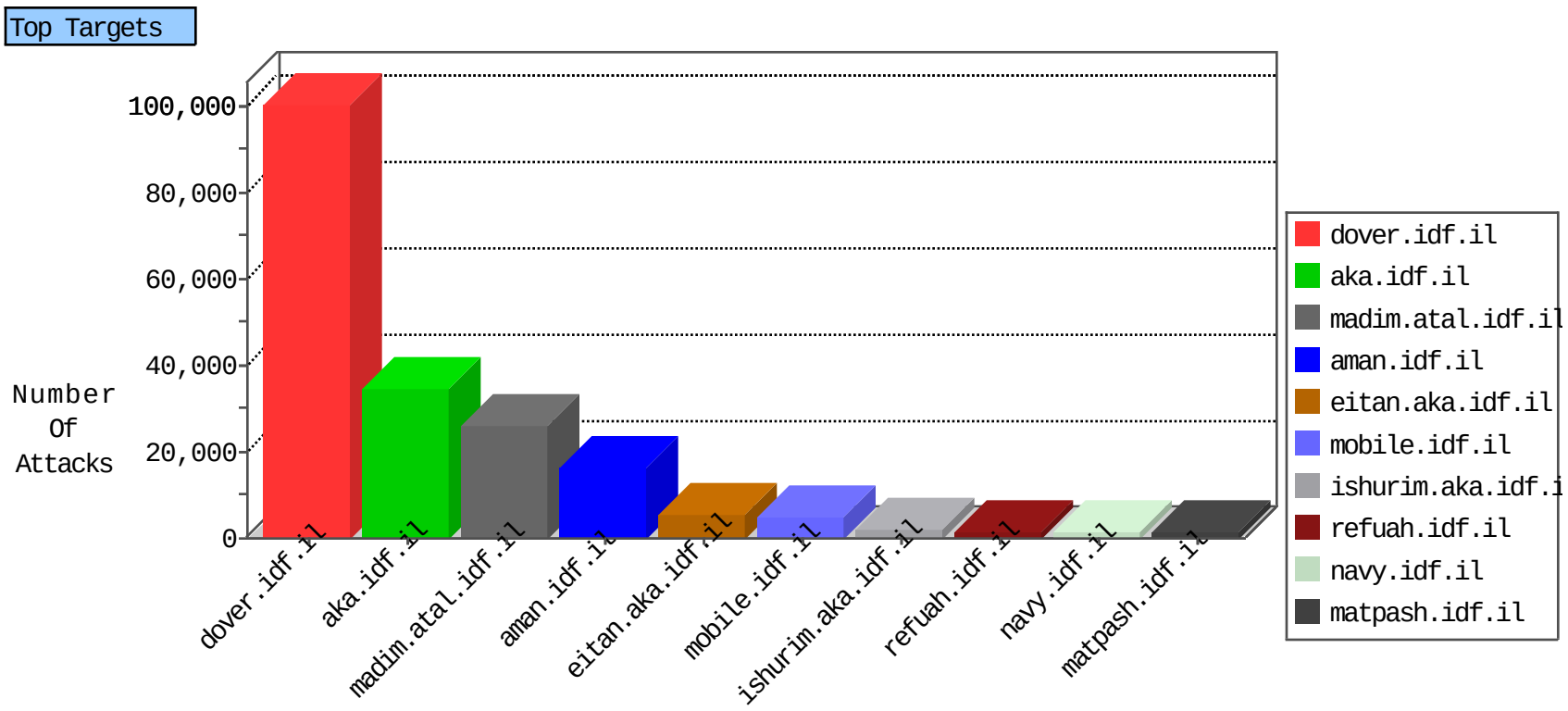
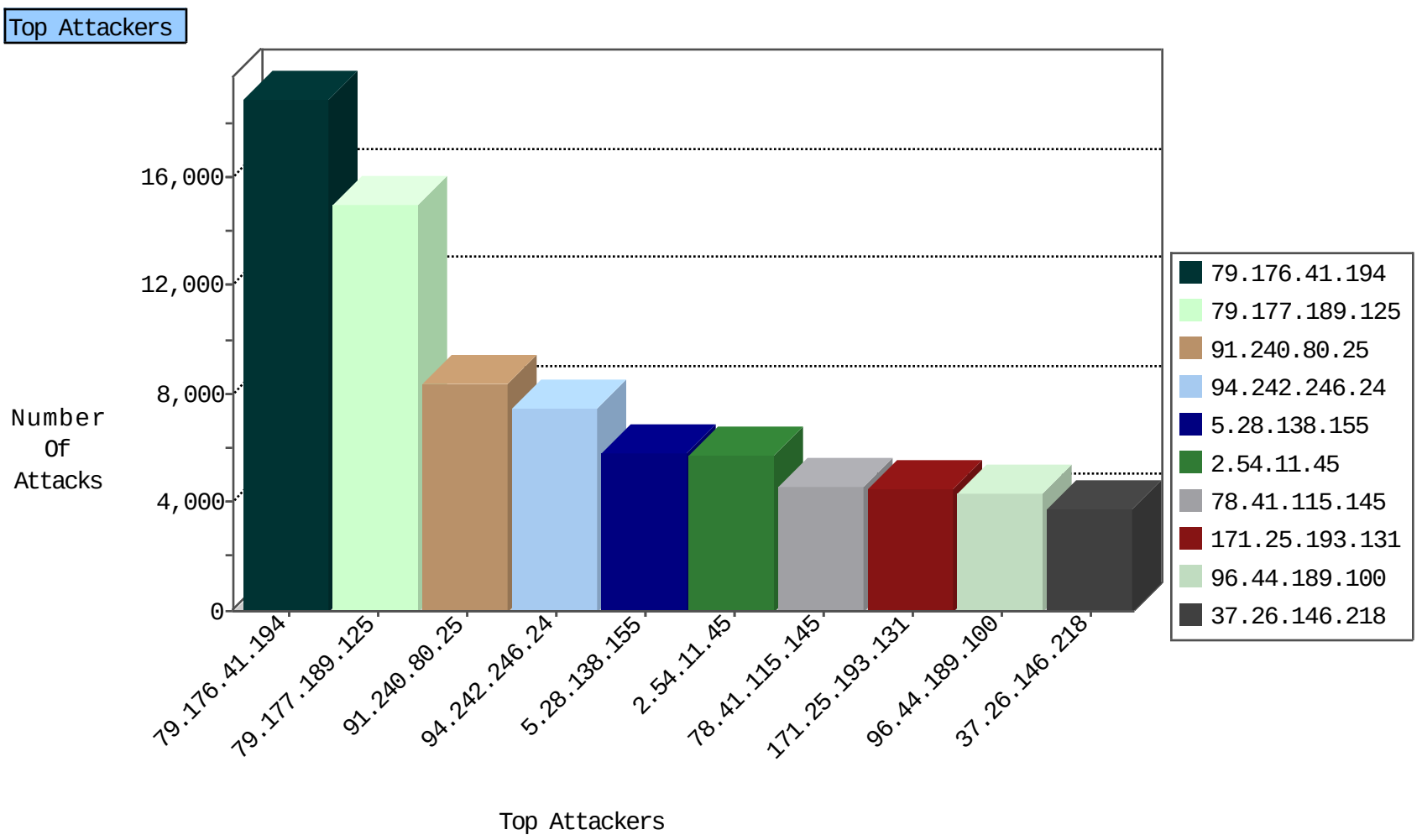
09-30-2015-00:00:04 to 10-01-2015-00:00:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-30-2015-00:00:04 to 10-01-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	7879
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4175
66.249.78.160	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3948
68.56.233.252	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1347
91.240.80.25	Lebanon	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1308
66.249.78.146	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	758
66.249.79.211	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	424
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	381
66.249.79.238	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	265
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	244
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	230
66.249.67.81	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	216
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	214
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	211
37.26.149.232	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	168
109.64.37.79	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	151
185.32.179.82	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	149
66.249.79.218	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	142
46.116.169.59	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	141
2.54.31.51	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	125
149.78.21.209	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	113
2.54.149.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	109
213.57.80.126	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	96
41.129.218.165	Egypt	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	86
79.182.210.68	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	83
109.65.20.13	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	79
77.125.80.162	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	79
46.19.85.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	79
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	73
2.54.42.182	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	71
46.19.85.198	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	71
37.26.147.240	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	71
2.52.128.53	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	61
46.19.85.99	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	59
93.172.80.112	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	48
185.32.179.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	46
2.54.133.248	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	46
37.26.149.239	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	46
46.19.85.11	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	46
80.246.139.61	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	44
37.252.230.59	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	42
77.126.2.178	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	42
31.210.186.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	41
2.54.7.64	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	40
80.246.139.82	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	38
185.32.179.196	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	36
66.249.64.151	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	35
37.142.68.76	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	35
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	34
46.19.85.63	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	30

09-30-2015-00:00:04 to 10-01-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.113.143	France	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	14
109.163.234.2	Romania	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	10
109.163.234.2	Romania	147.237.77.216	dover.idf.il	1178: HTTP: srchadm cgi Access	Permit	8
109.163.234.2	Romania	147.237.77.216	dover.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	6
108.67.169.124	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
23.91.121.130	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
189.38.90.189	Brazil	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
62.210.225.135	France	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
74.208.133.60	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
184.168.193.34	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
212.180.240.172	Poland	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
91.197.103.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
