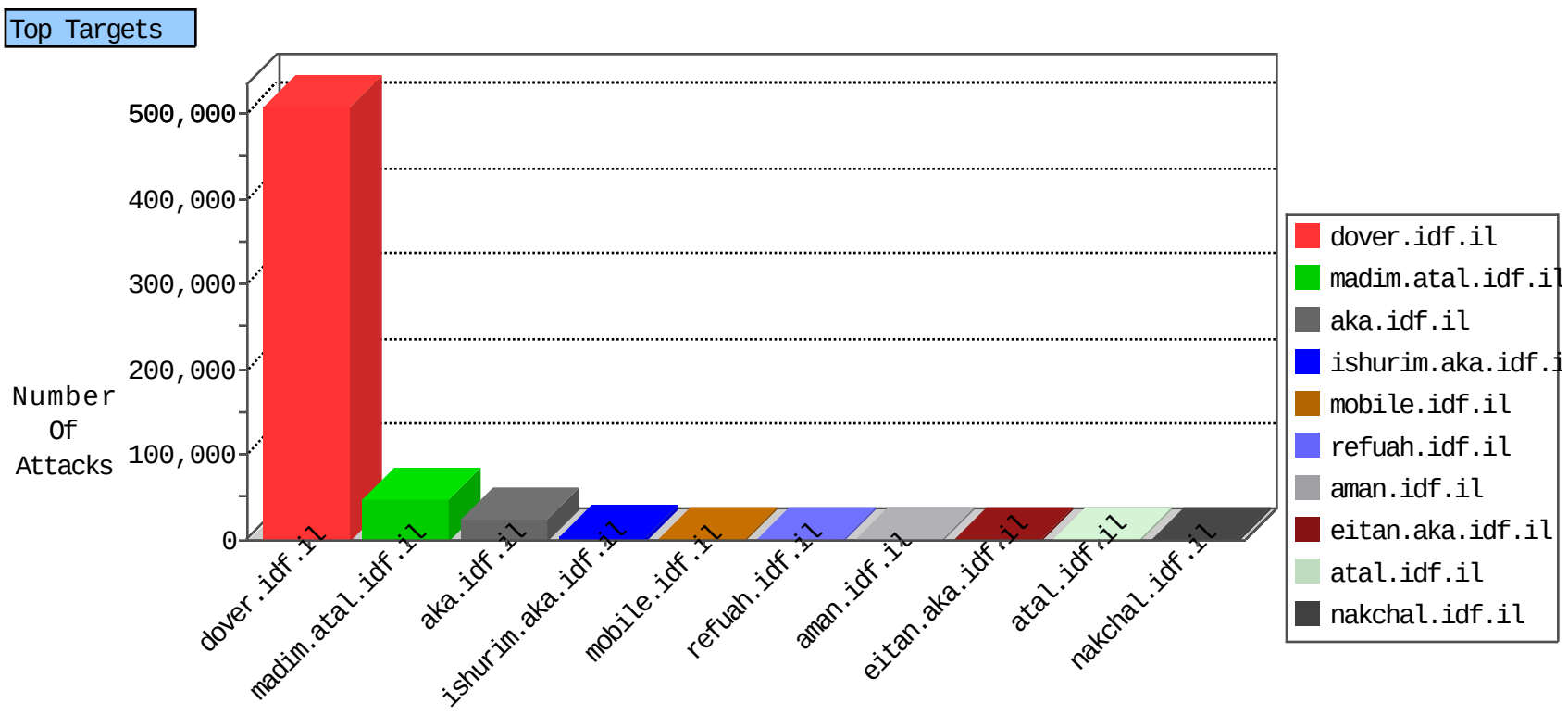
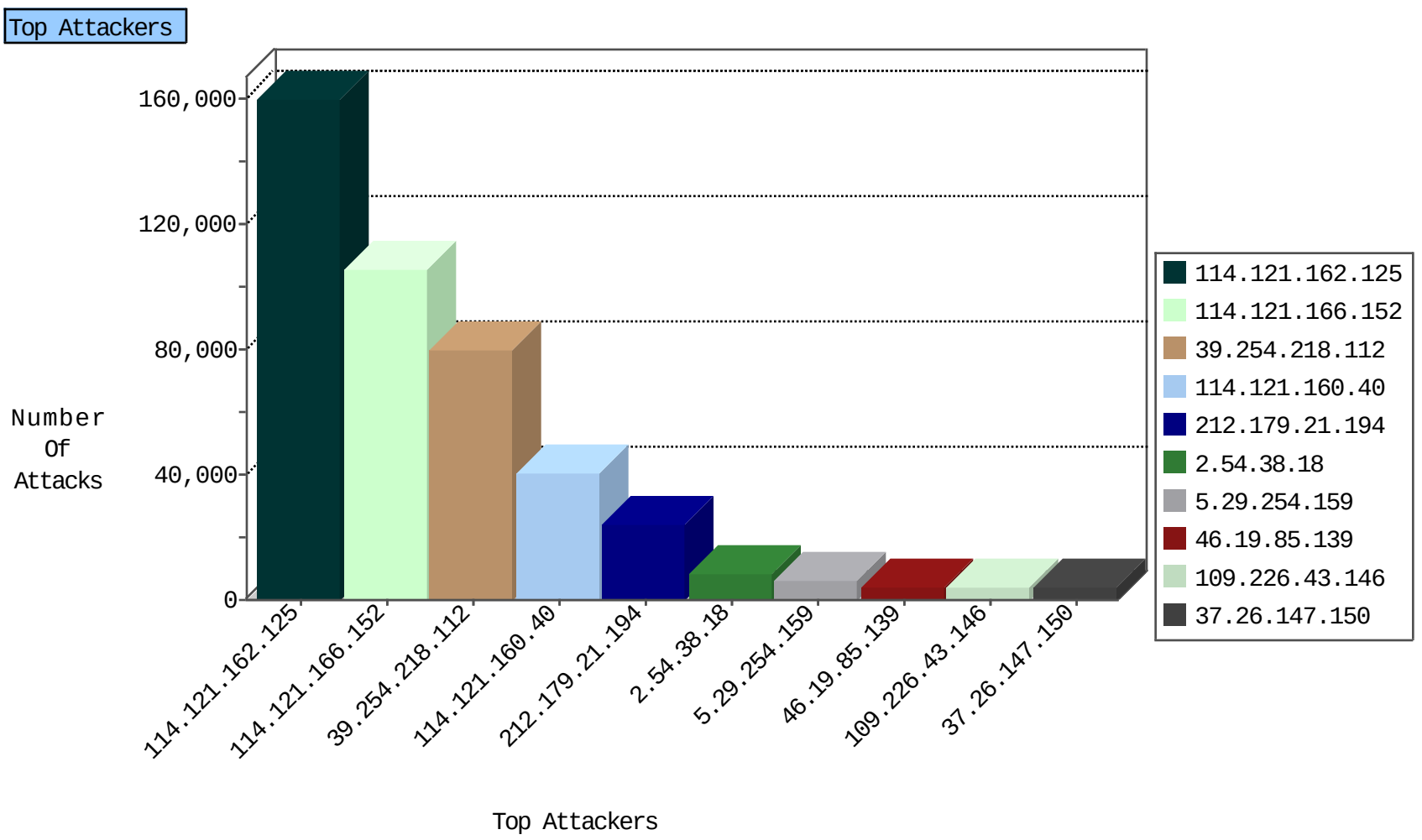
10-11-2015-00:00:01 to 10-12-2015-00:00:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-11-2015-00:00:01 to 10-12-2015-00:00:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
114.121.160.40	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10735
114.121.162.125	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8601
66.102.9.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6906
46.121.56.9	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6275
62.0.42.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5896
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3628
39.254.218.112	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3376
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2837
220.253.181.127	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1788
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1147
66.249.65.95	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	931
184.66.24.121	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	768
66.249.65.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	681
66.249.67.208	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	403
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	388
66.249.78.146	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	363
114.121.166.152	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	346
2.54.53.180	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	268
149.78.19.175	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	246
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	232
66.249.67.224	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	211
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
2.54.174.241	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	182
212.25.105.125	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
156.192.174.161		147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	149
2.54.144.93	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	146
84.229.184.162	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	138
46.19.86.202	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	134
94.159.247.161	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	132
80.246.136.163	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	129
197.39.255.60	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	129
46.19.86.255	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	127
46.19.86.138	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	116
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
46.19.86.73	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	104
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
2.52.12.115	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	95
79.177.21.43	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	90
80.246.136.20	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	90
185.32.179.168	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	89
2.54.2.222	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	87
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
149.202.112.62	Germany	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	84
37.26.148.203	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	83
46.19.85.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	82
91.228.248.251	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	79
2.54.188.86	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	77
185.32.179.206	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
79.177.190.122	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	71
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69

10-11-2015-00:00:01 to 10-12-2015-00:00:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.113.143	France	147.237.76.42	refuah.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	14
41.236.215.79	Egypt	147.237.77.216	dover.idf.il	12371: TCP: Hulk DDoS Tool	Block	9
64.31.44.3	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
31.168.136.9	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
87.68.161.80	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
41.236.218.2	Egypt	147.237.77.216	dover.idf.il	12371: TCP: Hulk DDoS Tool	Block	5
37.205.0.60	Turkey	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
147.236.30.190	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
83.168.248.11	Sweden	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
69.107.89.70	United States	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
216.249.102.195	United States	147.237.0.34	tikshuv.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
213.151.38.163	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
74.208.133.60	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
62.219.47.151	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
213.246.49.97	France	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
212.179.5.3	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
116.8.98.33	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
213.246.49.97	France	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	3
213.8.242.46	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
62.90.131.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
108.67.169.124	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
74.208.133.60	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
62.219.244.2	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.166.22.7	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.237.232.83	Iraq	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	2
80.93.62.66	Russian Federation	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
186.247.201.24	Brazil	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
210.75.99.11	China	147.237.72.166	aka.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
