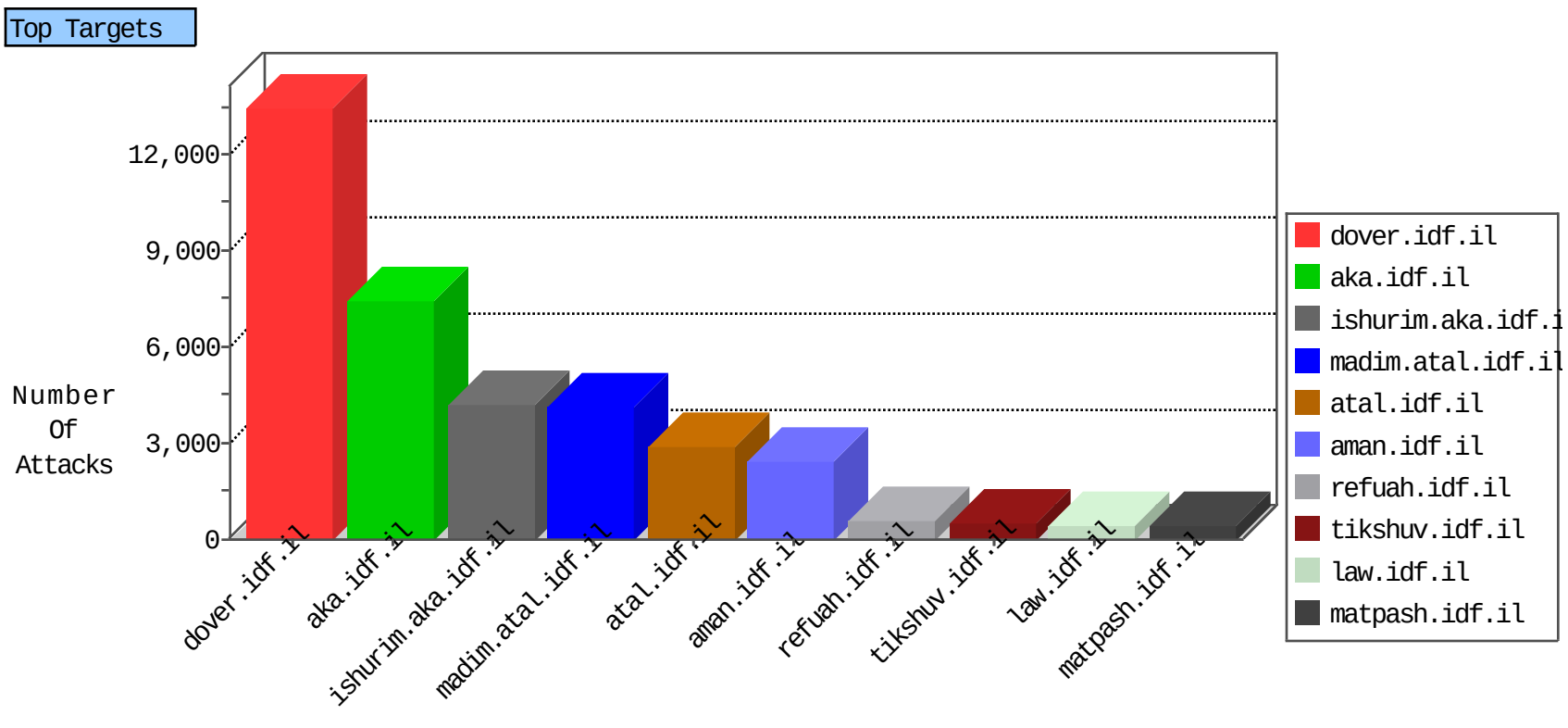
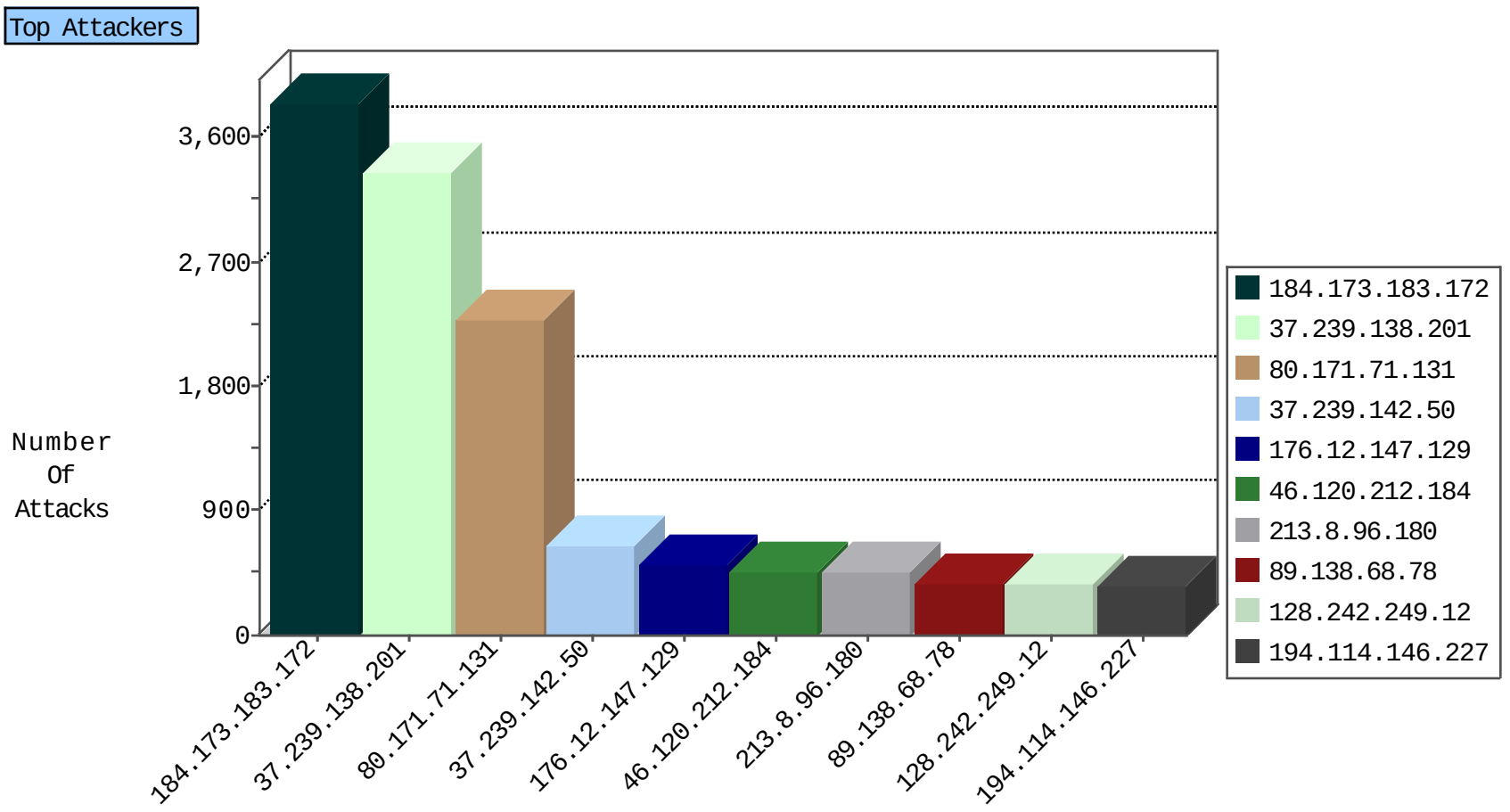
01-22-2015-00:00:00 to 01-23-2015-00:00:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-22-2015-00:00:00 to 01-23-2015-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
37.239.138.201	Iraq	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	4476
79.183.131.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	2782
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2640
37.239.138.201	Iraq	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2216
176.12.147.129	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	1134
85.250.2.183	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	840
79.182.145.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	839
37.239.138.201	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	712
37.239.138.201	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	673
212.76.102.120	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	588
79.180.153.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	511
77.127.144.140	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	448
79.181.51.121	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	357
85.250.62.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	348
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	313
37.60.44.119	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	255
176.12.143.243	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	226
213.57.225.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
85.65.95.236	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
79.181.51.121	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	168
109.66.148.91	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	162
77.127.176.243	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
109.253.147.147	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	159
213.57.161.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
94.159.186.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
95.86.112.247	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	130
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
109.66.22.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
109.253.147.147	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	120
217.132.85.54	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	118
109.160.218.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	114
217.132.124.22	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
62.219.187.126	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	112
5.29.97.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
5.28.181.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
46.120.169.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	102
2.54.170.198	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	100
77.126.152.123	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	100
87.69.63.20	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	97
93.172.184.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
37.239.137.211	Iraq	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	93
80.246.140.17	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
212.68.144.42	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	91
46.19.85.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
149.78.15.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87

01-22-2015-00:00:00 to 01-23-2015-00:00:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.233	atal.idf.il	Rep_Notify_Only_Tehila	Permit	2676
80.171.71.131	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	2280
184.173.183.172	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	529
128.242.249.12	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	368
194.114.146.227	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	325
184.173.183.172	United States	147.237.77.74	law.idf.il	Rep_Notify_Only_Tehila	Permit	278
192.117.150.233	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	211
184.173.183.172	United States	147.237.76.42	refuah.idf.il	Rep_Notify_Only_Tehila	Permit	193
