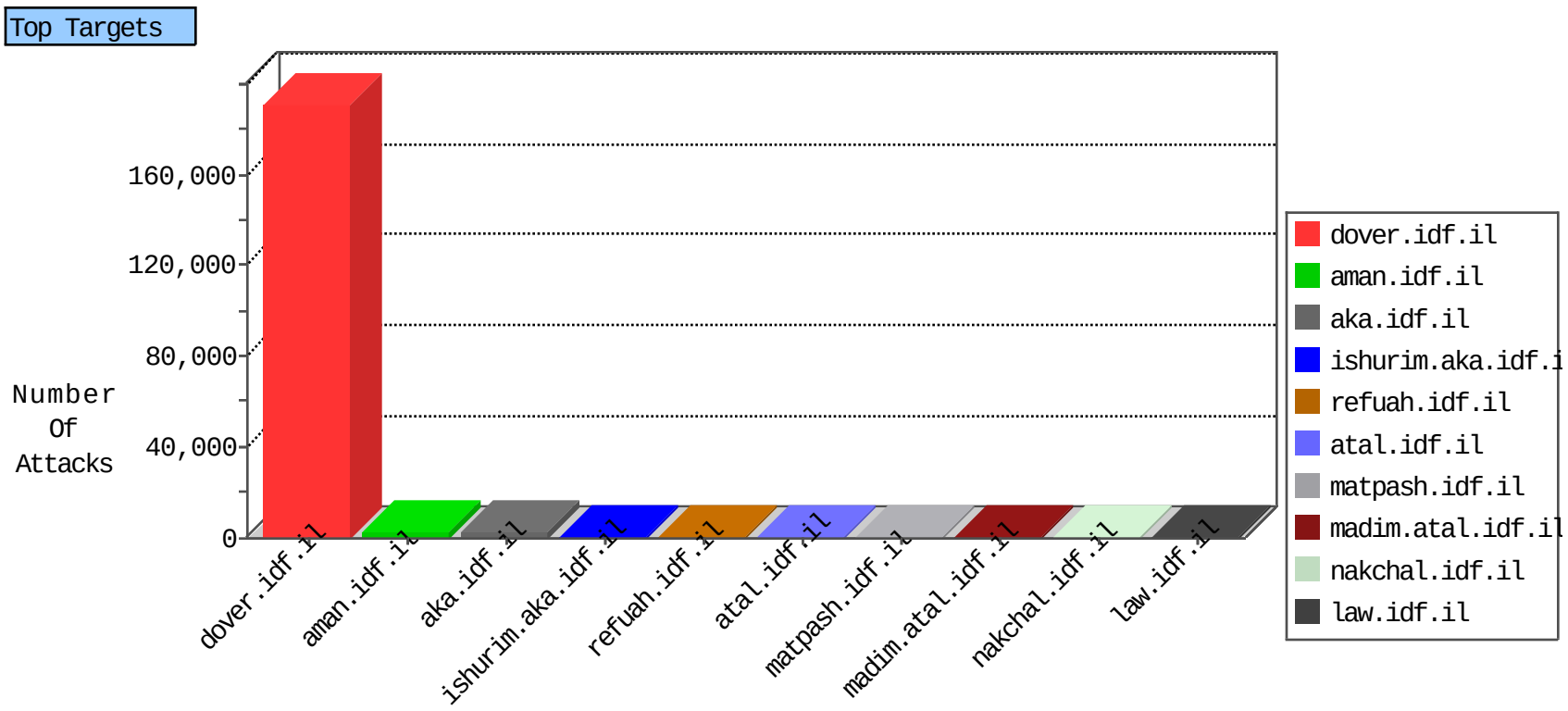
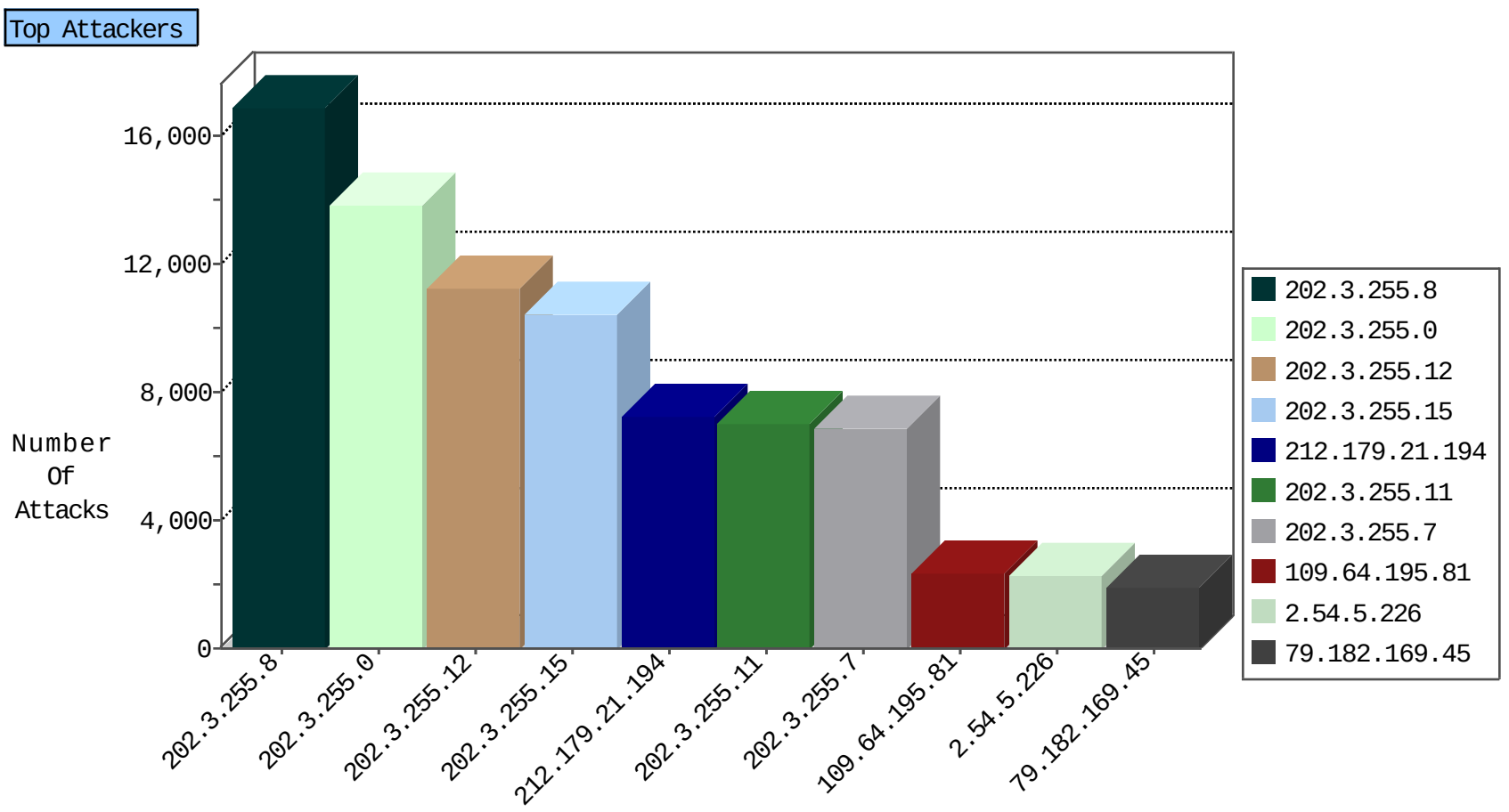
07-27-2015-00:00:06 to 07-28-2015-00:00:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



07-27-2015-00:00:06 to 07-28-2015-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
101.143.175.70	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3468
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	3463
2.52.141.30	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2590
119.25.131.96	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2540
109.65.35.151	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	831
2.248.177.124	Sweden	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	749
77.126.10.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	621
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	497
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	467
79.178.186.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	429
79.180.36.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	398
212.235.116.69	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	327
204.93.154.215	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	326
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	319
87.68.151.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	303
109.186.166.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	300
62.0.103.97	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	254
66.249.64.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	241
85.64.185.190	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	228
77.126.195.134	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	221
85.250.110.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	197
79.178.13.35	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
109.67.206.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	190
213.57.204.158	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	182
79.180.194.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
84.229.183.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	173
85.250.150.178	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
204.93.154.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	169
109.66.155.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
93.172.185.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
85.17.24.66	Netherlands	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	158
213.57.219.111	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	155
85.17.24.66	Netherlands	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	146
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	134
149.78.233.176	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	126
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	124
46.116.49.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
212.179.46.189	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	120
66.249.67.67	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	119
84.228.33.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
84.109.50.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
79.182.97.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
109.65.215.110	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
80.246.139.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
109.64.139.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	98
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
46.19.85.92	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	94
46.120.94.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
84.111.124.60	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88

07-27-2015-00:00:06 to 07-28-2015-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.102.216.32	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
212.199.224.24	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
87.69.54.42	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
84.94.181.145	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
149.78.242.68	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
79.179.211.105	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
177.134.84.169	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.250.109.253	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
93.89.239.75	Cyprus	147.237.76.42	refuah.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	6
93.89.239.75	Cyprus	147.237.76.42	refuah.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	6
79.178.196.120	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
74.10.162.1	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
82.80.84.168	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.27	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
93.173.135.236	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.228.176.246	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.62	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
211.59.8.170	Korea, Republic of	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
37.142.145.83	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.150.78.2	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
82.102.141.251	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.65.221.131	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.150.221.200	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.186.170.198	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
108.84.129.111	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.64.14	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.122	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
