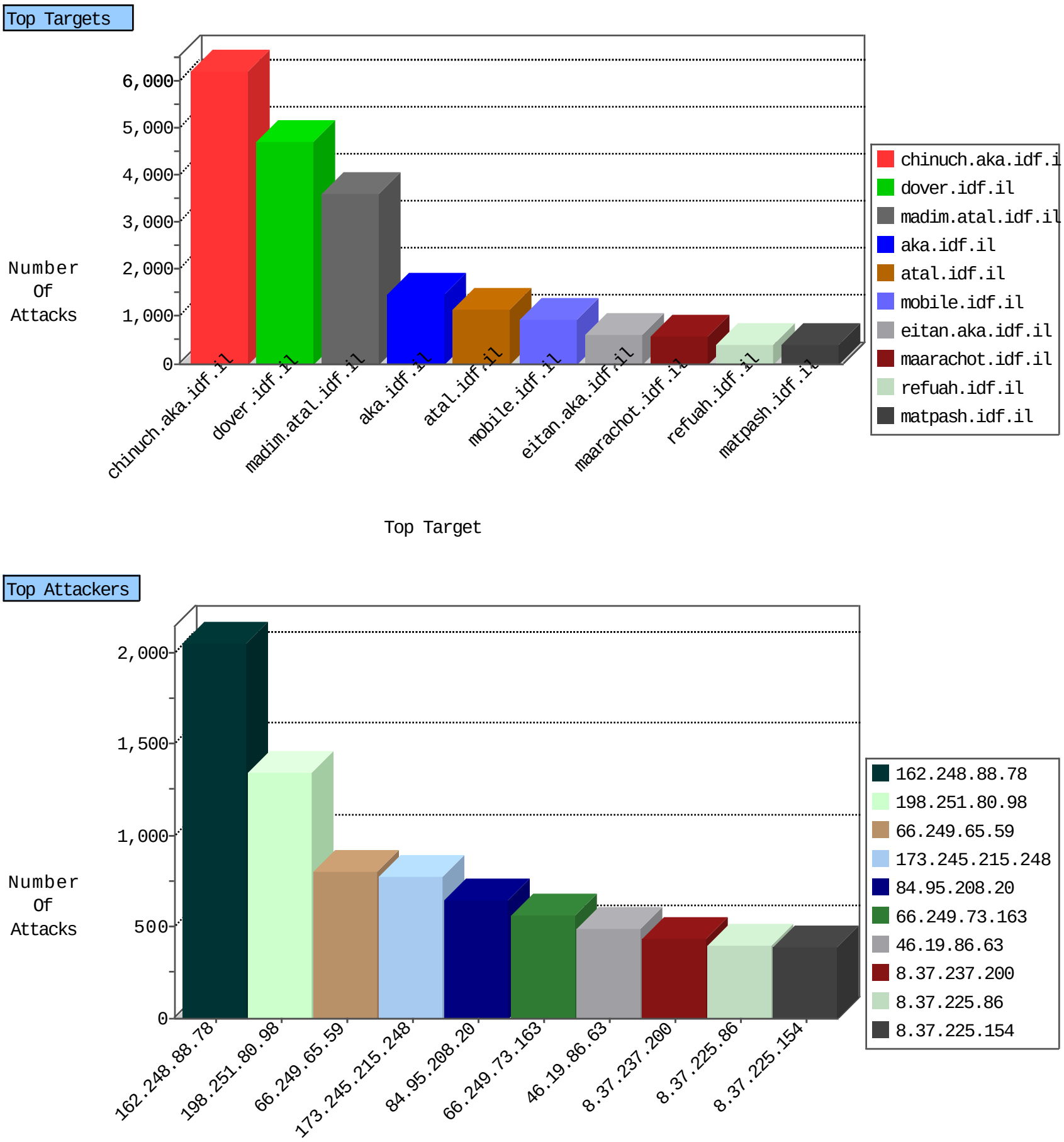
09-24-2016 to 09-25-2016

IDF Under Attack Daily Report



09-24-2016 to 09-25-2016

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	SYN Flood out of context	drop	52
8.37.231.144	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
8.37.231.144	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
168.235.197.23	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	18
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
66.249.82.81	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
176.228.130.188	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
109.67.29.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
8.37.237.200	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	7
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
128.242.249.13	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
107.170.124.221	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
168.235.197.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
198.204.224.238	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	4
68.180.231.57	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
69.30.193.250	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	4
66.102.6.19	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Black List	drop	3
2.53.136.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Black List	drop	3
8.37.231.144	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
66.249.91.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
45.35.64.142	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.197.23	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.86	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
66.249.69.232	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
157.55.39.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.154	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
63.141.242.198	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
198.204.224.234	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
168.235.197.23	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
66.102.6.21	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
63.141.242.195	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
121.86.173.9	Japan	147.237.76.197	e.himush.idf.il	Black List	drop	2
69.30.227.219	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
179.99.200.39	Brazil	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
69.30.226.219	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
173.208.197.205	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
198.204.224.235	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
46.19.85.146	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
63.141.242.198	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
63.141.242.196	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
63.141.231.214	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2

