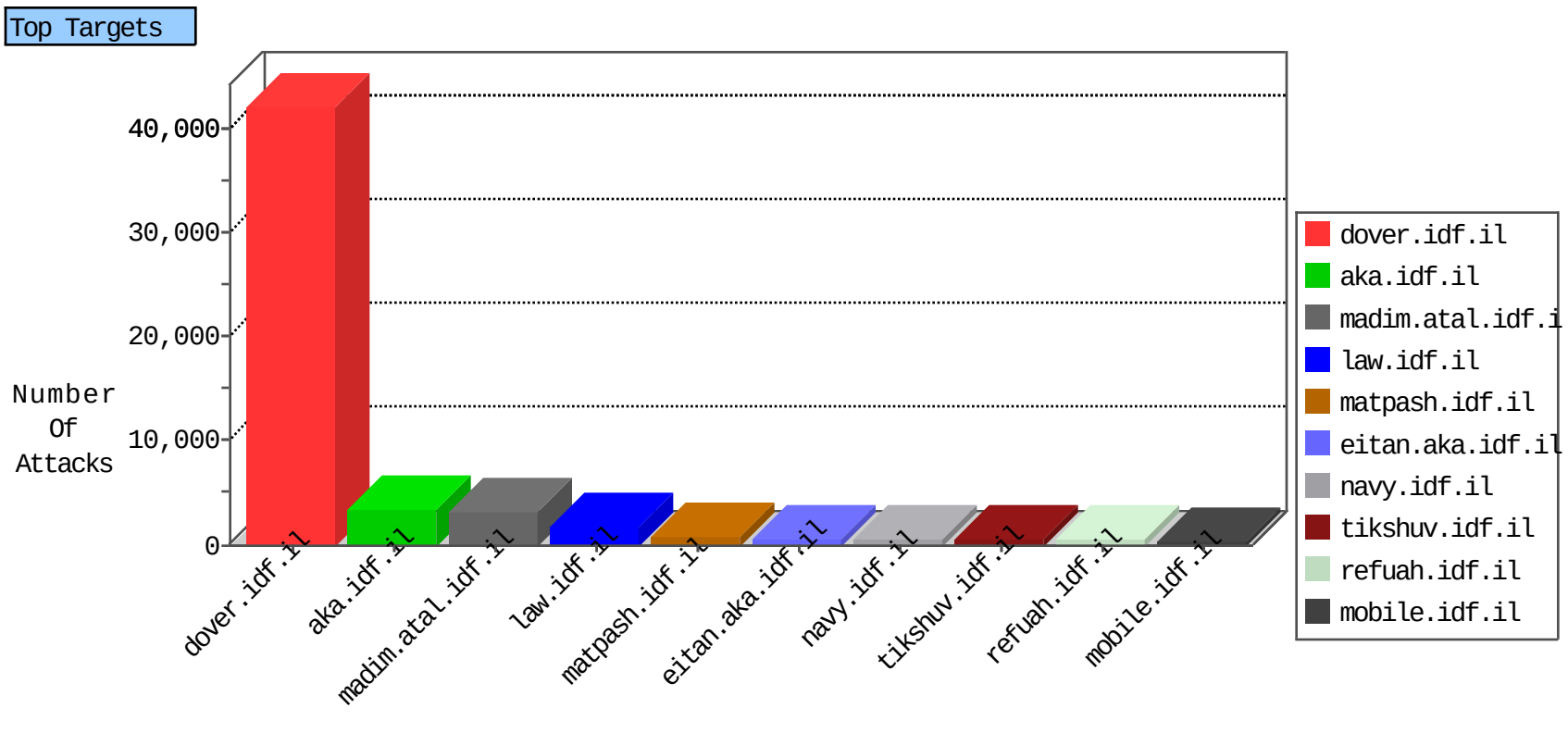
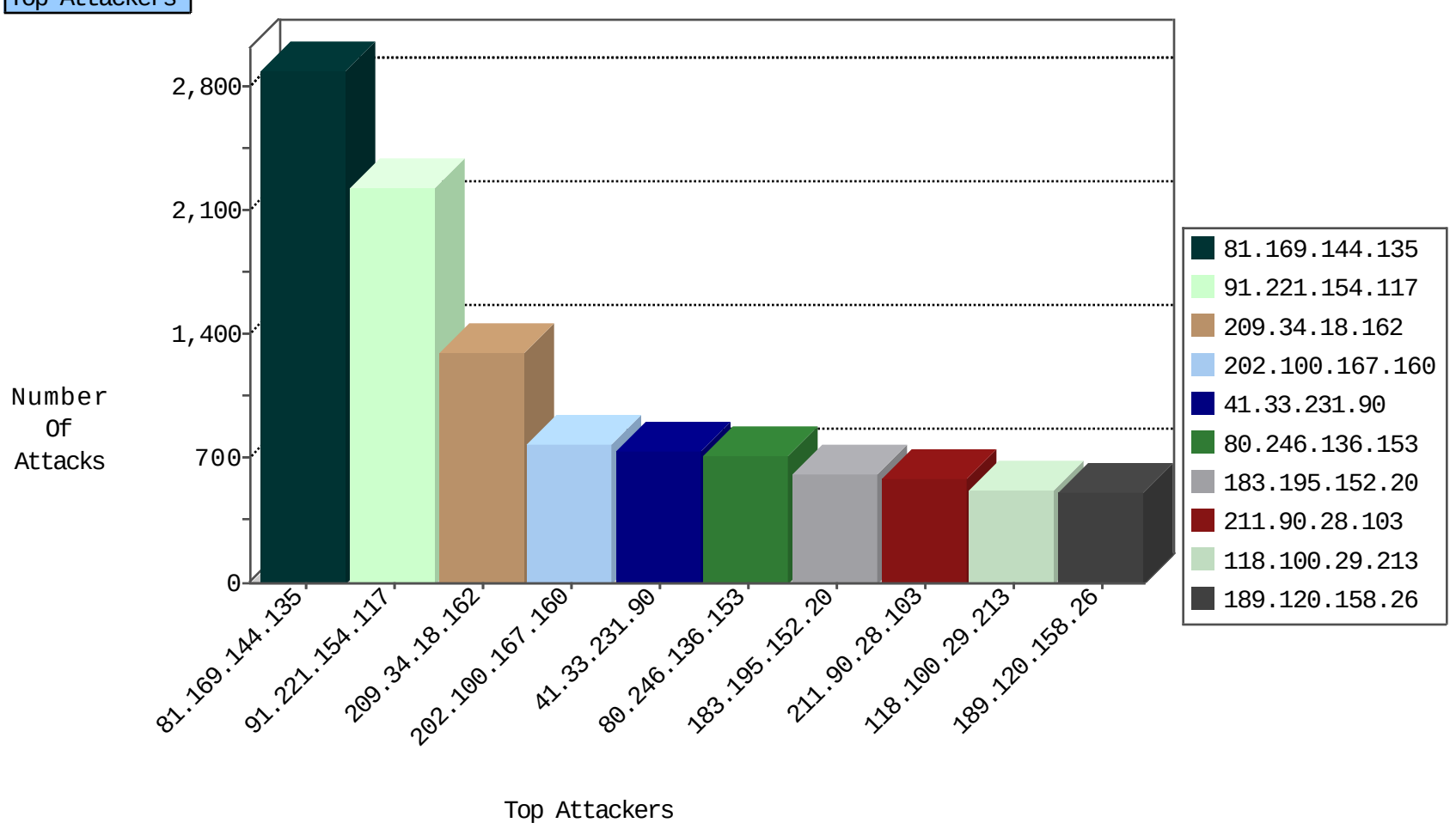
02-19-2016 to 02-20-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-19-2016 to 02-20-2016

