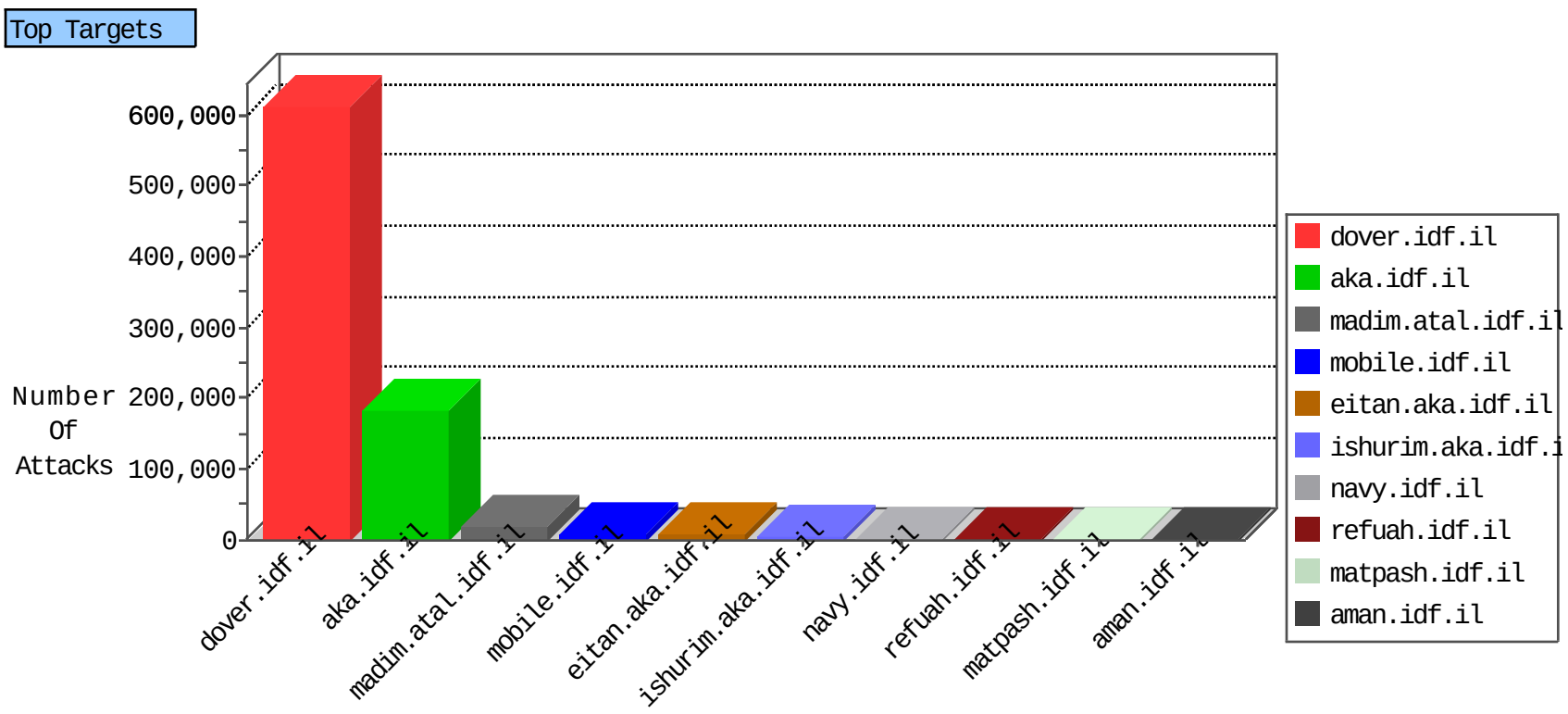
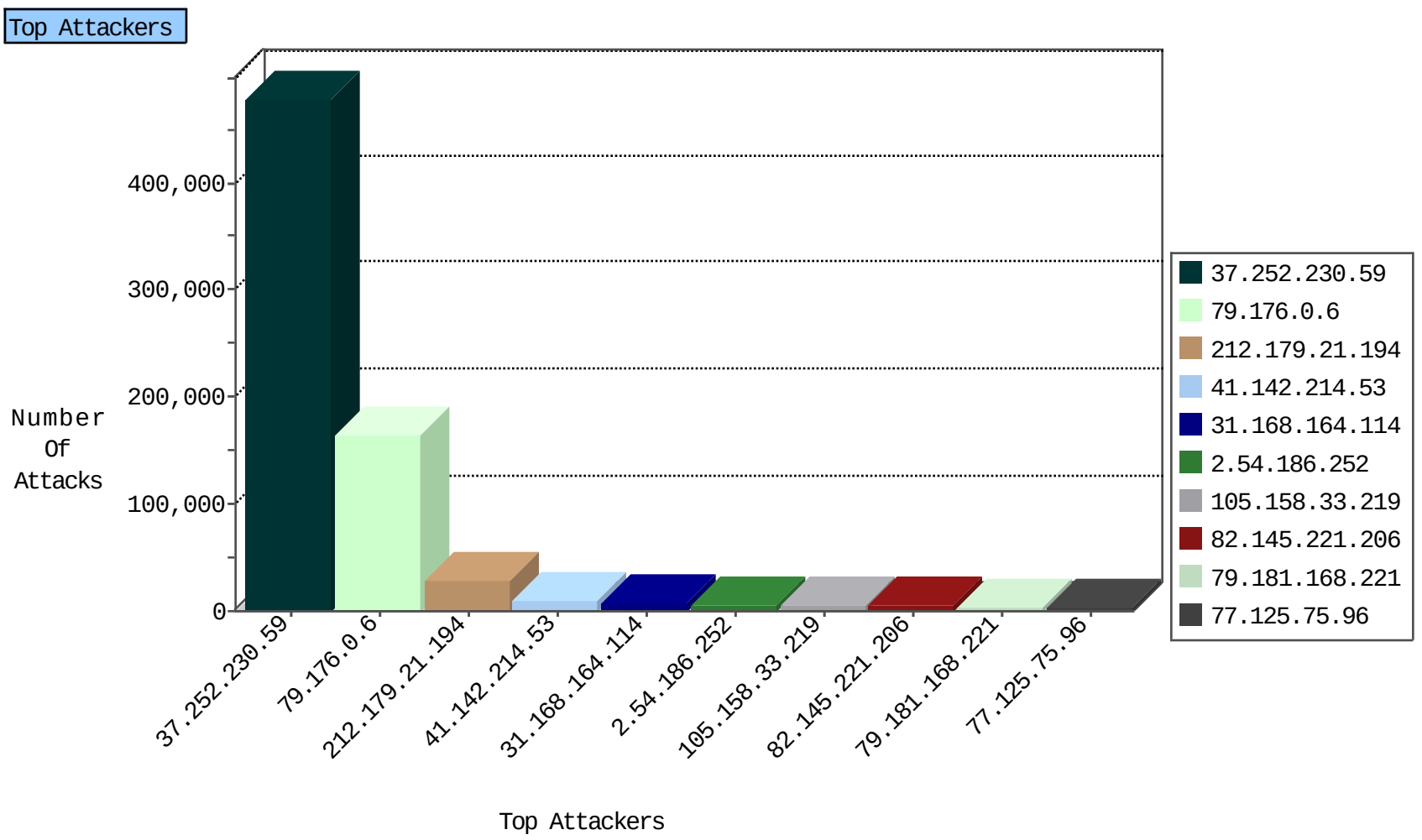
10-01-2015-00:00:00 to 10-02-2015-00:00:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-01-2015-00:00:00 to 10-02-2015-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.38	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	8490
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5696
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5426
72.9.148.10	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4715
66.249.64.156	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3078
86.157.181.249	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2146
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1353
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1084
66.249.79.225	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1025
197.215.255.110	Tanzania, United Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	654
66.249.79.211	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	638
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	546
195.53.175.26	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	410
178.255.215.87	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	371
79.179.176.113	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	298
46.19.85.3	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	274
79.182.36.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	250
149.88.27.1	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	197
66.249.69.109	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	186
46.19.85.9	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	171
46.19.86.190	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	157
37.26.146.206	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	117
79.176.20.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	112
37.26.148.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	101
2.52.27.68	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	100
37.26.148.255	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	87
149.78.21.209	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	83
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	81
2.54.141.152	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	81
46.19.86.13	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	73
2.54.154.91	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	69
46.19.85.237	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	59
2.54.15.97	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	54
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	53
46.121.92.143	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	48
185.32.179.5	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	48
185.32.179.230	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	46
2.52.49.77	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	43
176.67.121.48	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	39
80.230.48.14	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	32
100.100.71.245		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	32
85.250.156.211	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	31
46.19.85.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
2.54.35.4	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	30
46.121.92.143	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
46.19.86.16	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
103.25.58.145	Australia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-lgn	dest-reset	26
213.57.221.186	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
103.25.58.145	Australia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	24
195.250.33.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24

10-01-2015-00:00:00 to 10-02-2015-00:00:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.136.177	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
213.8.124.107	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
206.72.113.4	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
64.186.146.196	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
216.249.104.194	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
121.100.143.14	China	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	4
5.135.254.36	France	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
211.59.8.170	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
66.135.63.82	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
79.183.35.44	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