74.10.162.1	United States	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.178.107.85	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.43	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.108.33.90	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
37.26.147.253	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
180.97.106.161	China	147.237.77.74	law.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
87.69.125.177	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.180.167.63	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
84.94.161.66	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.177.232.114	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.127.60.239	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.167	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
2.54.128.15	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.179.21.194	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.118	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.138.47.60	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
209.213.104.25	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
108.84.129.111	United States	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
36.11.153.117	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.8	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-27-2015-00:00:06 to 07-28-2015-00:00:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	15560
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	12732
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	10335
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	9634
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	6455
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	6347
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	95
85.250.198.71	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	36
180.97.106.161	China	147.237.77.74	law.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	10
77.125.11.15	Israel	147.237.76.42	refuah.idf.il	GPL SCAN SYN FIN	8
77.125.11.15	Israel	147.237.76.42	refuah.idf.il	ET SCAN TCP Traffic (ET SCAN Malformed Packet SYN FIN)	8
180.97.106.162	China	147.237.77.74	law.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	6
82.166.22.217	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	6
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	SQL Injection - Select From	6
62.210.251.69	France	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	6
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	5
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	4
180.97.106.36	China	147.237.77.74	law.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	4
197.41.182.126	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	4
115.239.212.139	China	147.237.77.74	law.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	4
180.97.106.37	China	147.237.77.74	law.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.158	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
218.65.30.107	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
115.239.212.134	China	147.237.77.74	law.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	2
221.203.3.117	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
74.143.78.94	United States	147.237.72.166	aka.idf.il	ET DOS SSL Bomb DoS Attempt	2
88.250.115.119	Turkey	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
79.182.99.72	Israel	147.237.72.156	aman.idf.il	portscan: TCP Distributed Portscan	2
186.215.6.225	Brazil	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	2
45.114.11.49		147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.201	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
115.239.212.138	China	147.237.77.74	law.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	2
61.183.128.6	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
221.203.3.117	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2

07-27-2015-00:00:06 to 07-28-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6930
109.64.195.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2369
2.54.5.226	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2245
79.182.169.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1861
212.29.202.206	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1811
82.166.22.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1389
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1326
5.29.76.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1163
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1087
109.160.239.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1066
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	994
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	910
85.250.177.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	866
5.144.63.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	861
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	814
2.54.129.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	718
213.57.130.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	693
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	680
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	674
93.173.43.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	671
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	658
37.26.149.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	656
79.176.54.83	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	624