23.91.122.26	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
91.142.253.133	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
83.169.8.217	Germany	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
109.163.234.2	Romania	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	3
109.163.234.2	Romania	147.237.77.216	dover.idf.il	0893: HTTP: smssend.php Access	Permit	3
46.137.81.122	Ireland	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
84.228.21.122	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
174.139.243.58	United States	147.237.77.170	maarachot.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
81.89.96.88	Germany	147.237.77.216	dover.idf.il	1008: HTTP: nlog-smb Access	Block	2
84.228.123.94	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
193.106.206.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.163.234.2	Romania	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	2
81.218.245.1	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
198.143.164.7	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
80.230.39.207	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
213.108.203.70	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
91.240.80.25	Lebanon	147.237.77.216	dover.idf.il	12371: TCP: Hulk DDoS Tool	Block	1
209.159.138.19	United States	147.237.77.216	dover.idf.il	0360: HTTP: Protected Directory Access (~root)	Block	1
189.38.80.50	Brazil	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
114.27.224.74	Taiwan	147.237.77.176	matpash.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
46.137.81.122	Ireland	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
108.67.169.124	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
176.10.99.200	Switzerland	147.237.77.216	dover.idf.il	0495: HTTP: Shell Command Execution (cmd.exe)	Block	1
23.91.122.26	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	C1000158: HTTP(S): Hacked in the Payload	Block	1
209.159.138.19	United States	147.237.77.216	dover.idf.il	0863: HTTP: fpadmcgi.exe Access	Block	1
189.38.80.50	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
142.4.214.124	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
51.254.131.243	United Kingdom	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
2.94.19.99	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
109.163.234.2	Romania	147.237.77.216	dover.idf.il	0819: HTTP: admin.pl Access	Block	1
198.20.69.74	United States	147.237.8.14	e.orchot.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
176.10.99.200	Switzerland	147.237.77.216	dover.idf.il	C067: HTTP: attempt to access .config page	Block	1
37.214.6.225	Belarus	147.237.72.166	aka.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
209.159.138.19	United States	147.237.77.216	dover.idf.il	1185: HTTP: IIS admcgi CGI Access	Block	1
95.215.68.121	Russian Federation	147.237.77.176	matpash.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
189.38.90.189	Brazil	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

09-30-2015-00:00:04 to 10-01-2015-00:00:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.240.80.25	147.237.77.216	Lebanon	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1283
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	89
198.143.164.7	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	19
108.67.169.124	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	18
109.163.234.2	147.237.77.216	Romania	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	15
91.240.80.25	147.237.77.216	Lebanon	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	14
68.56.233.252	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	14
62.210.225.135	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	12
83.169.8.217	147.237.76.86	Germany	navy.idf.il	SQL Injection - Select From	12
189.38.90.189	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	11
23.91.121.130	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
176.12.146.233	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
91.142.253.133	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	6
74.208.133.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
67.55.73.76	147.237.72.166	United States	aka.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	6
66.249.67.79	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	6
23.91.122.26	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
189.38.80.50	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
109.163.234.2	147.237.77.216	Romania	dover.idf.il	SERVER-IIS viewcode.asp access	6
212.180.240.172	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	6
46.137.81.122	147.237.76.31	Ireland	nakchal.idf.il	SQL Injection - Select From	6