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	network flood IPv4 TCP-RST	drop	2232783
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	785548
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	436898
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	367036
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	147189
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	92685
220.181.108.155	China	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	2834
208.109.97.62	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	611
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	380
217.132.39.5	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	208
202.100.167.137	China	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	208
189.113.135.230	Brazil	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	207
69.31.51.7	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	202
217.132.39.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	171
113.183.192.247	Vietnam	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	120
212.106.4.68	Poland	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	108
202.100.167.160	China	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	107
122.129.79.89	Pakistan	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	106
43.243.112.77	Japan	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	106
113.107.57.76	China	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	104
94.75.214.129	Netherlands	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	104
202.100.167.169	China	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	103
88.32.124.83	Italy	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	102
64.20.48.83	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	102
84.111.65.196	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	95
79.182.168.253	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	71
118.100.29.213	Malaysia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	70
64.16.194.70	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	61
115.160.137.139	Hong Kong	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	56
46.117.70.27	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	49
120.52.72.30	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	48
191.250.41.161	Brazil	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	48
91.227.71.250	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	47
180.250.163.34	Indonesia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	46
113.167.19.135	Vietnam	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	45
111.47.13.2	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	42
14.176.64.197	Vietnam	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	39
79.176.11.142	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	36
213.128.81.82	Turkey	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34
5.13.199.244	Romania	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	33
212.34.12.62	Jordan	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	33
107.150.24.9	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	32
41.137.57.49	Morocco	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	32
62.219.225.194	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	29
91.221.154.117	Ukraine	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
85.65.131.225	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
185.95.255.42		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
41.137.57.49	Morocco	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	26
183.195.152.20	China	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25

02-19-2016 to 02-20-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.48.202	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	29
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	25
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	24
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
81.218.143.185	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
5.29.98.229	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
184.106.114.136	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
184.106.114.136	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
77.127.221.29	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	9
184.106.114.136	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
46.19.85.131	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
184.173.233.226	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.106.114.136	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
84.110.145.254	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
177.185.194.47	Brazil	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.106.114.136	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	7
184.106.114.136	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	6
79.182.207.81	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
2.54.167.81	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.33	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
85.250.111.222	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
77.126.209.51	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
109.64.214.104	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
46.19.85.43	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
149.88.113.120	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
209.15.196.171	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
64.87.23.55	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C1000023: HTTP: administrator in URI	Block	4
213.8.145.99	Israel	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
97.88.198.223	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.168.219.174	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	4
46.116.44.175	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
184.173.233.226	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.194.47	Brazil	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.135.63.82	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.194.47	Brazil	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
212.179.42.225	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
46.121.208.77	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
40.77.167.25	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	3
84.108.186.43	Israel	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	3
87.71.7.15	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	3
80.246.133.222	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	3
109.66.38.28	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	3
213.8.10.16	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
109.253.205.148	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
172.86.83.125		147.237.76.42	refuah.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	2

