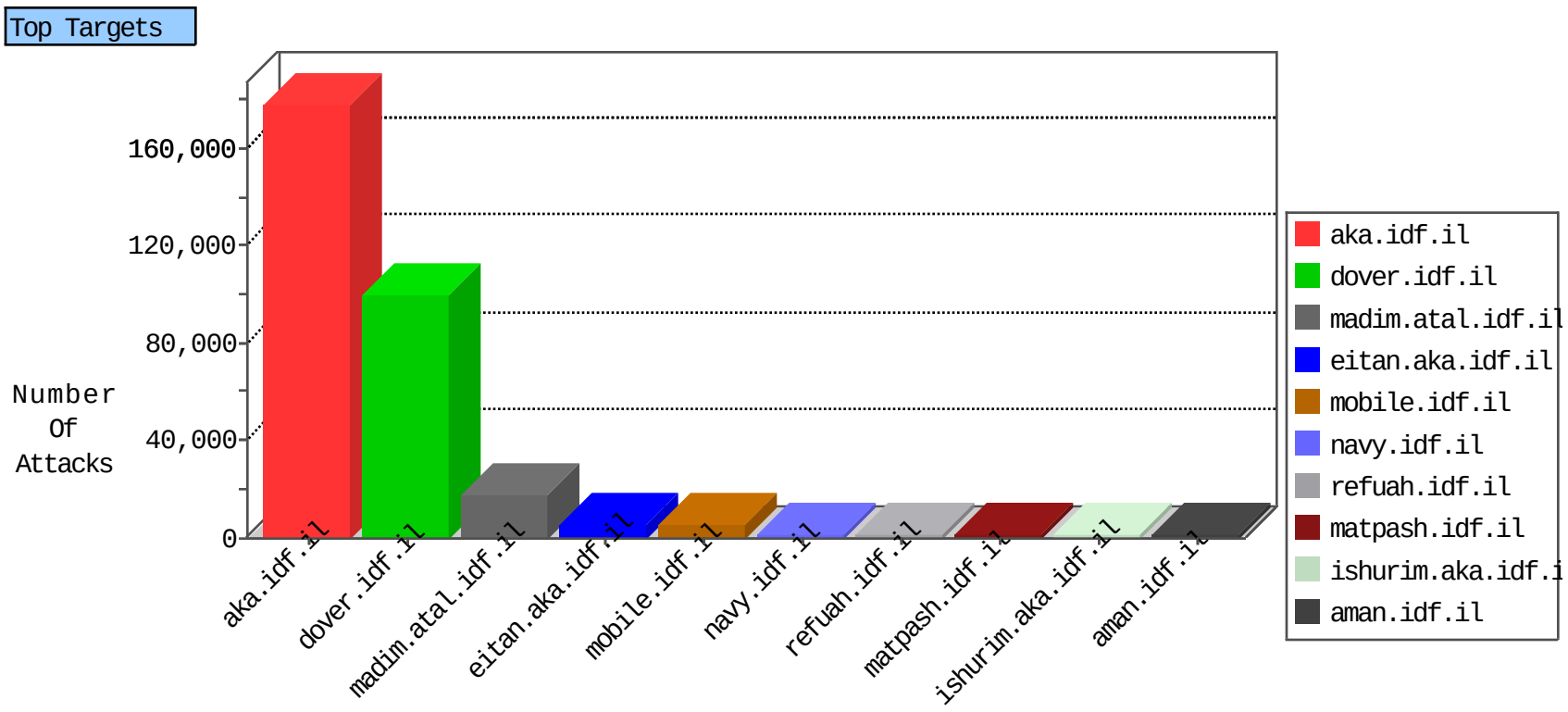
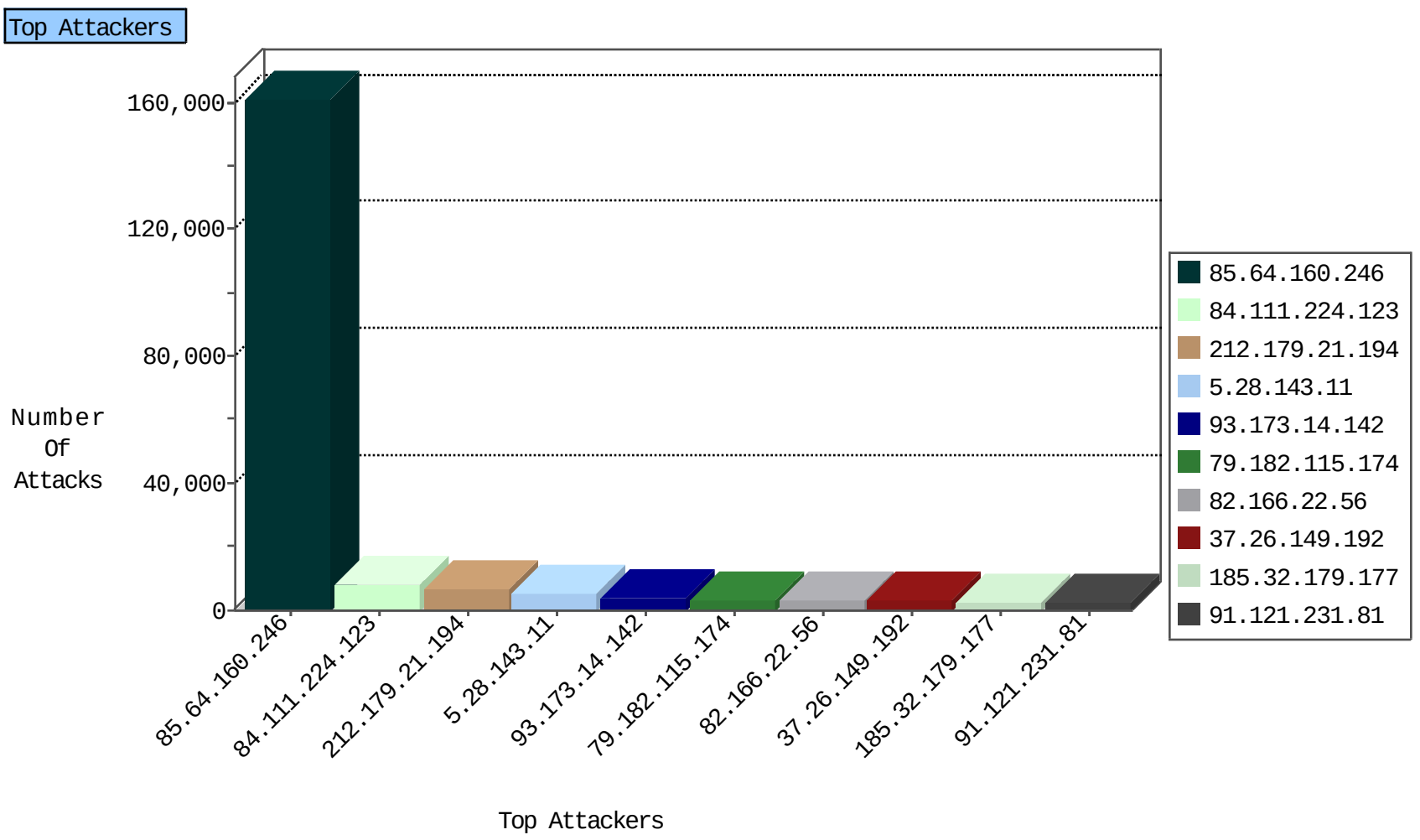
09-29-2015-00:00:06 to 09-30-2015-00:00:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2015-00:00:06 to 09-30-2015-00:00:06

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-POST-Segmented-DoS	dest-reset	12460
66.249.64.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7297
93.102.248.170	Portugal	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5280
37.252.248.93	Germany	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	5146
187.75.227.19	Brazil	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4329
91.121.231.81	France	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4191
66.249.78.160	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3173
66.249.78.146	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3050
66.249.65.179	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2803
5.102.254.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2546
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2312
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	656
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	514
37.26.149.203	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	376
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	245
85.250.100.162	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	190
31.154.92.8	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	172
89.139.24.37	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	161
2.54.188.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	141
66.249.79.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	120
212.199.57.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	114
2.52.146.221	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	113
79.181.48.97	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	94
46.19.86.61	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
5.102.254.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	91
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	89
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
149.78.223.188	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
87.68.49.219	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	66
149.202.112.63	Germany	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	58
2.54.139.19	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	53
37.26.148.146	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	44
46.19.86.178	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	44
94.70.168.47	Greece	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	44
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	43
109.65.141.230	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	36
2.54.28.227	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	36
79.182.127.207	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	36
46.19.85.178	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	36
46.148.18.74	Lithuania	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	32
176.228.82.193	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	30
92.222.113.177	France	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	29
50.170.130.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24
79.182.210.68	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	24
94.70.168.47	Greece	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	source-dest-reset	23
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22
1.136.96.15	Australia	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	source-dest-reset	21
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
85.10.210.199	Germany	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	20
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	20

09-29-2015-00:00:06 to 09-30-2015-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.168.97	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
212.180.240.172	Poland	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
108.168.219.166	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
85.136.227.77	Spain	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
92.241.60.82	Jordan	147.237.77.216	dover.idf.il	1072: FPSE: service.pwd Access	Permit	4
76.74.252.117	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
79.178.126.54	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.176.134.238	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.66.188.140	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
93.172.174.185	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
87.69.228.116	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.221.133.130	Iceland	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
178.137.91.69	Ukraine	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
91.76.247.0	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
