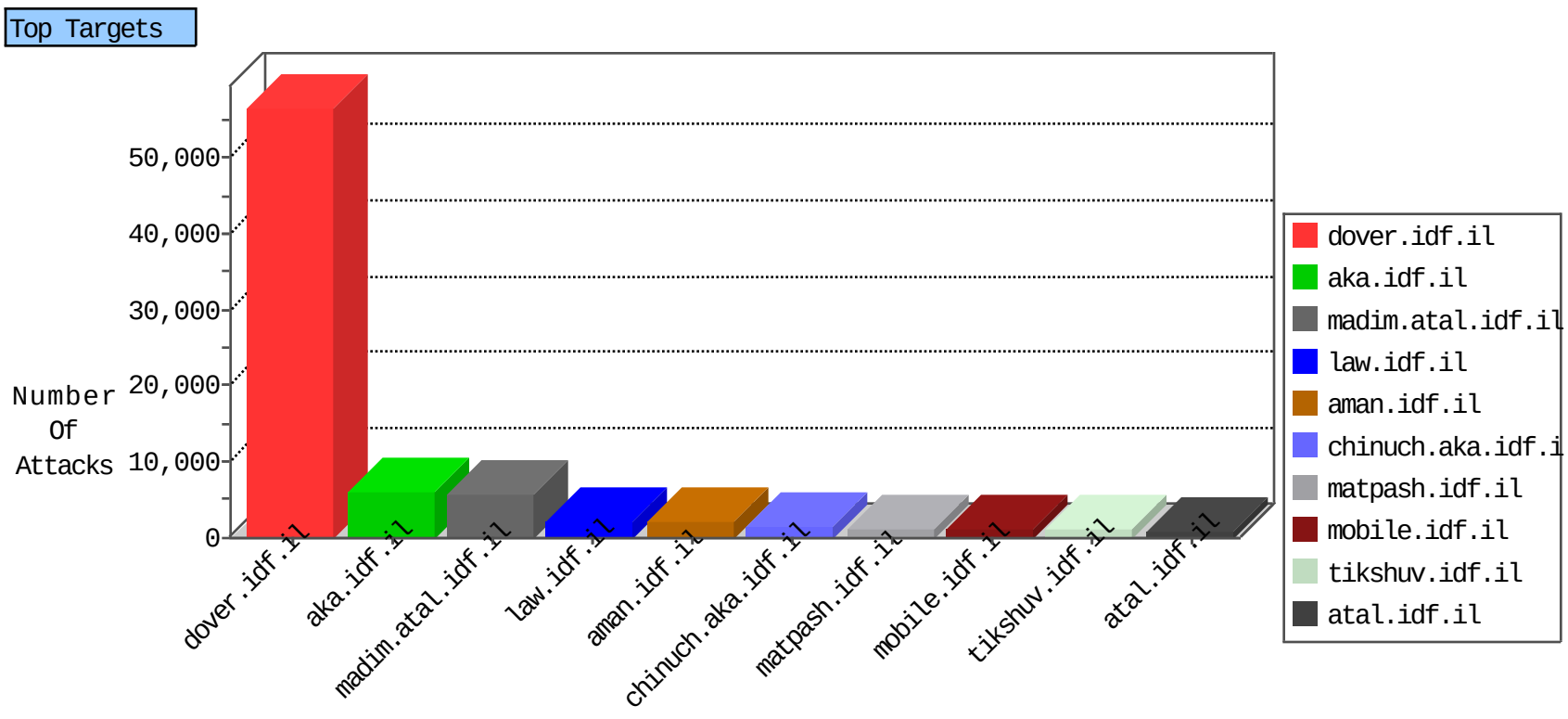
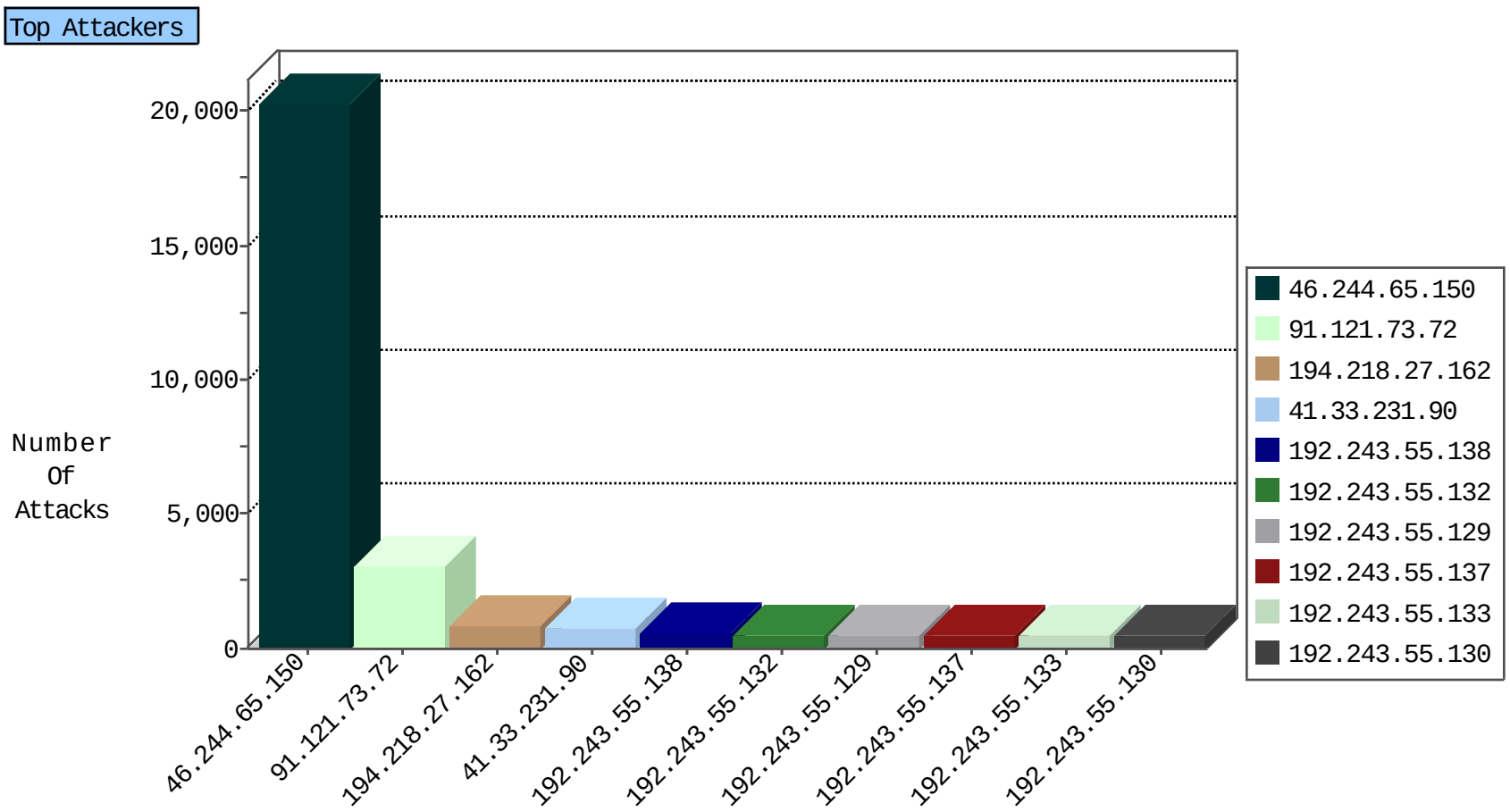
03-03-2016 to 03-04-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-03-2016 to 03-04-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
247.245.0.129		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35637
67.228.197.144	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34709
211.93.245.246	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34631
53.112.78.3	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34499
62.121.106.1	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34481
70.158.115.121	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34431
183.136.192.39	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34275
219.1.32.108	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34237
96.118.141.93	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34232
143.179.246.229	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34226
35.224.81.109	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34143
235.160.48.137		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34051
71.137.4.198	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34026
81.253.158.72	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34003
40.235.148.183	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33991
21.3.68.85	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33967
213.47.43.83	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33944
128.72.14.215	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33931
119.91.255.205	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33929
41.189.107.65	Cote D'Ivoire	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33819
16.162.182.64	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33815
110.229.47.48	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33792
78.248.155.57	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33729
143.229.217.226	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33697
126.129.58.140	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33665
185.97.171.49		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33632
234.50.138.170		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33597
174.94.38.245	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33594
152.5.171.203	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33548
123.185.202.128	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33538
129.184.14.229	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33512
40.56.236.94	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33509
198.62.94.25	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33485
117.239.154.30	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33450
44.160.227.123	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33440
16.116.98.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33377
77.100.85.151	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33277
189.146.197.55	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33274
245.75.245.112		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33218
250.4.89.191		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33181
116.97.148.204	Vietnam	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33173
220.9.46.74	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33139
96.177.88.85	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33108
253.63.65.129		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33107
207.40.246.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33093
118.171.230.101	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33045
89.65.161.183	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33023
29.120.175.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32966
2.2.134.106	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32964
148.239.24.106	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32947

03-03-2016 to 03-04-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	42
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	26
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	25
79.177.25.69	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
79.180.153.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
2.54.132.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
61.135.189.119	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	15
81.218.56.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.64.66.156	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
37.142.199.57	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
37.142.210.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
5.29.150.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.116.200.0	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
176.228.30.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
