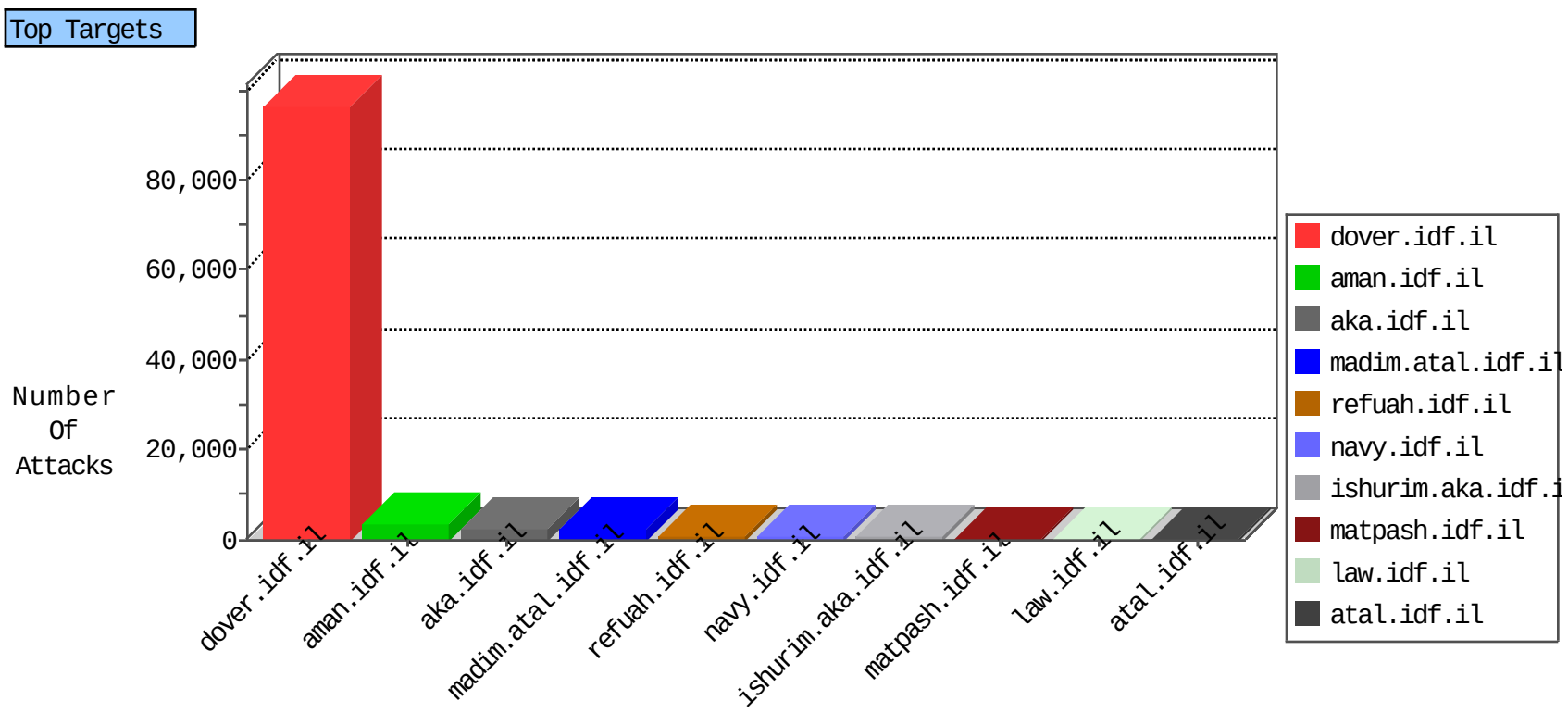
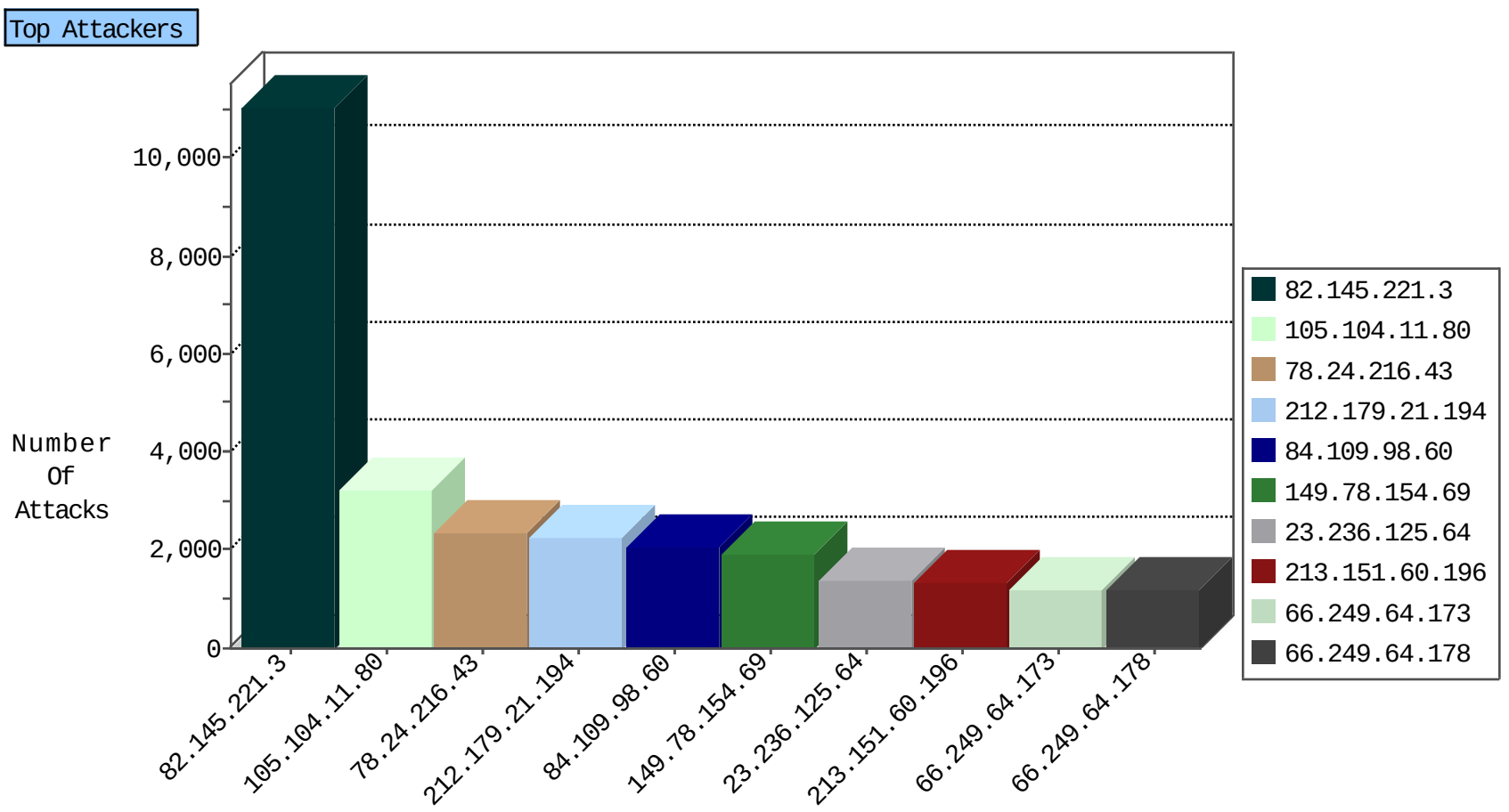
07-15-2015-00:00:07 to 07-16-2015-00:00:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



07-15-2015-00:00:07 to 07-16-2015-00:00:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.161	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4389
66.249.65.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4018
77.125.125.140	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3030
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2794
162.243.225.144	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2653
66.249.93.239	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2608
109.67.195.139	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1765
84.109.118.223	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	1612
175.142.168.165	Malaysia	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1611
54.166.162.106	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1504
31.186.228.29	United Kingdom	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1434
37.187.255.64	France	147.237.77.121	e.navy.idf.il	TCP handshake violation, first packet not syn	drop	1403
54.198.6.24	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1178
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1075
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	577
79.183.117.220	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	558
84.111.13.224	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	506
79.181.99.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	489
79.178.139.222	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	397
84.108.72.68	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	367
46.116.146.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	360
31.154.92.230	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	337
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	319
85.64.33.14	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	302
178.153.78.84	Qatar	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	291
82.80.17.247	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	281
84.108.1.223	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	277
82.166.22.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	277
84.108.132.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	272
192.117.183.158	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	263
84.228.197.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	248
79.179.102.60	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	232
109.65.11.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
79.176.135.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
77.127.6.62	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	214
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
79.181.4.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
54.198.38.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	190
37.142.12.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
109.66.173.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
79.183.194.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
84.228.116.223	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
84.228.175.51	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	166
5.28.171.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
212.25.84.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
84.109.86.175	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	150
46.121.64.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
79.177.180.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
79.176.211.201	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131

07-15-2015-00:00:07 to 07-16-2015-00:00:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
31.168.101.163	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
62.0.100.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
207.232.27.5	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
77.127.6.62	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
138.134.102.15	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
84.228.175.51	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
105.230.128.22	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
213.139.52.25	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
138.134.102.16	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