193.173.21.236	Netherlands	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
62.210.250.215	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
149.202.112.63	Germany	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
92.241.60.82	Jordan	147.237.77.216	dover.idf.il	1070: FPSE: administrators.pwd Access	Block	1
5.135.158.101	France	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
213.8.81.18	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
185.14.29.221	Netherlands	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
78.37.153.15	Russian Federation	147.237.77.176	matpash.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
46.19.86.231	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
2.94.19.99	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
91.121.231.81	France	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	1
193.201.224.8	Ukraine	147.237.77.176	matpash.idf.il	C1000196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
69.162.139.9	United States	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
24.230.181.31	United States	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
87.69.201.58	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.26.87.113	Romania	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
78.46.174.197	Germany	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	Block	1
46.165.230.5	Germany	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
109.111.159.86	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
2.94.19.99	Russian Federation	147.237.72.167	ishurim.aka.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
91.198.204.122	Denmark	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.74	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
162.221.184.64	United States	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
37.187.7.74	France	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
188.138.9.49	Germany	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
79.98.107.90	Bulgaria	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
149.78.208.157	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
5.9.36.66	Germany	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
91.219.236.222	Hungary	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
82.165.24.123	Germany	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
209.249.180.198	United States	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
176.31.51.199	Spain	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1

09-29-2015-00:00:06 to 09-30-2015-00:00:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.202.112.62	147.237.77.216	Germany	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	453
149.202.112.62	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	449
149.202.112.62	147.237.77.216	Germany	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	449
149.202.112.62	147.237.77.216	Germany	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	425
149.202.112.63	147.237.77.216	Germany	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	269
149.202.112.63	147.237.77.216	Germany	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	245
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	228
149.202.112.62	147.237.77.216	Germany	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	202
149.202.112.62	147.237.77.216	Germany	dover.idf.il	SQL generic sql with comments injection attempt - GET parameter	172
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	86
46.28.68.158	147.237.77.216	Ukraine	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	56
46.28.68.158	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	52
149.202.112.62	147.237.77.216	Germany	dover.idf.il	SQL waitfor delay function - possible SQL injection attempt	44
149.202.112.63	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	37
149.202.112.63	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	36
66.249.93.138	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	29
46.28.68.158	147.237.77.216	Ukraine	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	21
46.28.68.158	147.237.77.216	Ukraine	dover.idf.il	SQL generic sql with comments injection attempt - GET parameter	21
46.28.68.158	147.237.77.216	Ukraine	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	21
188.138.9.49	147.237.77.216	Germany	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	19
188.138.9.49	147.237.77.216	Germany	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	19
188.138.9.49	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	19
66.249.93.130	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	18
188.138.9.49	147.237.77.216	Germany	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	15
82.165.24.123	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	15