189.38.90.189	147.237.72.166	Brazil	aka.idf.il	SQL Injection - Select From	6
184.168.193.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.79.211	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
209.159.138.19	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP Novell Groupwise gwweb.exe access	4
66.249.78.160	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.79.231	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
78.129.196.161	147.237.72.166	United Kingdom	aka.idf.il	Tehila - Perl LWP with fake user agent	4
66.102.9.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
218.87.111.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	3
218.87.111.117	147.237.0.19	China	madim.atal.idf.i	ET SCAN Potential SSH Scan	3
66.249.64.151	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
66.249.78.172	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.78.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
41.240.225.22	147.237.77.216	Sudan	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.163.234.2	147.237.77.216	Romania	dover.idf.il	SERVER-IIS viewcode access	2
94.242.246.24	147.237.77.216	Luxembourg	dover.idf.il	SERVER-WEBAPP RBS ISP /newuser access	2
109.163.234.2	147.237.77.216	Romania	dover.idf.il	SERVER-IIS /SiteServer/Publishing/viewcode.asp access	2
182.100.67.4	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	2
213.204.127.27	147.237.77.170	Lebanon	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
31.179.192.119	147.237.77.227	Poland	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.85.164	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
193.107.17.72	147.237.0.34	Seychelles	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
182.100.67.4	147.237.72.14	China	dover.idf.il(old	ET SCAN Potential SSH Scan	2
176.10.99.200	147.237.77.216	Switzerland	dover.idf.il	SERVER-WEBAPP files.pl access	2

09-30-2015-00:00:04 to 10-01-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.240.80.25	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5507
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1732
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1730
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1394
46.19.86.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1348
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1026
212.235.22.158	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	960
77.125.1.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	906
95.86.112.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	869
155.56.68.217	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	766
109.64.167.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	752
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	738
78.41.115.145	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	730
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	710
96.44.189.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	683
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	664
79.179.106.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	650
66.249.79.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	640
212.76.103.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	620
134.159.156.68	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	620
168.235.196.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	614
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	601
46.19.86.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	588
66.249.79.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	582
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	562
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	556
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	538
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	534
77.125.134.7	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	534
66.249.79.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	518
91.240.80.25	Lebanon	147.237.77.216	dover.idf.il	drop	SAM rule	drop	503
79.180.36.162	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	498
37.26.147.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	482
84.108.49.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	471
37.26.147.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	468
109.186.168.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	451
5.22.129.134	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	447
85.64.137.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	435
91.240.80.25	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	428
91.240.80.25	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	426
46.19.86.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	420
