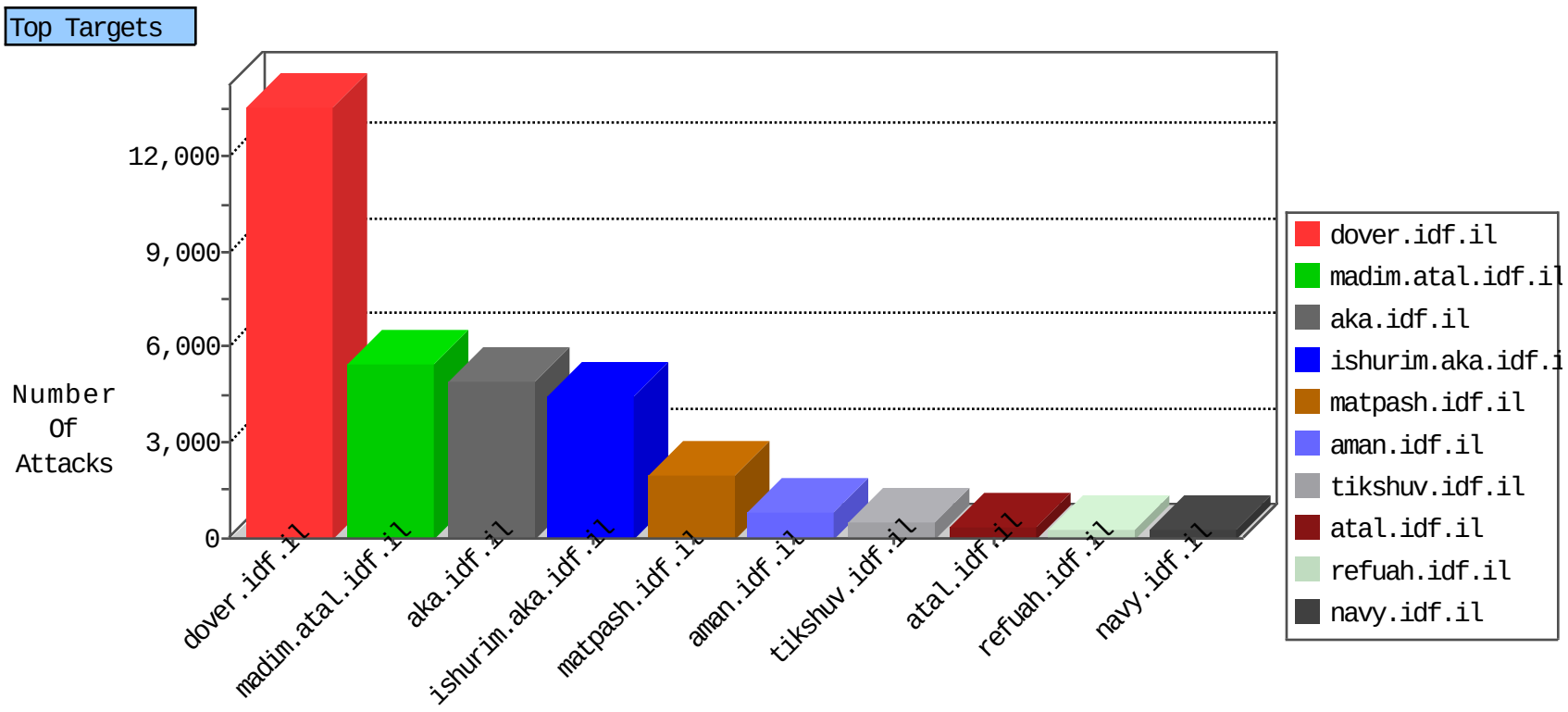
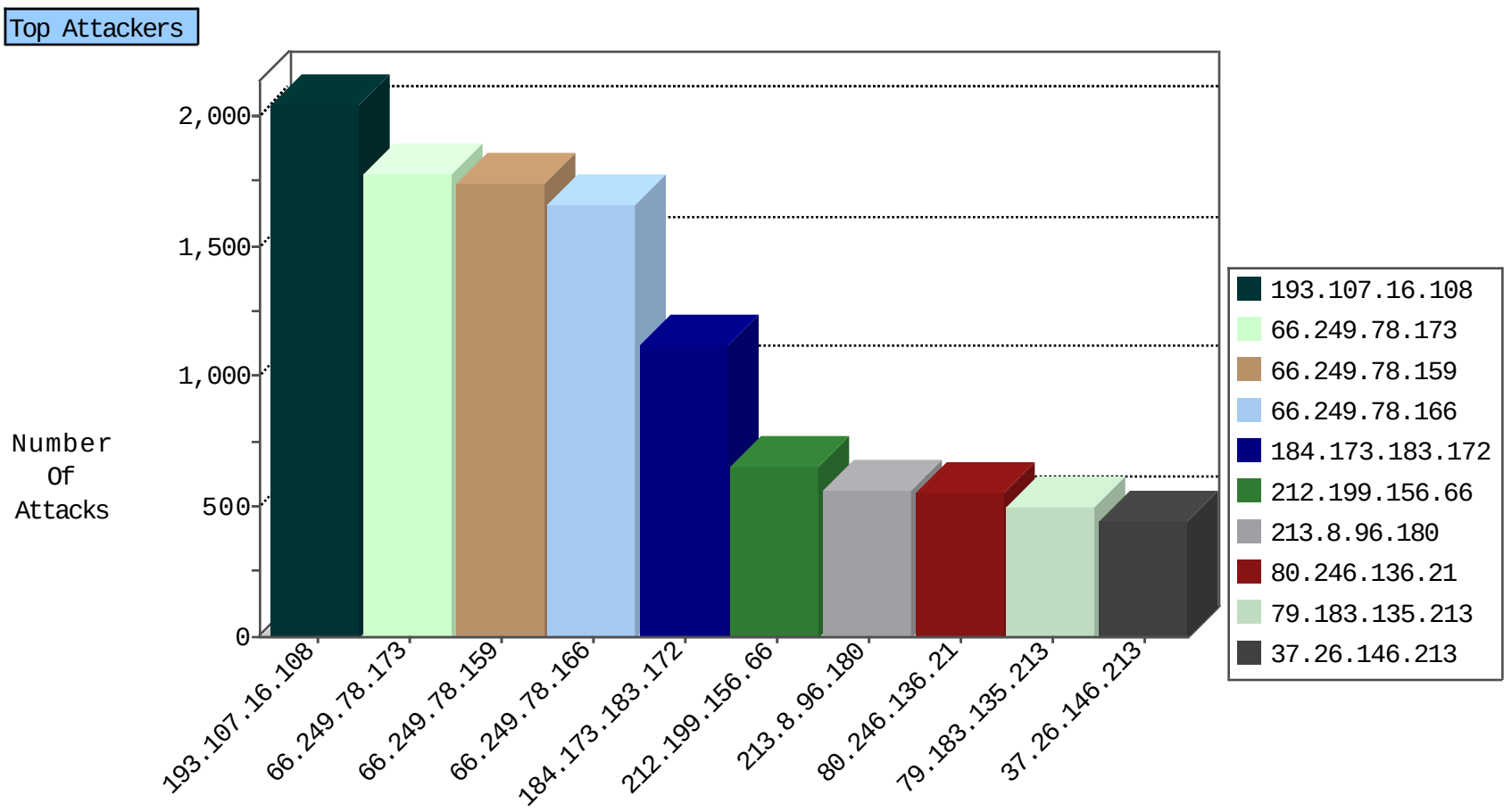
01-25-2015-00:00:00 to 01-26-2015-00:00:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-25-2015-00:00:00 to 01-26-2015-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.41	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	27107
66.249.67.83	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	611
66.249.64.45	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	598
84.109.127.172	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	539
212.235.79.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	353
87.68.104.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	310
84.228.135.123	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	282
85.250.1.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	266
212.76.116.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	209
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
46.121.132.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	188
84.229.42.175	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	185
212.25.105.125	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	184
37.142.138.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	166
194.90.239.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	149
84.108.75.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
176.12.136.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	134
87.68.85.12	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	129
46.117.190.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
84.229.60.42	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
85.64.21.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
109.64.61.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
62.128.62.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
94.159.141.172	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	116
109.66.22.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
46.121.142.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
176.12.149.75	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	110
46.19.85.92	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	106
85.65.222.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	103
213.57.155.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
149.78.145.182	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	93
77.125.76.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
149.78.163.212	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
46.117.228.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
80.246.136.249	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
79.182.128.67	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
5.29.134.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
185.32.179.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	83
185.32.179.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	81
79.181.126.188	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	79
176.12.136.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	78
37.26.147.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
149.78.137.28	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
192.115.248.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
109.64.120.224	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
46.19.85.48	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	74
46.117.88.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
89.138.78.145	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	73
149.78.145.182	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	73