149.202.112.63	147.237.77.216	Germany	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	15
91.121.231.81	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP backup access	13
149.202.112.62	147.237.77.216	Germany	dover.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	13
66.249.78.160	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	12
149.202.112.63	147.237.77.216	Germany	dover.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	12
149.202.112.63	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER SQL Injection Select Sleep Time Delay	11
37.252.248.93	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	11
149.202.112.63	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	11
149.202.112.62	147.237.77.216	Germany	dover.idf.il	SQL generic convert injection attempt - GET parameter	11
213.204.103.26	147.237.76.30	Lebanon	himush.idf.il	ET SCAN NMAP -sA (2)	10
149.202.112.63	147.237.77.216	Germany	dover.idf.il	SQL generic convert injection attempt - GET parameter	10
46.28.68.158	147.237.77.216	Ukraine	dover.idf.il	SQL waitfor delay function - possible SQL injection attempt	10
82.165.24.123	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	9
91.121.231.81	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP PHP-CGI remote file include attempt	9
82.165.24.123	147.237.77.216	Germany	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	9
82.165.24.123	147.237.77.216	Germany	dover.idf.il	SQL generic sql update injection attempt - GET parameter	9
91.121.231.81	147.237.77.216	France	dover.idf.il	ET WEB_SERVER safe_mode PHP config option in uri	9
91.121.231.81	147.237.77.216	France	dover.idf.il	ET WEB_SERVER disable_functions PHP config option in uri	9
149.202.112.63	147.237.77.216	Germany	dover.idf.il	SQL waitfor delay function - possible SQL injection attempt	9
82.165.24.123	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	9
91.121.231.81	147.237.77.216	France	dover.idf.il	ET WEB_SERVER allow_url_include PHP config option in uri	9
82.165.24.123	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	9
82.165.24.123	147.237.77.216	Germany	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	9
82.165.24.123	147.237.77.216	Germany	dover.idf.il	SQL declare varchar - possible SQL injection attempt	9
91.121.231.81	147.237.77.216	France	dover.idf.il	ET WEB_SERVER suhosin.simulation PHP config option in uri	9

09-29-2015-00:00:06 to 09-30-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.111.224.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7833
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6273
93.173.14.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3536
79.182.115.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3487
82.166.22.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3234
187.75.227.19	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2167
91.121.231.81	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1689
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1541
46.120.154.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1461
164.138.122.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1328
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1215
37.26.149.192	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1110
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	760
46.19.86.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	697
188.165.15.79	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	655
146.185.134.40	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	650
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	606
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	604
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	599
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	585
46.19.85.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	498
66.249.64.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	490
66.249.64.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	490
2.54.60.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	487
84.108.75.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	458
37.142.68.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	453
2.54.40.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	452
89.138.220.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	450
77.125.1.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	440
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	409
46.121.96.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	406
164.97.245.84	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	388
109.66.117.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	386
2.54.1.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	378
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	373
46.19.85.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	371
66.249.64.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	370