147.236.138.210	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.139.53.7	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
77.126.128.193	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
5.28.178.92	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.120.148.145	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
193.106.52.37	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
87.95.118.116	Finland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
86.27.92.192	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
31.154.92.63	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.250.27.68	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.108.114.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
2.54.166.61	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.181.54.92	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
148.251.182.223	Germany	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
84.228.113.156	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.243	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.25.102.63	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.203	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
121.222.240.189	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.29.208.81	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.178.53.126	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.94	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.139.50.19	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
77.126.128.193	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
117.223.26.39	India	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.190	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.32	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.105	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.102.135.78	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.40	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.250.254.177	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.110.109.23	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.183.132.104	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
46.116.101.60	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.67.1.172	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
197.248.141.142	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.183.154.232	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
167.220.196.189	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.13	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.116.178.140	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-15-2015-00:00:07 to 07-16-2015-00:00:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	105
46.19.86.119	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	93
99.48.176.9	United States	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
175.142.168.165	Malaysia	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	12
148.251.182.223	Germany	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	8
78.167.75.61	Turkey	147.237.76.86	navy.idf.il	SERVER-WEBAPP admin.php access	4
66.249.79.51	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.40	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
46.118.119.63	Ukraine	147.237.77.176	matpash.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	3
37.115.187.54	Ukraine	147.237.77.74	law.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	3
188.119.20.111	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	3
78.167.75.61	Turkey	147.237.76.86	navy.idf.il	SERVER-WEBAPP adminlogin access	3
130.193.196.93	Iraq	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	3
37.115.187.54	Ukraine	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	3
5.39.216.121	Netherlands	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.239	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
218.65.30.107	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
46.19.86.174	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
218.65.30.107	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
223.130.24.20	Australia	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
176.12.138.72	Israel	147.237.76.31	nakchal.idf.il	INDICATOR-SCAN myscan	2
128.30.52.73	United States	147.237.76.86	navy.idf.il	Tehila - Perl LWP with fake user agent	2