211.59.8.170	Korea, Republic of	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
67.216.79.204	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.137.81.122	Ireland	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.116.201.122	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
193.143.55.47	Finland	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
94.73.145.90	Turkey	147.237.77.226	www.chamatz.aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
139.162.28.69	Netherlands	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
78.46.94.179	Germany	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	3
199.255.210.43	Anonymous Proxy	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	3
87.69.140.25	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.176.41.194	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.117.51.173	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.121.131.148	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.165.214.208	France	147.237.77.216	dover.idf.il	20114: HTTP: PHP Malicious Archive File Transfer	Block	2
212.143.191.43	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
192.174.80.36	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
192.174.80.36	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
121.100.143.14	China	147.237.77.216	dover.idf.il	C023: HTTP: administrator in URI	Permit	1
5.22.130.203	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
176.67.121.48	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.118	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
186.188.202.115	Panama	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
197.7.10.201	Tunisia	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
61.161.130.242	China	147.237.0.15	kosher-kravi.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
36.81.0.48	Indonesia	147.237.77.74	law.idf.il	9220: PHP: Malicious Obfuscated PHP Program Access	Block	1
94.73.145.90	Turkey	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
119.101.94.33	China	147.237.77.216	dover.idf.il	8479: HTTP: Suspicious HTTP Request	Block	1
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
61.161.130.242	China	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
144.76.29.162	Germany	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
37.8.6.145	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C1000101: HTTP Hacked in the URL	Block	1
103.25.58.145	Australia	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	1
120.37.244.230	China	147.237.77.176	matpash.idf.il	13764: HTTP: China Chopper Malware Communication Attempt	Block	1
2.54.138.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
86.108.19.245	Jordan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
37.8.6.145	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C1000158: HTTP(S): Hacked in the Payload	Block	1

10-01-2015-00:00:00 to 10-02-2015-00:00:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.225	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	172
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	87
46.19.85.105	147.237.76.30	Israel	himush.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	71
176.67.121.48	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	42
176.67.121.48	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	35
94.245.88.217	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	26
46.19.86.14	147.237.77.243	Israel	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
197.7.10.201	147.237.77.216	Tunisia	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	19
176.67.121.48	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SQL Injection - Select From	18
62.210.113.143	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	13
62.210.113.143	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	13
67.55.73.76	147.237.77.226	United States	www.chamatz.aka.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	12
67.216.79.204	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
216.249.104.194	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	12
37.8.6.145	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	11
121.100.143.14	147.237.77.216	China	dover.idf.il	SERVER-WEBAPP login.htm access	11
197.7.10.201	147.237.77.216	Tunisia	dover.idf.il	ET SCAN Sqlmap SQL Injection Scan	11
121.100.143.14	147.237.77.216	China	dover.idf.il	SERVER-WEBAPP adminlogin access	11
66.249.79.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	10
176.67.121.48	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	10
66.249.67.87	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	10