02-19-2016 to 02-20-2016

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	89
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	77
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	29
184.106.114.136	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	26
184.106.114.136	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	26
177.185.194.47	147.237.76.31	Brazil	nakchal.idf.il	SQL Injection - Select From	18
37.26.146.145	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	14
184.173.233.226	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	14
80.246.130.71	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	14
213.8.145.99	147.237.77.74	Israel	law.idf.il	SQL Injection - Select From	12
108.168.219.174	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	12
82.205.21.59	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP login.htm access	7
209.15.196.171	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	6
82.205.21.59	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP admin.php access	6
97.88.198.223	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
64.87.23.55	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
80.246.136.153	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
66.135.63.82	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
66.249.81.148	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
120.192.21.7	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -f -sS	4
120.192.21.7	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 2048	4
80.246.133.102	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
82.205.21.59	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP adminlogin access	3
66.102.9.91	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
115.236.75.201	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	2
218.246.0.97	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
61.149.161.186	147.237.76.148	China	gqcenter.aka.idf.il	GPL SCAN nmap TCP	2
66.249.66.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	2
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.102.9.107	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.144	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.240	147.237.76.201		e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
121.207.226.199	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.30.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.211.184.107	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
194.50.116.104	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.236.120.129	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.93.185.246	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
37.230.212.25	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.230.110.51	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
146.185.250.105	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.198.127.173	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
106.187.90.86	147.237.76.30	Japan	himush.idf.il	GPL SCAN superscan echo	1
198.20.69.74	147.237.77.226	United States	www.chamatz.aka.idf.il	ET DROP Dshield Block Listed Source	1

02-19-2016 to 02-20-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
81.169.144.135	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2847
91.221.154.117	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2181
209.34.18.162	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1298
202.100.167.160	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	719
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	692
183.195.152.20	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	563
211.90.28.103	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	509
189.120.158.26	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	489
118.100.29.213	Malaysia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	425
54.173.9.10	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	390
60.29.248.142	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	354
180.250.163.34	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	297
92.53.7.9	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	269
119.30.240.199	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	218
118.97.66.2	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	216
202.100.167.142	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	201
185.128.36.42		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	191
120.52.72.47	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	190
52.5.133.46	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	188
126.120.61.44	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	171
132.71.170.7	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	168
202.100.167.170	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	165
194.90.116.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	158
120.52.72.19	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
113.183.192.247	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	151
120.198.244.29	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	150
79.120.72.222	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	141
109.160.132.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
14.12.36.0	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	140
124.192.88.182	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	135
124.192.214.181	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
124.193.23.158	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	125
104.245.99.228		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	120
198.12.82.102	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	120
23.94.191.234	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	120
37.26.146.155	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
70.39.186.79	Satellite Provider	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
70.39.187.150	Satellite Provider	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
124.192.88.182	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
177.124.215.130	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
69.7.227.159	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	113
70.39.186.79	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
14.181.22.39	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
124.192.163.7	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	102
113.167.19.135	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
124.192.163.7	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
14.12.36.0	Japan	147.237.77.216	dover.idf.il	SYN Attack		reject	100
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	100
70.39.187.150	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
116.105.164.225	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	410
2.54.189.177	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.189.177	Block	252
84.94.33.117	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.94.33.117	Block	203
80.246.136.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
2.54.189.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	134
80.246.136.153	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 80.246.136.153	Block	133
84.94.33.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	129
5.28.179.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	122
5.28.179.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
2.54.189.177	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.189.177	Block	102
149.50.97.245	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
85.65.106.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
80.179.109.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
85.65.106.69	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.65.106.69	Block	81
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 82.205.21.59	Block	67
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.205.21.59	Block	63
46.19.86.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
176.13.9.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
149.88.213.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
89.138.177.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
149.50.97.245	United States	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 149.50.97.245	Block	52
2.54.39.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
84.110.144.118	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
79.176.11.142	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.11.142	Block	44
79.178.147.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
82.205.21.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	41
5.28.179.81	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 5.28.179.81	Block	39
109.253.138.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
80.179.109.2	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.179.109.2	Block	36
176.13.14.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
109.160.160.138	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.160.138	Block	33
46.116.44.175	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
2.52.179.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
109.253.201.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
197.38.197.170	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	20
197.38.197.170	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	20
37.26.146.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
5.29.75.248	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.75.248	Block	15
87.69.178.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
79.181.236.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
79.177.96.230	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.96.230	Block	12
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	12
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
69.31.51.7	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
80.246.137.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
37.26.146.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.13.17.224	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	9
87.70.43.59	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	9
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9