113.240.250.156	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.79.25	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
208.80.155.213	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
218.65.30.107	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.37	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
218.65.30.107	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
62.212.73.138	Netherlands	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
82.205.108.4	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
176.12.138.72	Israel	147.237.76.31	nakchal.idf.il	GPL SCAN myscan	2
218.65.30.107	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
222.187.98.36	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
80.82.70.239	Netherlands	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.65.30.107	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
58.211.5.189	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
189.2.52.130	Brazil	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.157	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.203.8	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.111.107	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
203.100.83.32	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.116.182.142	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
123.164.227.202	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
54.157.25.107	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
168.187.246.41	Kuwait	147.237.77.234	halag.idf.il	ET SCAN NMAP -f -sS	1
112.84.178.18	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

07-15-2015-00:00:07 to 07-16-2015-00:00:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.221.3	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11043
105.104.11.80	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3175
78.24.216.43	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2365
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2132
84.109.98.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2061
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1926
23.236.125.64	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1385
213.151.60.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1337
81.218.50.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	992
85.64.77.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	807
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	776
62.207.60.229	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	742
109.253.35.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	732
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	627
95.86.80.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	625
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	623
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	621
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	616
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	605
168.235.196.145		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	566
158.82.202.5	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	459
109.186.0.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	450
66.249.64.178	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	439
168.235.197.149		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	438
46.19.86.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	422
148.167.2.30	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	422
66.249.64.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	415
66.249.64.168	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	405
46.210.168.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	392
46.19.85.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	392
79.183.8.38	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	379
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	359
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	354
132.66.40.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	341
95.86.70.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	335
105.0.224.230		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	323
188.165.15.193	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	323
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	311
66.249.64.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	297
71.201.156.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	293
