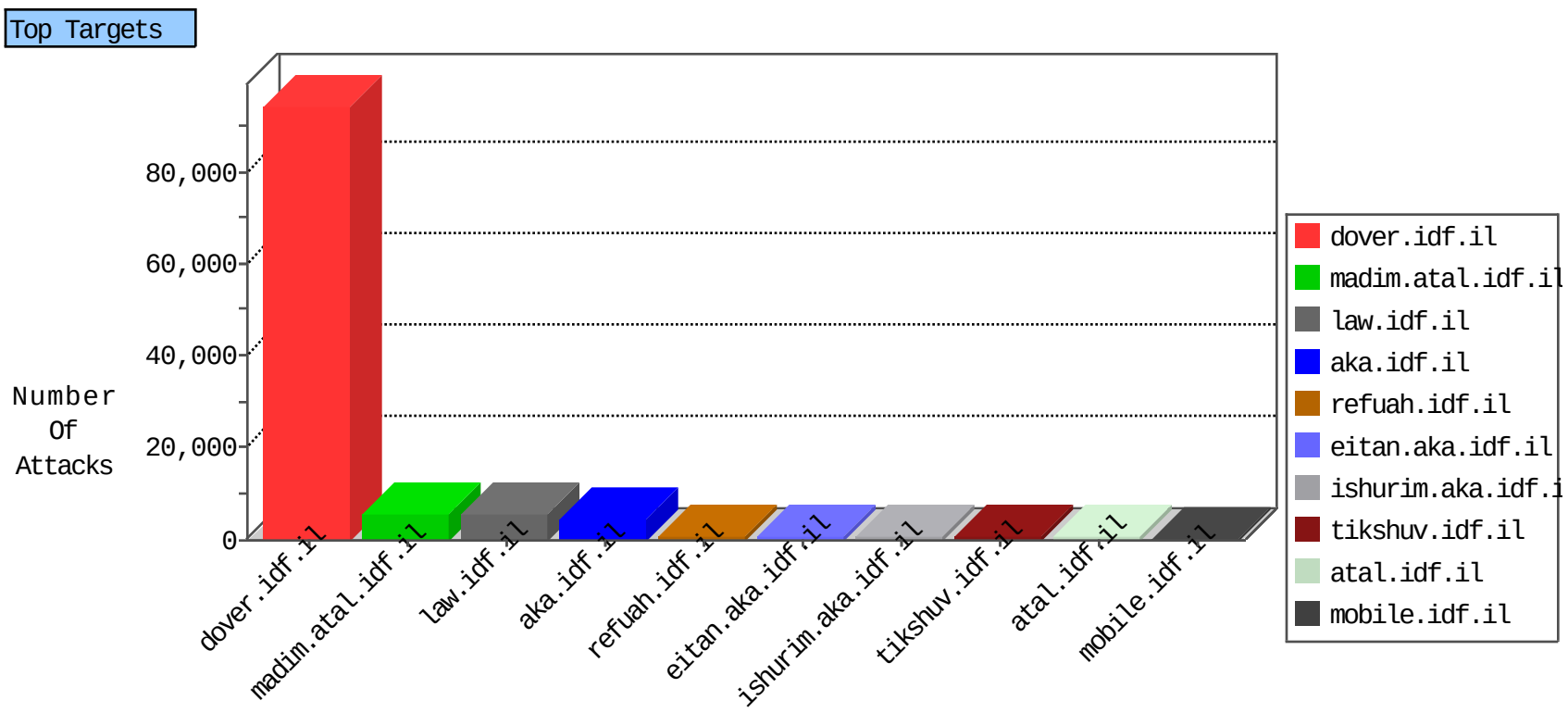
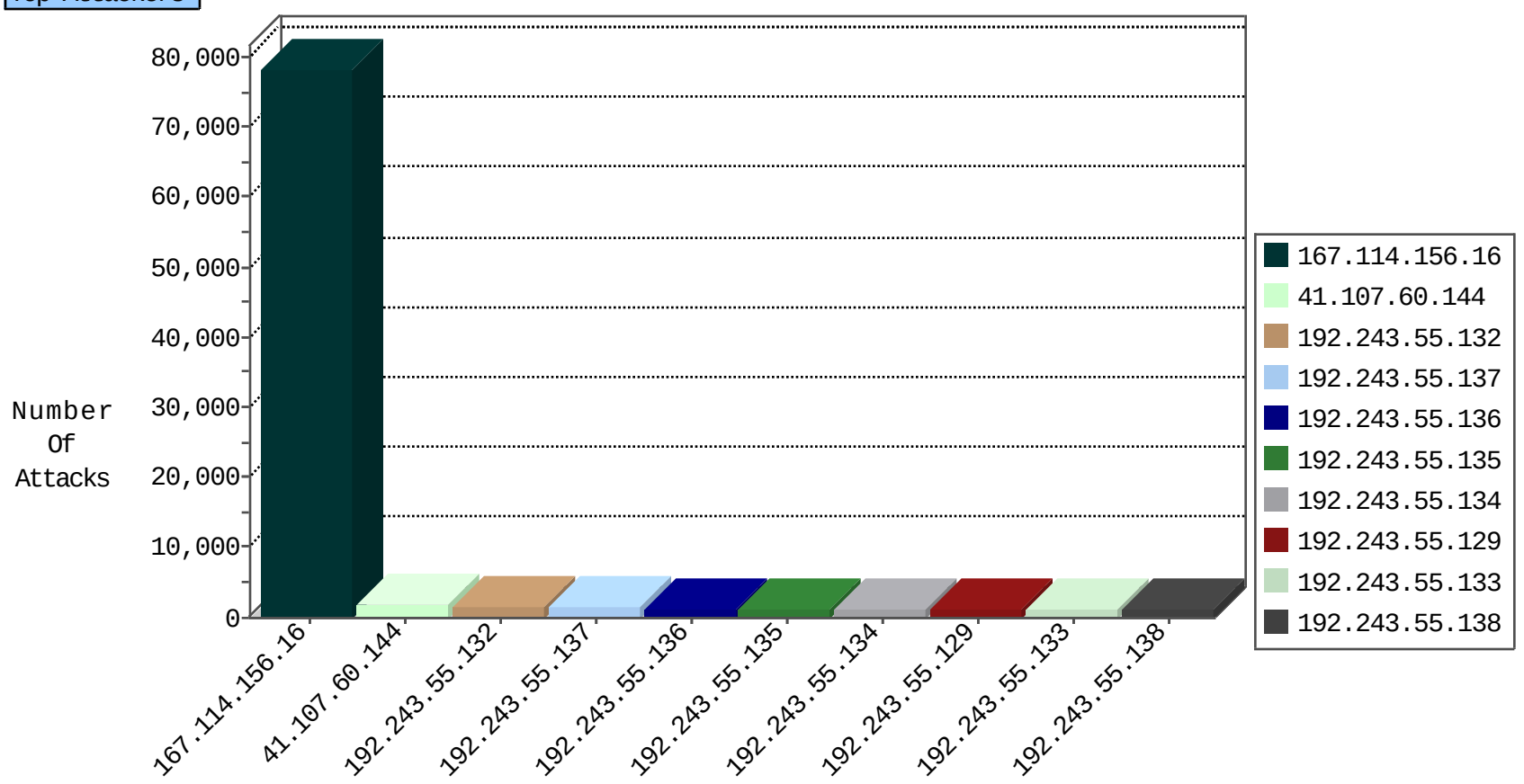
04-12-2016 to 04-13-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-12-2016 to 04-13-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	78403
41.105.118.160	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	5071
24.130.213.84	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4245
180.249.208.112	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2848
192.243.55.136	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2713
147.236.27.99	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2384
192.243.55.138	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2004
80.246.137.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1854
109.160.221.9	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1536
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1511
212.116.163.73	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1497
89.139.146.140	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1363
199.203.83.190	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1237
79.177.243.31	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1217
41.107.2.205	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1031
109.253.199.140	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	917
79.177.137.251	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	906
93.173.15.244	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	895
197.116.94.11	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	827
162.243.37.178	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	813
31.168.4.242	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	714
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	690
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	676
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	656
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	621
211.28.223.175	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	586
170.24.136.3	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	527
2.55.32.191	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	513
46.19.86.236	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	469
192.243.55.132	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	460
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	450
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	443
193.43.246.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	417
37.38.138.254	Kuwait	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	390
2.53.5.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	382
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	301
176.13.12.131	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	251
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	246
84.109.60.144	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	182
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	179
216.72.40.186	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	176
79.180.197.110	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	159
197.116.94.11	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	145
125.16.3.251	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	131
192.115.177.203	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	124
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	103
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	98
81.218.125.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	97
46.19.86.48	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	96
192.114.3.241	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	79