184.173.183.172	United States	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	172
176.10.99.204	Switzerland	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	167
46.19.85.91	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	105
212.199.7.198	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	105
5.28.177.217	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	104
81.218.241.26	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	86
87.69.33.243	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	84
212.179.61.122	Israel	147.237.77.216	dover.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	83
2.54.14.83	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	80
46.19.85.243	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	79
217.41.38.13	United Kingdom	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	72
109.253.140.199	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	70
37.239.138.201	Iraq	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	70
194.90.226.58	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	69
213.57.154.82	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	64
2.54.185.40	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	63
80.246.140.220	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	63
46.117.222.106	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	57
84.109.213.35	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	57
195.200.205.40	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	57
46.19.85.122	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	56
87.68.91.86	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	56
2.54.15.53	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	56
80.246.137.122	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	55
176.12.143.102	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	54
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	53
85.64.32.163	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	53
79.177.152.233	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	51
109.66.22.26	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	50
37.26.146.139	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	49
176.12.141.160	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	49
82.80.164.158	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	48
109.186.154.248	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	47
5.28.161.76	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	47
176.12.146.0	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	46
46.19.86.199	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	46
212.179.61.122	Israel	147.237.76.177	ncore.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	43
212.143.34.185	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	42
188.120.148.82	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	40
95.86.66.110	Israel	147.237.72.166	aka.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	40
109.253.140.124	Israel	147.237.72.156	aman.idf.il	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	39
109.253.130.233	Israel	147.237.72.167	ishurim.aka.idf.i	19266: TLS: Microsoft SChannel Client Hello Memory Corruption Vulnerability	Permit	38

01-22-2015-00:00:00 to 01-23-2015-00:00:00

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	263
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	131
109.169.45.231	United Kingdom	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	9
89.139.80.232	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
109.169.45.231	United Kingdom	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
109.169.45.231	United Kingdom	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
85.250.179.179	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
109.169.45.231	United Kingdom	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
109.169.45.231	United Kingdom	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.233	atal.idf.il	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	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.19	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.61	e.cogat.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	4
