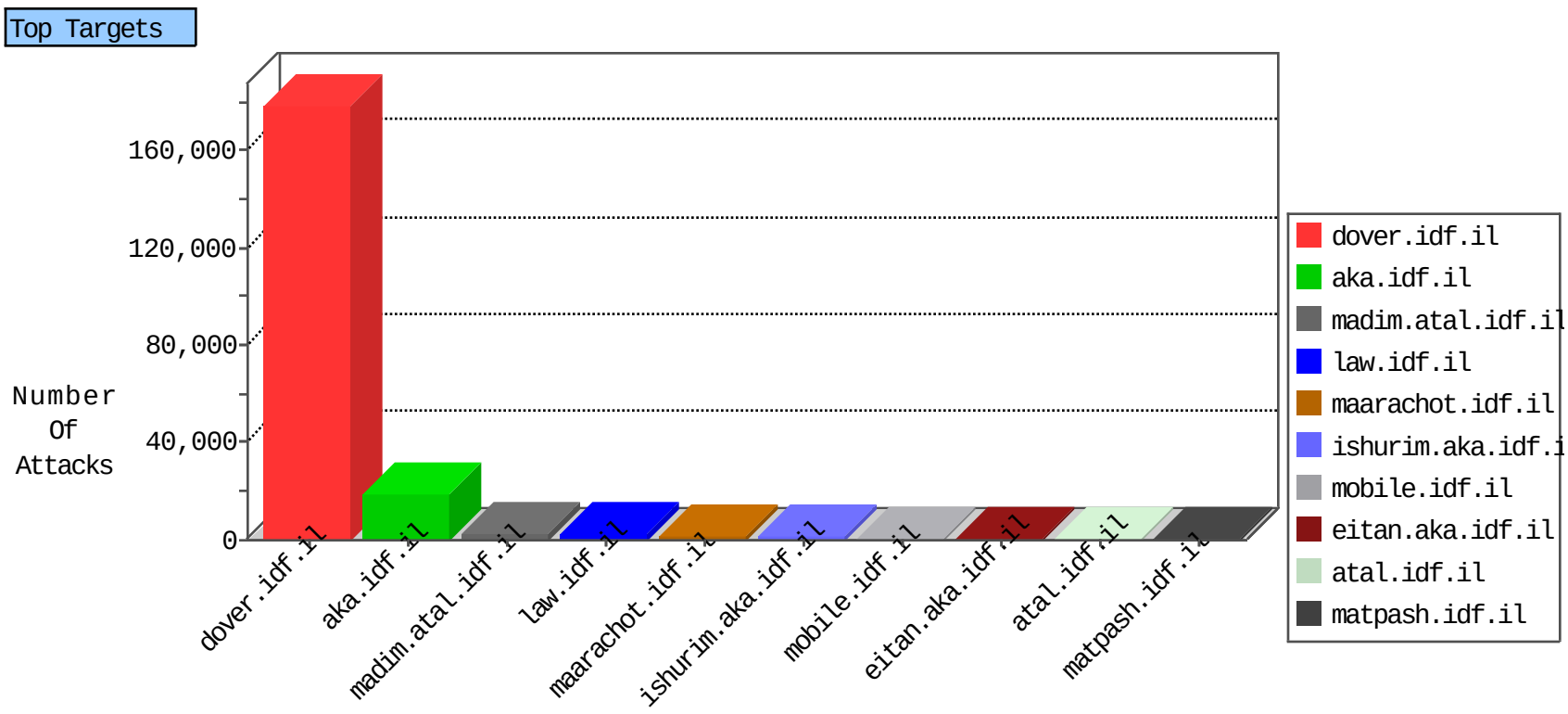
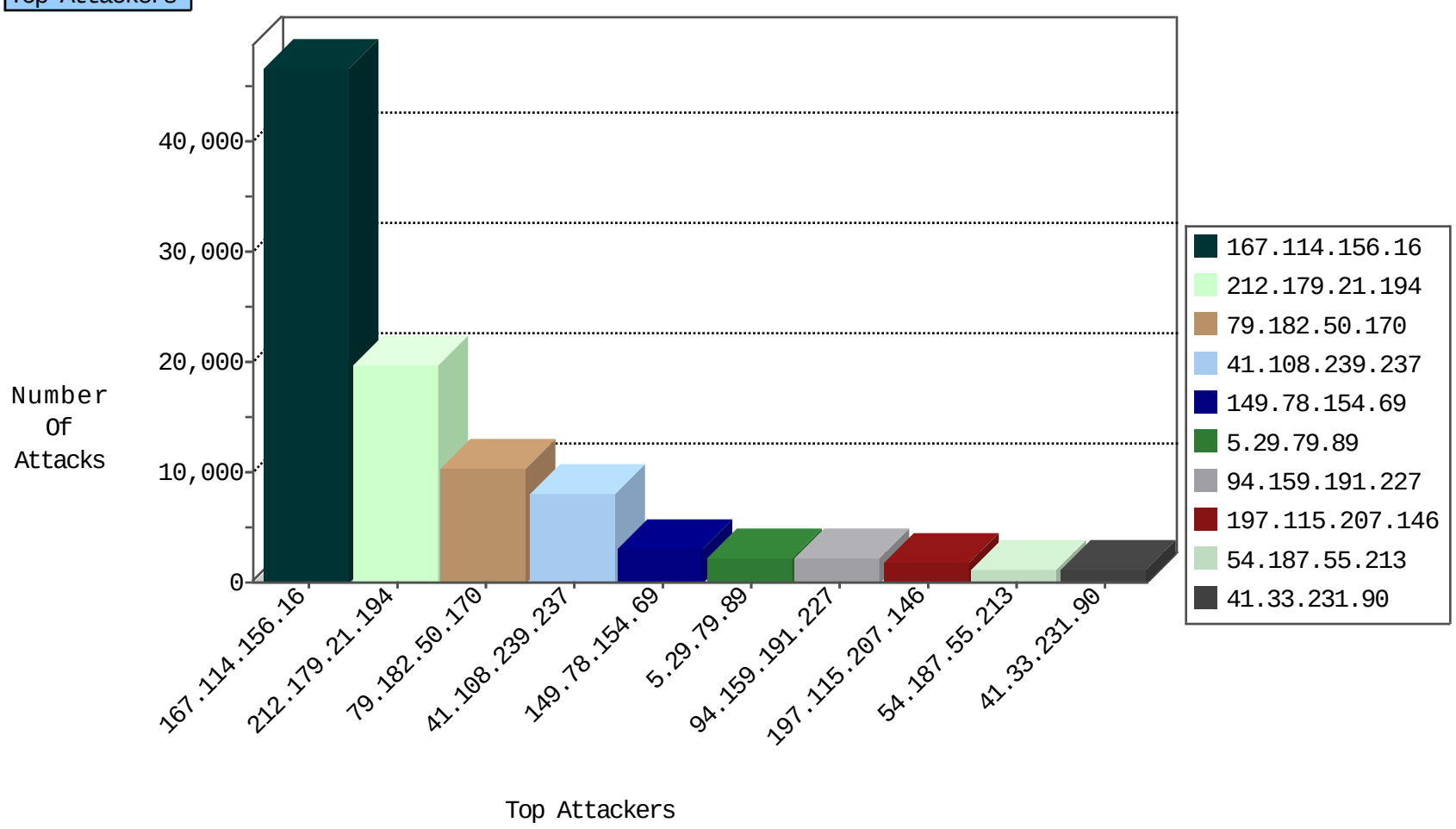
11-04-2015 to 11-05-2015