66.249.64.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	291
70.199.106.250	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	289
66.249.64.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	275
68.180.228.176	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	270
207.46.13.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	265
37.231.183.114	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	249
1.254.6.66	Korea, Republic of	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	249
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	241
46.19.86.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	227
66.87.123.189	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	224

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.120.148.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	502
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	377
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	360
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	357
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	317
46.19.85.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	211
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	191
176.13.11.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
176.12.142.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
46.19.85.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	107
109.253.128.250	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.128.250	Block	99
78.167.75.61	Turkey	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 78.167.75.61	Block	97
2.54.33.121	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.33.121	Block	97
78.167.75.61	Turkey	147.237.76.86	navy.idf.il	PHP Attempt	Block	74
185.32.178.86	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.178.86	Block	72
2.54.0.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
167.114.64.100	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 167.114.64.100	Block	71
2.52.32.165	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.32.165	Block	64
80.246.136.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
78.167.75.61	Turkey	147.237.76.86	navy.idf.il	Multiple Admin Blocking from 78.167.75.61	Block	45
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	43
176.13.9.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
37.59.29.19	France	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 37.59.29.19	Block	40
84.94.85.251	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	40
2.54.33.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	24
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	23
77.126.142.171	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	23
105.104.11.80	Algeria	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	23
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.92	Block	22
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	22
202.63.164.104	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	20
78.167.75.61	Turkey	147.237.76.86	navy.idf.il	Parameter Type Violation f in www.navy.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	19
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.89	Block	15
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.95	Block	15
149.88.186.164	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.186.164	Block	12
78.167.75.61	Turkey	147.237.76.86	navy.idf.il	Parameter Type Violation SessionCode in www.navy.idf.il/shared/ajax/createcaptchaimage.aspx	Block	11
78.167.75.61	Turkey	147.237.76.86	navy.idf.il	Parameter Type Violation rnd in www.navy.idf.il/shared/ajax/createcaptchaimage.aspx	Block	11
27.126.188.85	Hong Kong	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	10
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	10
95.86.71.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
113.175.64.173	Vietnam	147.237.76.86	navy.idf.il	PHP Attempt	Block	9
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	9
77.125.133.128	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 77.125.133.128	Block	8
176.13.20.213	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
79.178.26.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
68.180.230.113	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	7
79.181.200.75	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7

07-15-2015-00:00:07 to 07-16-2015-00:00:07