01-25-2015-00:00:00 to 01-26-2015-00:00:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
193.107.16.108	Russian Federation	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	1316
193.107.16.108	Russian Federation	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	732
212.199.156.66	Israel	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	650
184.173.183.172	United States	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	465
184.173.183.172	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	448
213.8.118.92	Israel	147.237.72.167	ishurim.aka.idf.il	Rep_Notify_Only_Tehila	Permit	361
128.242.249.12	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	245
184.173.183.172	United States	147.237.77.233	atal.idf.il	Rep_Notify_Only_Tehila	Permit	212
96.44.189.100	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	148
176.10.99.206	Switzerland	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	87
95.130.15.97	France	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	42
180.76.5.193	China	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	36
216.99.158.82	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
23.234.30.19	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	30
82.211.201.188	Denmark	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	23
82.116.120.3	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
96.47.226.22	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
77.95.229.11	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
91.109.247.173	United Kingdom	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
167.88.40.152		147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
77.95.229.19	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
82.211.223.3	Denmark	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
77.95.229.21	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
62.212.89.116	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
96.44.189.101	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
217.115.10.134	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
178.217.187.39	Poland	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
176.36.150.246	Ukraine	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	15
171.25.193.20	Sweden	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	15
184.77.85.126	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
81.218.251.251	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	Rep_Notify_Only_Tehila	Permit	10
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	10
92.240.15.1	United Kingdom	147.237.72.166	aka.idf.il	C1000098: Block - dns poisoning	Block	10
184.77.85.126	United States	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
213.8.118.92	Israel	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	8
195.154.255.148	France	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	7
62.0.101.97	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
80.254.148.107	Europe	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.199.156.66	Israel	147.237.72.166	aka.idf.il	7610: IP Reputation	Permit	5
46.210.210.241	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
80.179.225.42	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.183.50.76	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
93.173.141.126	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
132.74.58.123	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.251.206.224	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	4
79.173.192.99	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.95.133.112	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4