2.52.44.93	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.142.68.88	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.176.177.186	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.179.31.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
109.64.5.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
119.97.146.76	China	147.237.0.34	tikshuv.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	8
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.57.34.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
132.66.233.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
157.55.39.179	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
2.52.39.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.52.48.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.161	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
77.125.2.174	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.133.0	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.68.251.254	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.70.84.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
176.13.7.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
192.116.55.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.117.104.113	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.181.183.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
85.64.181.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
2.52.32.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.142.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.142.161.146	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.178.31.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4

03-03-2016 to 03-04-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.75	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	307
66.249.93.234	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	138
209.66.70.253	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	25
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	16
80.230.25.10	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	13
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
185.32.179.250	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
66.249.93.127	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
66.249.66.105	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
213.136.91.26	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
93.113.125.11	147.237.0.200	Romania	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
79.180.8.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
61.153.237.122	147.237.76.148	China	gqcenter.aka.idf.il	GPL SCAN nmap TCP	2
216.227.58.7	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -f -sS	2
188.120.148.148	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.74.96	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
109.253.194.235	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.109	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
112.204.24.124	147.237.77.216	Philippines	dover.idf.il	portscan: TCP Distributed Portscan	2
119.97.146.76	147.237.0.34	China	tikshuv.idf.il	ET WEB_SERVER Muieblackcat scanner	2
82.221.48.130	147.237.76.42	Iceland	refuah.idf.il	Tehila - Perl LWP with fake user agent	2
185.120.125.27	147.237.72.166		aka.idf.il	ET SCAN NMAP -sA (2)	2
216.227.58.7	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	2
82.117.208.243	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
209.126.116.147	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
188.120.157.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.79.108	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sA (2)	2
109.253.194.235	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
60.12.88.242	147.237.76.148	China	gqcenter.aka.idf.il	GPL SCAN nmap TCP	2
198.20.69.74	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	2
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
185.72.179.221	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.118	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
1.62.116.156	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
212.116.184.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.19.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
175.99.87.209	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.146.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.134.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-03-2016 to 03-04-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1229
91.121.73.72	France	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1229
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	738
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	515
91.121.73.72	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	264
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	260
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	215
79.181.207.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	197