62.163.78.143	Netherlands	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
108.67.169.124	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
80.93.62.67	Russian Federation	147.237.72.156	aman.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
213.246.49.97	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
189.38.90.212	Brazil	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
74.208.133.60	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
62.210.107.201	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
189.38.90.212	Brazil	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
95.86.75.102	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
79.176.29.72	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
198.20.69.74	United States	147.237.8.50	e.tikshuv.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
62.90.131.78	Israel	147.237.72.166	aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	1
106.38.241.118	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
80.93.62.66	Russian Federation	147.237.72.156	aman.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
62.210.167.131	France	147.237.77.216	dover.idf.il	3959: HTTP: Cross-Site Scripting (Cookie Manipulation)	Block	1
149.202.54.5	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
85.25.185.157	Germany	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.69.74	United States	147.237.77.212	e.dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-11-2015-00:00:01 to 10-12-2015-00:00:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	98
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	47
108.168.219.166	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	21
87.68.243.138	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	15
213.246.49.97	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	14
83.168.248.11	147.237.72.166	Sweden	aka.idf.il	SQL Injection - Select From	12
64.31.44.3	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
66.249.93.134	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	9
108.67.169.124	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	9
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	8
189.38.90.212	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
74.208.133.60	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
37.205.0.60	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	6
66.249.64.156	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	6
74.208.133.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	5
223.196.228.123	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	4
66.249.65.95	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.81.208	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	4
216.249.102.195	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	4
82.80.89.41	147.237.72.166	Israel	aka.idf.il	GPL SCAN nmap TCP	3
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
66.249.67.6	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
156.192.174.161	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	3
66.249.78.206	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
176.12.144.63	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
66.249.67.208	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
82.117.208.243	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
37.26.148.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
176.12.149.222	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
66.249.78.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
176.12.144.63	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
85.250.218.31	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
79.180.142.44	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	2
66.249.67.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
114.121.162.125	147.237.77.216	Indonesia	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.93.200	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
176.12.149.222	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
210.61.150.154	147.237.76.198	Taiwan	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
42.233.18.180	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.48.105.216	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.205	Canada	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.64.81	147.237.0.33	Netherlands	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
61.152.104.140	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
190.147.73.50	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.56.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.172.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
79.138.70.153	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

10-11-2015-00:00:01 to 10-12-2015-00:00:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23741
114.121.162.125	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10509
114.121.166.152	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5473
109.226.43.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3853
39.254.218.112	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3768
62.0.42.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2987
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1786
185.52.233.145	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1680
46.19.86.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1644
95.86.88.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1229
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1027
149.202.112.62	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1012
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	989
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	982
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	928
192.114.23.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	886
132.66.40.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	848
