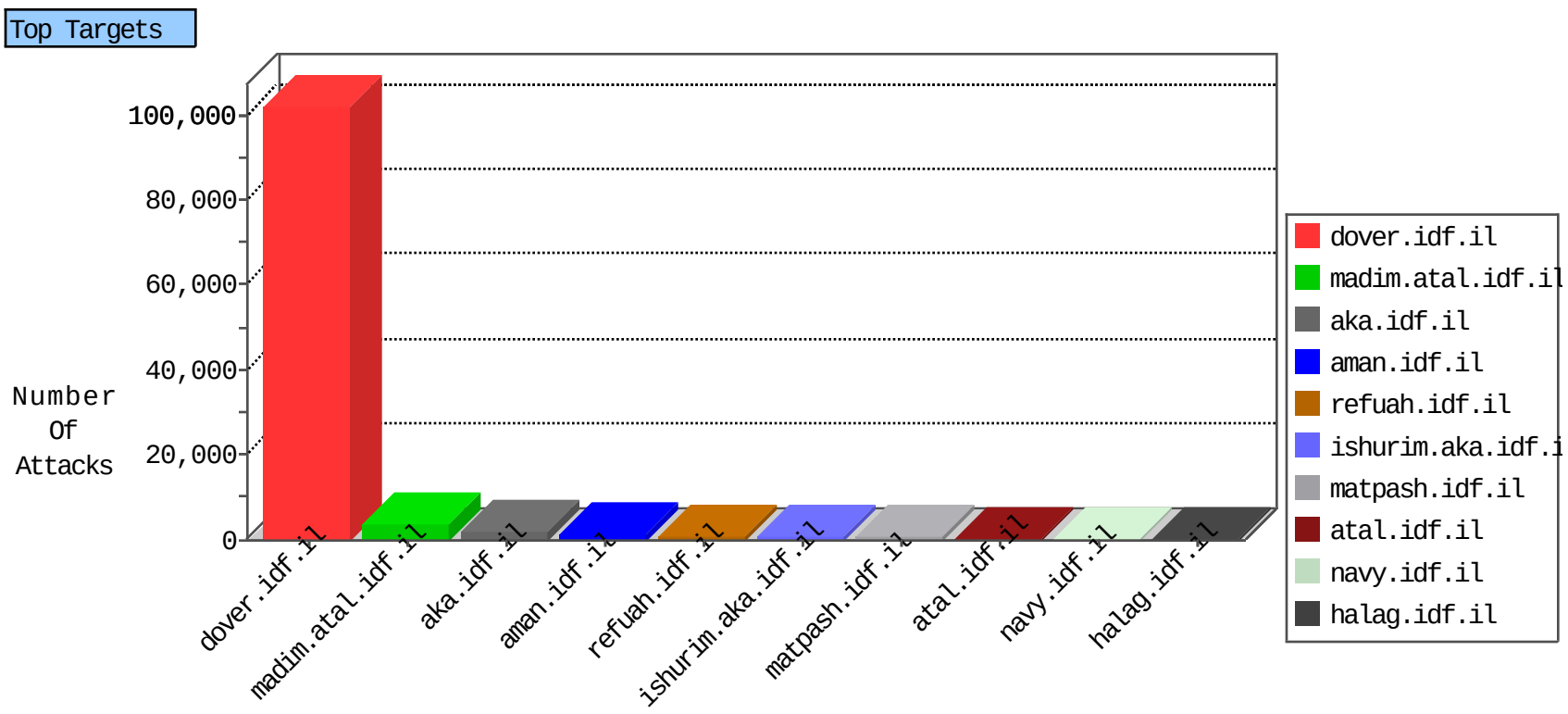
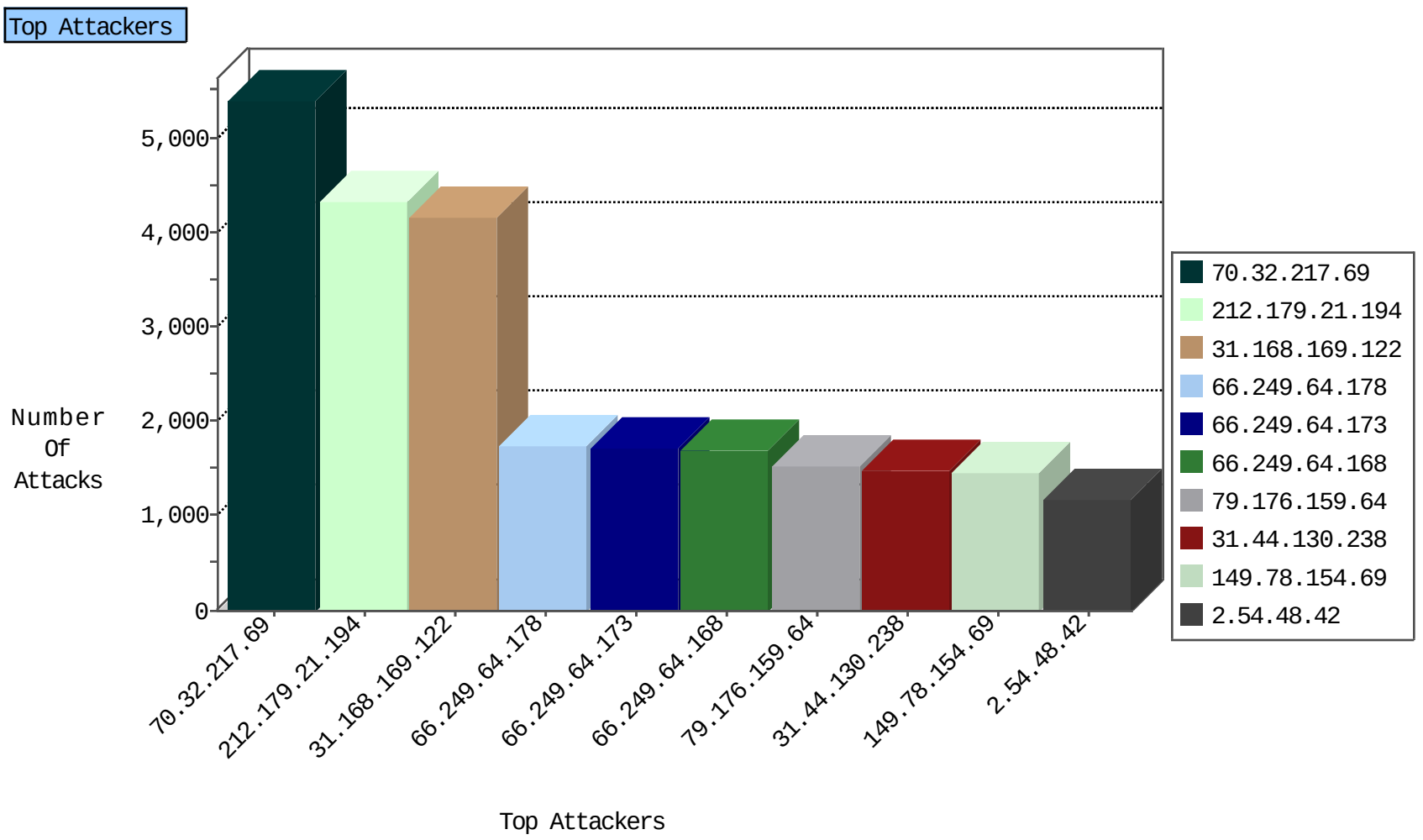
07-09-2015-00:00:02 to 07-10-2015-00:00:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