109.169.45.231	United Kingdom	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.77.216	dover.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	147.237.76.177	ncore.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
109.169.45.231	United Kingdom	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
208.80.155.189	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	3
109.65.119.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
109.169.45.231	United Kingdom	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
107.167.110.60	United States	147.237.72.156	aman.idf.il	Tehila - Perl LWP with fake user agent	3
109.169.45.231	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
109.169.45.231	United Kingdom	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
109.169.45.231	United Kingdom	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.121.142.156	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.139.179.14	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

01-22-2015-00:00:00 to 01-23-2015-00:00:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.239.138.201	Iraq	147.237.77.216	dover.idf.il		drop	drop	1872
37.239.142.50	Iraq	147.237.77.216	dover.idf.il		drop	drop	494
213.8.96.180	Israel	147.237.76.31	nakchal.idf.il		drop	drop	202
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	154
8.37.227.54	Anonymous Proxy	147.237.76.86	navy.idf.il		drop	drop	151
213.8.96.180	Israel	147.237.72.166	aka.idf.il		drop	drop	149
82.102.141.202	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	127
66.249.93.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	126
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	118
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	108
200.144.26.79	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	92
66.249.81.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	88
66.249.81.203	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	86
5.28.185.153	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	85
66.249.81.197	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	74
90.24.230.67	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
82.102.141.202	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	67
79.179.149.253	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	65
159.53.110.143	United States	147.237.77.176	matpash.idf.il		drop	drop	58
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
168.235.196.54		147.237.77.216	dover.idf.il		drop	drop	54
157.55.39.217	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
213.8.96.180	Israel	147.237.77.216	dover.idf.il		drop	drop	47
190.49.244.137	Argentina	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
37.239.142.50	Iraq	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	45
212.143.138.205	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
93.186.23.113	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
217.194.202.13	Israel	147.237.72.166	aka.idf.il		drop	drop	42
80.147.119.123	Germany	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
78.108.161.226	Lebanon	147.237.77.176	matpash.idf.il		drop	drop	40
109.66.42.127	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
78.108.161.226	Lebanon	147.237.76.86	navy.idf.il		drop	drop	38
66.249.93.195	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
192.117.97.63	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
46.19.85.59	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il		drop	drop	34
131.253.26.192	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
50.185.100.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
84.228.43.201	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
79.176.54.81	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
46.19.86.118	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
37.26.147.240	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
138.162.0.43	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.83.175	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