46.248.215.251	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	330
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	329
164.215.110.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	301
79.181.180.68	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	300
77.127.227.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	299
109.67.248.100	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	291
77.125.134.7	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
176.106.226.194	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
62.90.2.56	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	252
128.69.142.136	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	252
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	252
37.216.10.244	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	244
8.37.227.173	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	243

09-29-2015-00:00:06 to 09-30-2015-00:00:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.160.246	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	107467
85.64.160.246	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.160.246	Block	53853
5.28.143.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5480
185.32.179.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2610
84.95.228.36	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.95.228.36	Block	2427
37.26.149.192	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.149.192	Block	1875
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1655
217.132.195.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 217.132.195.199	Block	890
176.13.10.1	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.10.1	Block	875
176.13.21.30	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.21.30	Block	850
93.173.147.222	Israel	147.237.76.86	navy.idf.il	Too Many of the Same Response Code (404) in Session from 93.173.147.222	Block	690
37.142.125.80	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.125.80	Block	650
80.246.139.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	441
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	370
185.32.179.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	370
188.165.15.79	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.79	Block	360
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	340
2.52.147.172	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.147.172	Block	338
46.116.187.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	270
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	270
185.32.179.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	250
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	240
46.120.184.9	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.184.9	Block	210
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	210
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	200
66.249.79.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.231	Block	140
176.12.151.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	130
84.108.122.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	108
176.13.22.78	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	100
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	100
46.19.85.223	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	100
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	100
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	100
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	100
80.246.136.28	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
212.179.61.123	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.61.123	Block	90
66.249.79.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.238	Block	90
176.12.149.232	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	90
213.57.226.203	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.226.203	Block	90
79.182.127.148	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	80
37.26.146.219	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	80
176.12.142.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	70
176.106.227.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/highstairs-a.akamaihd.net/a24/utils/js/highstairsly9oawdoc3rhaxjzlweuywthbwfpagqubmv0l2eyna272	Block	70
176.13.14.25	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	70
2.52.2.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	70
91.121.231.81	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.121.231.81	Block	70
89.138.207.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	70
46.120.122.205	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	70
46.19.85.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	60
79.178.126.54	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.178.126.54	Block	60

09-29-2015-00:00:06 to 09-30-2015-00:00:06