109.160.191.53	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	411
89.138.220.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	401
78.41.115.145	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	353
96.44.189.100	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	329
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	323
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
109.226.22.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	302
82.166.22.133	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	285
82.132.232.213	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	277

09-30-2015-00:00:04 to 10-01-2015-00:00:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.41.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	18770
79.177.189.125	Israel	147.237.72.156	aman.idf.il	Too Many of the Same Response Code (404) in IP from 79.177.189.125	Block	15044
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.242.246.24	Block	5972
5.28.138.155	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.28.138.155	Block	5855
2.54.11.45	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.11.45	Block	5717
37.26.146.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3765
37.26.149.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3538
78.41.115.145	Austria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.41.115.145	Block	3520
96.44.189.100	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 96.44.189.100	Block	3290
37.26.146.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2778
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 171.25.193.131	Block	2640
79.182.114.96	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.114.96	Block	1354
209.159.138.19	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 209.159.138.19	Block	1285
109.65.20.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1228
212.235.22.158	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.235.22.158	Block	1110
46.120.184.9	Israel	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 46.120.184.9	Block	745
37.26.146.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	737
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.115.95.204	Block	540
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	496
80.246.139.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	400
185.32.179.80	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.80	Block	326
109.163.234.2	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.163.234.2	Block	290
5.22.129.134	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 5.22.129.134	Block	275
176.10.99.200	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.10.99.200	Block	250
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	242
84.94.174.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.174.194	Block	240
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	207
81.89.96.88	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.89.96.88	Block	190
79.180.166.156	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.166.156	Block	187
66.249.79.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.231	Block	180
37.26.146.242	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.242	Block	165
188.165.15.79	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.79	Block	160
66.249.79.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.238	Block	160
176.13.0.255	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	153
77.125.158.2	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	139
79.178.119.34	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	132
2.54.37.12	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	130
185.32.179.51	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.51	Block	130
45.35.20.205		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	121
45.35.20.205		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.35.20.205	Block	121
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	120
93.173.40.87	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	117
79.176.41.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.41.194	Block	110
46.121.60.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.60.250	Block	109
46.19.86.67	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	100
109.64.96.180	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	100
149.78.34.83	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	99
176.12.142.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	96
176.13.4.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
208.115.111.72	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	82

09-30-2015-00:00:04 to 10-01-2015-00:00:04