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-04-2015 to 11-05-2015

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	TCP handshake violation, first packet not syn	drop	511022
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	150104
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	98018
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	97793
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	83035
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	75304
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	67743
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	49896
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48636
197.115.207.146	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41041
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33266
66.249.65.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32615
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	31715
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	31411
66.249.65.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30771
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	29610
128.164.65.178	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	28758
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25697
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23356
66.249.69.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23179
66.249.79.10	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	20364
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19472
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18977
54.244.22.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17553
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	17309
66.249.67.202	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	17205
66.249.67.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	16557
54.187.55.213	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15671
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	14787
66.249.81.218	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14577
149.32.192.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14538
66.249.79.16	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	13083
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12764
66.249.93.192	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12618
66.249.67.216	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12015
192.236.7.252	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	11909
192.198.151.45	Europe	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11435
37.26.148.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10981
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10851
178.238.182.254	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10767
152.62.109.206	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9992
68.4.93.63	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9789
189.84.30.69	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9764
37.26.148.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9674
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9314
188.161.32.97	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	8622
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	8299
38.64.174.94	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8215
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7986
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7516

11-04-2015 to 11-05-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.136.227.77	Spain	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20
194.114.146.227	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
81.218.251.252	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.182.145.63	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.121.96.55	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
58.59.239.98	China	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
212.143.99.142	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
95.215.227.115	United Kingdom	147.237.0.34	tikshuv.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
23.91.70.50	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
109.64.42.117	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
95.86.102.126	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
66.249.69.34	Israel	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
217.12.204.163	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
95.30.34.246	Russian Federation	147.237.76.30	himush.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
77.125.6.180	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.74	United States	147.237.76.199	e.nakchal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
46.4.32.75	Germany	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
95.30.34.246	Russian Federation	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
85.93.89.81	Germany	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
217.12.204.163	Ukraine	147.237.76.30	himush.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
184.173.233.226	United States	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
58.180.228.110	Korea, Republic of	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
95.30.34.246	Russian Federation	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
79.176.142.200	Israel	147.237.72.167	ishurim.aka.idf.i	C1000098: Block - dns poisoning	Block	1
212.130.109.156	Denmark	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
151.80.44.115	Italy	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
95.86.74.153	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
217.12.204.163	Ukraine	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
61.160.213.11	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
95.30.34.246	Russian Federation	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
217.12.204.163	Ukraine	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
95.30.34.246	Russian Federation	147.237.0.34	tikshuv.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
63.237.114.10	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
23.91.70.50	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
109.67.145.42	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
95.30.34.246	Russian Federation	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
212.235.56.185	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
177.153.16.116	Brazil	147.237.77.170	maarachot.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
217.12.204.163	Ukraine	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
95.30.34.246	Russian Federation	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
198.20.69.74	United States	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
31.154.91.48	Israel	147.237.72.166	aka.idf.il	C1000098: Block - dns poisoning	Block	1