01-25-2015-00:00:00 to 01-26-2015-00:00:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	238
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	132
109.169.45.231	United Kingdom	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
147.236.30.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	7
109.169.45.231	United Kingdom	147.237.77.19	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
109.169.45.231	United Kingdom	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
109.169.45.231	United Kingdom	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
66.249.93.159	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	6
109.169.45.231	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
2.54.35.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	5
109.169.45.231	United Kingdom	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
185.32.178.222	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
109.169.45.231	United Kingdom	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
84.111.65.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
5.29.16.72	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
46.105.113.8	France	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	4
109.169.45.231	United Kingdom	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
213.57.155.196	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
109.169.45.231	United Kingdom	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
37.142.246.83	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
149.78.99.199	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
109.169.45.231	United Kingdom	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
95.86.94.221	Israel	147.237.76.86	navy.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	3
109.169.45.231	United Kingdom	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
198.20.232.83	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	3
109.169.45.231	United Kingdom	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
95.86.93.58	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	3
79.180.96.46	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3

01-25-2015-00:00:00 to 01-26-2015-00:00:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1730
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1689
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1608
213.8.96.180	Israel	147.237.77.216	dover.idf.il		drop	drop	535
66.249.64.145	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	402
66.249.64.149	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	382
66.249.64.141	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	342
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	82
85.130.217.202	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	76
205.189.94.12	Canada	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	68
85.130.130.16	Israel	147.237.72.166	aka.idf.il		drop	drop	67
66.249.64.116	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
66.249.93.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
5.22.129.211	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	50
5.22.129.211	Israel	147.237.72.156	aman.idf.il		drop	drop	45
188.161.7.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SAM rule	drop	drop	45
108.15.72.231	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
46.19.86.107	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
23.234.30.19	United States	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	39
66.249.81.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
85.64.241.4	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
46.43.122.151	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il		drop	drop	36
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
46.19.86.195	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
46.19.86.160	Israel	147.237.77.216	dover.idf.il		drop	drop	35
87.68.150.203	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
80.178.95.245	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
46.19.86.239	Israel	147.237.72.166	aka.idf.il		drop	drop	32
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
79.180.161.122	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
94.230.86.21	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	30
31.210.186.24	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	30
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
46.120.17.180	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.81.203	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
5.64.174.208	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il		drop	drop	29
62.90.72.130	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
212.179.131.58	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
93.173.1.127	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
79.178.20.123	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
77.126.124.192	Israel	147.237.72.166	aka.idf.il		drop	drop	25
94.230.86.104	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	25
89.3.110.247	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
80.179.126.26	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
217.194.199.124	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
79.182.52.219	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
31.210.186.37	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	23
193.43.244.102	Israel	147.237.72.167	ishurim.aka.idf.il		drop	drop	23
79.180.160.220	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	23

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.246.136.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	536
79.183.135.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	491
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	446
66.249.78.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	425
66.249.78.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	420
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	393
109.66.4.118	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.4.118	Block	353
109.253.129.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	333
2.54.22.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	323
109.253.132.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	317
80.246.136.249	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.249	Block	298
212.150.174.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	250
109.253.134.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	212
84.228.126.126	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.126.126	Block	200
185.32.177.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	193
109.253.149.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
2.54.156.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	167
95.35.27.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	155
109.253.139.207	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.139.207	Block	147
176.12.140.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
5.29.227.141	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.227.141	Block	124
2.54.170.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	98
46.19.86.229	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.229	Block	79
46.19.86.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
37.26.146.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
46.19.85.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
66.249.64.55	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.55	Block	57
66.249.64.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.51	Block	56
176.12.149.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
66.249.64.47	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.47	Block	52
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	47
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	40
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	40
132.70.66.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
104.173.225.247		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	35
85.65.151.38	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	34
79.180.184.141	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 79.180.184.141	Block	34
95.86.109.110	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	33
2.54.49.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
213.57.102.4	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.102.4	Block	29
37.142.157.36	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 37.142.157.36	Block	29
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	28
5.29.39.178	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 5.29.39.178	Block	28
212.179.131.58	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	27
188.161.7.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.161.7.240	Block	27
37.60.45.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	23
82.102.141.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
84.228.128.214	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.228.128.214	Block	18
149.78.96.82	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	15
95.86.93.58	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	14

01-25-2015-00:00:00 to 01-26-2015-00:00:00