80.246.140.130	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	27
174.48.112.181	United States	147.237.72.166	aka.idf.il		drop	drop	27
80.246.140.130	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	27
80.246.140.130	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	27
31.210.187.112	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	26
192.114.105.254	Israel	147.237.72.166	aka.idf.il		drop	drop	25

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.120.212.184	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.212.184	Block	453
37.239.138.201	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	414
37.239.138.201	Iraq	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	408
89.138.68.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	377
2.54.184.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	346
185.32.178.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	291
176.12.139.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	275
109.253.132.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	256
23.236.125.140	United States	147.237.77.216	dover.idf.il	Too Many of the Same Response Code (404) in Session from 23.236.125.140	Block	197
185.32.178.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	149
109.253.147.147	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.147.147	Block	142
2.54.35.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	141
176.12.146.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	130
109.253.133.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	114
5.29.140.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
213.57.186.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	101
37.26.146.227	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.227	Block	95
37.239.137.211	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	92
80.246.136.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	92
66.249.78.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	86
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	83
66.249.78.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	80
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.67	Block	74
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
176.12.147.129	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.147.129	Block	50
80.246.136.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
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	49
37.239.142.50	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	45
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
79.183.21.253	Israel	147.237.0.16	my-kosher-kravi.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 79.183.21.253	None	38
46.19.86.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
80.246.137.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
185.32.176.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
85.64.95.176	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 85.64.95.176	Block	19
85.64.168.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	19
2.54.152.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	19
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	16
5.28.185.153	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	16
162.243.26.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 162.243.26.16	Block	16
37.239.138.49	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	16
213.57.242.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
79.177.52.235	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/<html><head><title>502 bad gateway</title></head><body bgcolor=	Block	14
72.76.163.71	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	13
5.144.50.108	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
2.54.42.159	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	13
162.234.12.176	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	12
109.67.36.56	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 109.67.36.56	Block	12
85.65.90.214	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.65.90.214	Block	12

01-22-2015-00:00:00 to 01-23-2015-00:00:00