07-09-2015-00:00:02 to 07-10-2015-00:00:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2606
176.12.147.35	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2563
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	2221
79.179.195.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1224
37.142.204.207	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	797
77.127.204.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	690
79.176.21.196	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	687
5.29.18.244	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	687
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	562
79.176.108.119	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	508
79.181.58.15	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	452
94.159.171.73	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	448
37.142.213.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	447
93.172.222.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	402
213.57.209.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	385
79.176.182.49	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	375
84.109.2.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	340
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	320
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	317
37.142.9.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	307
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	249
85.65.57.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	239
79.181.208.251	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	221
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	211
109.186.6.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	209
79.179.139.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	198
85.65.48.15	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	191
86.184.122.26	United Kingdom	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	187
79.183.17.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
84.108.9.189	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	178
5.144.59.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
220.181.108.144	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	176
94.159.156.236	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
62.219.160.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
87.69.205.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
213.57.228.145	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
84.228.103.82	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
77.125.151.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
79.181.138.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
5.29.117.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
81.218.2.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
2.54.26.255	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
109.67.184.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
46.19.86.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	139
46.19.86.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	135
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
79.176.80.209	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	129

07-09-2015-00:00:02 to 07-10-2015-00:00:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
92.241.40.225	Jordan	147.237.77.216	dover.idf.il	C017: HTTP: Malicous UserAgent FOCA	Block	34
79.176.182.49	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	18
213.139.53.10	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
213.139.53.10	Jordan	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
77.127.204.103	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
79.182.21.90	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
213.139.52.82	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.178.122.4	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.181.216.137	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
24.76.249.149	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
89.138.238.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.89	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.165	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.253.118.65	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
199.189.81.36	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.183.20.24	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.109.153.176	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.67.21.70	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.100	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.232	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.67.134.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.102	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.64.184.161	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.57	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.116.227.123	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
185.93.187.51		147.237.77.176	matpash.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	2
80.246.130.3	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.214	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.239	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.66.111.94	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
213.151.39.138	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.11	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
128.248.201.22	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.64.58.199	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.181.164.135	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.125.240.145	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
199.203.151.37	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.43	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
89.139.5.57	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.26.147.178	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.254	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
79.183.205.64	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.195	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
103.53.225.47		147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
79.178.20.83	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