11-04-2015 to 11-05-2015

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	108
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	49
2.52.36.185	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	42
2.54.172.131	147.237.77.243	Israel	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	23
85.136.227.77	147.237.77.74	Spain	law.idf.il	SQL Injection - Select From	22
66.249.67.79	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	11
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	7
66.249.79.41	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	7
185.58.201.28	147.237.76.30	Lebanon	himush.idf.il	ET SCAN NMAP -sA (2)	7
95.215.227.115	147.237.0.34	United Kingdom	tikshuv.idf.il	SQL Injection - Select From	6
23.91.70.50	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
80.40.134.104	147.237.77.216	United Kingdom	dover.idf.il	GPL SCAN nmap TCP	4
66.249.79.16	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.79.45	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
184.173.233.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
66.102.9.15	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
194.63.140.74	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	2
185.82.201.17	147.237.77.216		dover.idf.il	ET DOS SSL Bomb DoS Attempt	2
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
177.37.128.117	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
194.63.140.74	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
80.246.136.84	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
187.60.247.195	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.6	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
187.60.247.195	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN Potential SSH Scan	2
5.22.131.252	147.237.77.176	Israel	matpash.idf.il	INDICATOR-SCAN myscan	2
87.68.147.217	147.237.76.30	Israel	himush.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
177.37.128.117	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	2
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.67.208	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
80.246.137.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
187.60.247.195	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
5.22.131.252	147.237.77.176	Israel	matpash.idf.il	GPL SCAN myscan	2
104.192.0.20	147.237.77.74	United States	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.230.40.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.63.140.74	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
187.60.247.195	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
1.235.195.234	147.237.77.235	Korea, Republic of	sviva.idf.il	ET SCAN NMAP -f -sS	1
123.126.113.80	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.0.15	Turkey	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.160.254.96	147.237.76.148	Korea, Republic of	gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
68.65.121.91	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
24.228.112.59	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-04-2015 to 11-05-2015

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	19525
41.108.239.237	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7958
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3257
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2939
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2658
5.29.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2166
94.159.191.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2165
197.115.207.146	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1586
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1133
84.109.69.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1099
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	947
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	932
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	929
109.166.128.39	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	887
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	879
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	810
176.31.117.76	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	746
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	721
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	642
212.76.111.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	584
87.68.155.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	563
109.226.20.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	552
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	520
46.19.85.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	511
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	488
51.254.113.74	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	476
167.114.156.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	468
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	458
109.64.162.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	454
93.104.209.118	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	434
79.182.211.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	420
149.255.232.172	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	410
194.90.255.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	406
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	404
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	395
107.167.108.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	389
95.86.119.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	385
38.64.174.94	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	380
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	374
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	353
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	352
77.127.240.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	340
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	330
79.181.107.74	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	330
147.236.238.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	303
184.151.118.89	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	294
66.249.69.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	290
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	290
66.171.228.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	279
81.218.251.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	276

11-04-2015 to 11-05-2015

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.182.50.170	Block	4407
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1548
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	1445
80.246.136.84	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.84	Block	363
79.182.103.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.103.77	Block	273
176.13.6.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
80.246.136.84	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.246.136.84	Block	121
80.246.136.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
79.182.103.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
79.182.103.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 79.182.103.77	Block	101
176.13.6.154	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.6.154	Block	99
176.13.19.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
37.26.147.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
185.120.126.11		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.13.19.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
176.12.145.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
176.12.141.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
185.3.146.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.121.26.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
176.12.141.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
2.54.18.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
37.26.147.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
46.19.86.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
213.57.225.227	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.225.227	Block	53
176.12.141.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
89.139.4.147	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
185.120.126.11		147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
46.19.86.84	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	43
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
207.232.21.105	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 207.232.21.105	Block	42
176.13.18.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.86.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.9.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
176.12.145.147	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.145.147	Block	24
2.52.32.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.54.37.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
193.106.55.244	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	20
37.142.184.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
37.142.103.18	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.103.18	Block	17
149.78.251.252	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.251.252	Block	17
89.138.198.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.198.137	Block	17
46.19.86.157	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 46.19.86.157	Block	16
80.246.139.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
5.29.94.171	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	16

11-04-2015 to 11-05-2015