114.121.160.40	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	801
66.249.65.89	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	767
66.249.65.95	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	748
2.54.172.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	725
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	697
79.177.221.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	657
66.249.65.92	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	656
85.250.59.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	636
164.138.125.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	624
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	572
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	541
5.28.168.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	540
108.171.128.166	United Kingdom	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	523
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	520
213.151.48.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	513
109.226.15.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	463
46.19.86.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	449
213.151.41.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	444
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	417
66.249.65.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	376
46.117.64.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	375
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	367
77.126.3.194	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	366
66.249.65.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	354
66.249.65.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	347
31.186.228.94	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	328
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	313
149.202.112.62	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	313
77.125.248.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	309
46.19.86.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	305
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	304
37.60.45.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	287
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	281

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
114.121.162.125	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	149095
114.121.166.152	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99751
39.254.218.112	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76130
114.121.160.40	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39423
2.54.38.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8126
5.29.254.159	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.254.159	Block	6222
46.19.85.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3872
37.26.147.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3844
87.68.32.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2858
176.13.20.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2450
46.19.86.241	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.241	Block	2380
2.54.152.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2304
2.54.50.179	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.50.179	Block	2184
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2153
176.12.146.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2148
176.12.141.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1860
2.54.133.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1538
176.12.142.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1396
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1344
31.168.136.9	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	936
85.250.224.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	895
46.117.165.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	744
75.101.180.96	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 75.101.180.96	Block	744
176.13.19.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	660
79.176.157.62	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.157.62	Block	612
176.13.8.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	555
85.65.236.70	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.236.70	Block	528
75.126.122.176	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	528
54.187.55.213	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	456
2.54.144.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	360
176.13.16.138	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.16.138	Block	348
80.246.137.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	324
176.13.21.209	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.21.209	Block	300
2.54.31.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	300
75.126.122.176	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	288
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	288
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.155.129	Block	288
77.126.3.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 77.126.3.194	Block	204
46.19.85.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.89	Block	168
176.12.137.46	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.12.137.46	Block	164
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	156
114.121.166.152	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	132
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	131
84.108.237.118	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ufi/reaction/	Block	115
207.46.13.24	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	108
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.95	Block	108
109.64.39.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	108
2.54.140.241	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 2.54.140.241	None	107
176.13.4.182	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.4.182	None	84