07-09-2015-00:00:02 to 07-10-2015-00:00:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
70.32.217.69	United States	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5267
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	60
213.57.174.63	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	36
109.160.240.160	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	14
176.12.136.215	Israel	147.237.77.216	dover.idf.il	SERVER-WEBAPP generic server HTTP Auth Header buffer overflow attempt	7
80.246.136.207	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
109.253.142.96	Israel	147.237.77.216	dover.idf.il	SERVER-WEBAPP generic server HTTP Auth Header buffer overflow attempt	4
37.115.187.54	Ukraine	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	3
218.87.111.107	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	3
46.229.164.101	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
221.203.3.117	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
5.57.6.27	Lebanon	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
221.203.3.117	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	Germany	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
79.180.142.236	Israel	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
221.203.3.117	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
188.121.41.143	Netherlands	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
218.87.111.107	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
199.203.59.121	Israel	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
92.241.40.225	Jordan	147.237.77.216	dover.idf.il	SERVER-WEBAPP .DS_Store access	2
5.199.172.154	Lithuania	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
103.225.220.163	Pakistan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
221.203.3.117	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
210.61.150.154	Taiwan	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
183.230.17.149	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
42.62.49.167	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
222.219.187.9	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.77.192.156	Saudi Arabia	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.111.107	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
79.177.147.104	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
200.195.135.82	Brazil	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 4096	1
58.240.33.163	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
124.207.3.67	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.156.8.189	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.167.112.16		147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
221.203.3.117	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
89.138.8.41	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.65.30.107	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
66.18.250.29	Canada	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
193.238.152.34	Ukraine	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.211.254	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

07-09-2015-00:00:02 to 07-10-2015-00:00:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
31.168.169.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4161
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4145
79.176.159.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1521
31.44.130.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1483
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1462
2.54.48.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1168
109.67.49.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1030
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	896
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	829
95.86.109.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	823
94.71.73.252	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	697
46.19.85.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	688
46.19.85.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	667
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	666
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	658
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	632
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	626
109.186.0.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	567
66.249.64.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	528
178.77.160.73	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	508
66.249.64.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	507
38.111.147.88	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	504
66.249.64.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	492
77.127.147.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	485
62.201.200.194	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	473
2.54.39.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	469
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	421
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	408
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	398
188.165.15.195	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	398
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	388
68.180.229.178	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	380
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	368
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	362
85.250.108.225	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	341
37.26.146.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	333
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	320
83.111.230.90	United Arab Emirates	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	311
46.19.85.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	302
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	298
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	270
178.135.118.18	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	270
109.65.116.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	267
70.39.187.5	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	262
79.179.134.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	242
2.54.137.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	240
66.249.84.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	232
87.69.126.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	221
66.249.64.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	216
195.34.150.18	Austria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	216

07-09-2015-00:00:02 to 07-10-2015-00:00:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.246.136.207	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.207	Block	766
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	590
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	553
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	552
77.127.224.57	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.127.224.57	Block	355
46.19.85.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	300
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	285
176.13.13.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	281
176.13.4.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	264
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	211
62.90.131.82	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 62.90.131.82	Block	180
176.12.145.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	173
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	173
212.150.214.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
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	103
185.32.178.228	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.178.228	Block	98
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	97
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	96
2.54.21.134	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.21.134	Block	87
2.54.41.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
31.168.164.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
46.19.86.215	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.215	Block	65
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.25	Block	61
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.160.240.11	Block	55
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	46
79.176.107.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
58.62.235.208	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 58.62.235.208	Block	33
46.116.133.201	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.116.133.201	Block	32
79.179.135.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	27
58.62.235.208	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	23
46.19.86.167	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.167	Block	19
176.13.16.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
77.127.92.23	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.92.23	Block	16
89.138.16.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.16.113	Block	16
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_bottom.asp	Block	15
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_bottom.asp	Block	15
37.26.148.171	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	12
5.28.181.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.28.181.113	Block	12
79.180.154.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
79.182.219.217	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	10
87.69.54.178	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.54.178	Block	9
212.179.42.241	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.42.241	Block	9
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	8
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	Block	8
46.117.73.249	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	7
79.181.52.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
176.12.149.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
5.29.81.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
77.125.210.94	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	7
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	6

07-09-2015-00:00:02 to 07-10-2015-00:00:02