149.78.150.154	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	175
79.182.28.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	165
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
2.54.167.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	134
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	96
87.71.14.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	90
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	89
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	83
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	82
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	79
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	78
80.246.133.224	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	78
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	78
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	72
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	69
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	68
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	67
37.46.39.223	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	65
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	64
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	64
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	63
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	63
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	63
31.168.195.36	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	61
79.181.229.213	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	60
79.181.153.32	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	60
176.13.22.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
212.179.218.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	59
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	59
46.19.85.26	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	59
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	59
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	59
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	57
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.25.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	337
79.178.147.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	328
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	256
37.26.148.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	179
109.253.139.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	173
109.253.209.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	171
2.52.144.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
46.19.86.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
212.199.151.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
109.253.133.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	159
185.32.179.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	156
185.32.179.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	155
109.253.136.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	152
46.19.85.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	147
176.13.18.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
213.8.129.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	140
185.32.179.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	134
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
37.26.149.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
2.54.153.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
94.159.170.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
109.253.205.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
87.70.64.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
2.54.190.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
46.19.86.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
176.13.11.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
79.178.147.104	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	60
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	52
132.70.66.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
37.26.149.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
109.64.116.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
176.13.22.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
2.54.157.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
109.253.198.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
173.208.136.170	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	40
109.160.151.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
176.13.7.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
37.26.147.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.28.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.166.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.9.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	28
2.52.172.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28

03-03-2016 to 03-04-2016