04-12-2016 to 04-13-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	25
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	24
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
5.29.16.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	18
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	17
61.135.189.98	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	17
84.228.16.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
84.108.129.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
89.138.115.14	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
217.132.33.254	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
2.53.40.43	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
95.91.75.31	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	12
213.57.231.142	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
95.91.75.31	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	9
87.71.44.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
217.132.112.131	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
192.114.5.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
157.55.39.215	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.78.168.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
95.91.75.31	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	7
23.91.70.121	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
46.19.85.7	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
85.65.99.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.85.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.7	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.176.88.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
95.91.75.31	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	6
80.246.130.122	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.121.124.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.180.7.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
31.210.187.34	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
23.91.70.121	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
46.120.3.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
212.117.143.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
31.154.41.17	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
46.116.15.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
103.3.173.97	Malaysia	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
209.15.196.171	Canada	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.143.34.37	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
2.53.34.112	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
194.90.153.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
41.185.31.40	South Africa	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
94.188.248.78	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
144.76.29.66	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
23.91.70.77	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
212.143.54.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4

04-12-2016 to 04-13-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	69
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	52
23.91.70.121	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	29
66.102.9.81	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	27
177.79.41.77	147.237.77.216	Brazil	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
103.3.173.97	147.237.77.74	Malaysia	law.idf.il	SQL Injection - Select From	24
66.96.128.60	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	17
66.249.93.74	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	14
63.143.34.37	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	12
80.246.130.215	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
46.19.85.87	147.237.76.42	Israel	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	9
209.15.196.171	147.237.72.166	Canada	aka.idf.il	SQL Injection - Select From	6
23.91.70.77	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
91.219.122.4	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	6
41.185.31.40	147.237.77.216	South Africa	dover.idf.il	SQL Injection - Select From	6
213.246.49.97	147.237.77.74	France	law.idf.il	SQL Injection - Select From	5
66.249.93.109	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	4
80.246.136.81	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
66.249.78.86	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.93.79	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	4
192.243.55.133	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	3
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
89.163.212.37	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.44	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
91.228.248.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
192.116.83.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
109.253.139.15	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
61.94.23.143	147.237.77.216	Indonesia	dover.idf.il	Tehila - Perl LWP with fake user agent	2
185.32.179.53	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
176.13.4.137	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
89.163.212.37	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
208.100.26.228	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.139.15	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
64.233.172.171	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
89.163.212.37	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential SSH Scan	2
77.125.84.30	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
208.100.26.228	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
163.172.140.23	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	2
176.13.4.137	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
89.163.212.37	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.18	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	2
88.204.187.90	147.237.0.19	Kazakstan	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
198.20.69.98	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
79.178.5.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.245.78.52	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.84.149.32	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
113.59.33.61	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 2048	1
89.163.212.37	147.237.77.170	Germany	maarachot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.76.44	Lithuania	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

04-12-2016 to 04-13-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	964
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	606
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	254
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	220
207.46.13.74	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	212
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	201
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	198
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop		drop	190
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	187
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	169
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	163
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	162
109.66.29.177	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	161
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	160
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	158
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	157
192.243.55.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	153
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	152
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	150
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	146
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	145
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	144
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	142
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	142
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	141
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	139
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	136
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	135
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	133
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	132
192.243.55.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	131
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	130
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	129
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	127
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	126
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	126
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	125
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	123
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	121
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
84.228.16.249	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	114
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	111
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	110
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	110
192.243.55.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	109
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	109

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.105.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	423
2.53.152.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	410
80.246.136.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	352
2.55.6.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	272
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	222
79.178.17.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	217
109.253.139.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	198
46.19.86.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	193
46.116.12.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	178
176.13.16.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	171
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	163
2.53.17.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
176.13.12.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
37.26.147.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
2.55.187.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	135
109.253.140.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
46.19.86.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
89.139.172.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
109.253.128.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
80.246.136.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
185.32.179.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
176.13.8.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	89
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
80.246.136.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
176.13.21.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
2.53.17.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
176.13.1.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
2.53.62.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.253.200.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
109.253.206.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
2.53.175.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
109.253.203.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	60
79.183.39.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
176.13.17.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
176.13.2.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
2.53.169.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	25
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
37.26.149.218	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 37.26.149.218	Block	23
176.13.14.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
176.13.5.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21

04-12-2016 to 04-13-2016