212.25.102.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	615
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	602
169.145.3.40	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	601
85.250.247.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	562
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	562
82.145.220.137	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	557
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	538
109.65.118.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	534
46.19.85.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	508
66.249.64.178	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	506
31.210.177.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	493
2.52.171.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	492
80.230.74.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	477
109.66.149.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	463
197.79.1.15	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	458
66.249.64.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	456
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	442
109.65.32.98	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	429
66.249.64.168	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	414
84.111.100.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	401
84.228.219.189	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	401
46.19.86.41	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	398
46.19.85.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	394
175.113.144.213	Korea, Republic of	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	387
165.125.178.11	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	367
46.19.86.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	365
79.178.137.50	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	365

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.21.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	100
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	96
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	85
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	82
198.204.230.130	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.204.230.130	Block	74
77.127.88.56	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.127.88.56	Block	67
176.13.14.107	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.14.107	Block	57
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.23	Block	43
198.204.230.130	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	41
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	39
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	34
207.241.237.211	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/error.htm	Block	19
198.204.230.130	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 198.204.230.130	Block	14
37.26.148.215	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	14
89.139.28.52	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	11
5.22.130.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
93.172.139.33	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	10
109.65.115.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
79.181.152.106	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	9
77.127.201.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	8
87.68.244.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	7
176.12.143.154	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	6
46.120.16.118	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
2.54.10.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	6
212.14.239.20	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	6
37.187.240.25	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
84.108.56.70	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/	Block	5
109.65.65.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
198.1.127.179	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 198.1.127.179	Block	5
109.64.14.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
82.166.221.34	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.166.221.34	Block	5
46.120.167.200	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
74.63.254.218	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.63.254.218	Block	5
37.187.240.25	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.187.240.25	Block	5
46.19.86.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
188.165.15.94	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.94	Block	5
176.228.176.129	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$password in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	5
85.65.54.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
93.173.45.159	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	4
188.165.15.27	France	147.237.76.30	himush.idf.il	Unknown Parameter l in www.chimush.atal.idf.il/templates/sendtofriend/sendtofriend.aspx	None	4
93.173.53.219	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
194.90.41.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.41.227	Block	4
84.228.176.246	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
212.199.57.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
84.94.161.118	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
109.73.250.59	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-17675-en/dover.aspx -	Block	4
2.54.62.154	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.62.154	Block	4