09-24-2016 to 09-25-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.211.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	184
5.9.85.4	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	156
95.91.45.174	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	78
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	69
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	66
5.9.85.4	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	49
95.91.45.174	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	39
5.9.85.4	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	32
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	32
95.91.45.174	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	31
163.172.49.61	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	26
5.9.85.4	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	24
162.210.196.100	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	24
162.210.196.100	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	8
163.172.49.61	United Kingdom	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	8
163.172.49.61	United Kingdom	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	7
69.30.211.2	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	7
46.243.173.2	Russian Federation	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
62.149.132.179	Italy	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.33	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
162.210.196.100	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	6
95.91.45.174	Germany	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	6
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6
95.91.45.174	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
106.38.241.106	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
95.91.45.174	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	4
95.91.45.174	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	4
51.254.97.218	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
173.234.159.250	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
95.91.45.174	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.209	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
163.172.49.61	United Kingdom	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
142.54.184.90	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
51.254.97.218	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	2
163.172.49.61	United Kingdom	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
5.9.62.130	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
188.135.45.237	Oman	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
51.254.131.243	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.100	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.116.197	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-24-2016 to 09-25-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.65.59	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	803
66.249.73.163	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	563
66.249.64.112	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	97
46.243.173.2	147.237.77.216	Russian Federation	dover.idf.il	SQL Injection - Select From	56
79.178.242.28	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	31
62.149.132.179	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	8
184.168.27.33	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
185.120.124.1	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
197.253.242.144	147.237.77.216	Morocco	dover.idf.il	GPL SCAN nmap TCP	4
188.135.45.237	147.237.77.216	Oman	dover.idf.il	SQL Injection - Select From	3
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	3
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	3
220.82.87.133	147.237.8.50	Korea, Republic of	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
93.70.141.81	147.237.76.196	Italy	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
78.129.171.173	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
218.103.242.29	147.237.76.202	Hong Kong	e.halag.idf.il	ET SCAN Potential SSH Scan	2
93.70.141.81	147.237.76.44	Italy	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
78.97.159.124	147.237.0.33	Romania	idf.il	ET SCAN Potential SSH Scan	2
93.70.141.81	147.237.76.39	Italy	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	2
93.70.141.81	147.237.77.212	Italy	e.dover.idf.il	ET SCAN Potential SSH Scan	2
202.112.38.190	147.237.0.19	China	madim.atal.idf.il	GPL SCAN nmap TCP	2
91.224.118.2	147.237.77.61	Poland	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
218.103.242.29	147.237.77.216	Hong Kong	dover.idf.il	ET SCAN Potential SSH Scan	2
218.103.242.29	147.237.77.179	Hong Kong	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.158	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.171	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
27.72.57.38	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	2
218.103.242.29	147.237.77.19	Hong Kong	law-forum.idf.il	ET SCAN Potential SSH Scan	2
87.71.32.58	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	2
59.59.254.132	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
218.103.242.29	147.237.76.42	Hong Kong	refuah.idf.il	ET SCAN Potential SSH Scan	2
62.210.111.84	147.237.77.216	France	dover.idf.il	Xenu Link Sleuth User Agent	2
222.186.56.199	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
78.129.171.173	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential SSH Scan	2
211.197.201.106	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
93.70.141.81	147.237.76.200	Italy	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
218.103.242.29	147.237.77.74	Hong Kong	law.idf.il	ET SCAN Potential SSH Scan	2
82.76.111.239	147.237.76.200	Romania	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
61.131.58.91	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
139.162.187.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
14.220.65.204	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.191.55.97	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
195.143.227.35	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.221	147.237.76.39	Switzerland	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
117.169.85.170	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

09-24-2016 to 09-25-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
162.248.88.78	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2050
173.245.215.248	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	776
8.37.225.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	347
8.37.225.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	335
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	332
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	314
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	311
8.37.237.200	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	243
213.249.217.237	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	232
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	219
72.184.165.61	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	215
108.227.93.208	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	192
141.226.218.74	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	189
8.37.237.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	187
69.131.82.83	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	158
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	158
65.190.132.85	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	156
70.57.232.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	141
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
80.246.130.102	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	121
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
141.0.14.147	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
41.111.0.252	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
8.37.231.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
141.0.14.216	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
46.19.85.80	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
2.53.147.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
109.67.143.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
141.0.14.147	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	60
187.190.28.190	Mexico	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	59
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
109.66.33.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
77.139.51.23	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
8.37.225.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	50
8.37.225.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	49
176.13.20.231	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
92.241.53.150	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
172.56.29.251	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	45
192.116.94.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
8.37.231.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	44
168.235.197.23	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	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
75.115.184.185	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	39
216.52.148.4	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
31.18.255.36	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
68.170.254.21	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	35
141.0.14.216	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	32
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
5.102.242.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	494
213.57.146.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	339
79.180.48.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	287
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	194
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	163
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
2.55.168.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
46.210.144.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	136
109.67.164.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
46.117.2.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
46.19.85.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	91
46.120.69.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
185.120.125.132	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	74
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	73
79.177.3.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.253.194.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
5.102.207.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
84.108.232.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
37.26.146.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
2.53.183.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
176.13.229.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
46.116.45.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
77.127.18.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.116.70.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
176.228.169.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
89.139.117.216	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	30
37.26.149.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	26
185.32.179.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
46.116.117.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	22
79.176.143.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
185.120.125.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	17
182.42.52.199	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 182.42.52.199	Block	17
36.248.165.83	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 36.248.165.83	Block	16
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	14
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
87.71.42.63	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
85.64.36.132	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 85.64.36.132	Block	10
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	10
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	9

09-24-2016 to 09-25-2016