67.55.73.76	147.237.77.176	United States	matpash.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	9
192.174.80.36	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	9
188.165.214.208	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	9
176.67.121.48	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SQL use of concat function with select - likely SQL injection	8
66.249.79.211	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	8
176.67.121.48	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	8
5.135.254.36	147.237.72.166	France	aka.idf.il	Tehila - Perl LWP with fake user agent	8
78.46.94.179	147.237.72.166	Germany	aka.idf.il	Tehila - Perl LWP with fake user agent	8
176.67.121.48	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	8
67.55.84.212	147.237.77.226	United States	www.chamatz.aka.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	6
67.55.84.212	147.237.72.166	United States	aka.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	6
206.72.113.4	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
67.55.73.76	147.237.72.156	United States	aman.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	6
185.5.154.223	147.237.77.216	Saudi Arabia	dover.idf.il	ET SCAN NMAP -sA (2)	6
46.137.81.122	147.237.77.74	Ireland	law.idf.il	SQL Injection - Select From	6
64.186.146.196	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
94.73.145.90	147.237.77.226	Turkey	www.chamatz.aka.idf.il	SQL Injection - Select From	6
67.55.73.76	147.237.77.74	United States	law.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	6
121.100.143.14	147.237.77.216	China	dover.idf.il	SERVER-WEBAPP admin.php access	5
31.154.92.178	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
218.65.30.23	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	4
66.249.78.166	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
80.246.136.213	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
66.249.69.109	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.69.93	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
176.12.137.79	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.79.222	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4

10-01-2015-00:00:00 to 10-02-2015-00:00:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27243
31.168.164.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7397
41.142.214.53	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6242
82.145.221.206	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5685
105.158.33.219	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5336
77.125.75.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2998
213.57.56.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2318
121.100.143.188	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2031
41.142.214.53	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1925
121.100.143.14	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1893
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1815
79.181.168.221	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1424
79.176.182.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1260
46.19.85.167	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1185
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1088
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	801
85.64.71.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	797
46.116.116.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	792
95.86.112.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	760
103.25.58.145	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	758
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	754
85.65.74.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	660
168.235.197.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	659
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	609
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	605
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	604
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	601
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	597
192.197.178.2	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	590
78.149.161.25	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	574
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	554
86.157.181.249	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	553
31.168.99.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	541
82.205.11.15	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	534
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	508
190.31.135.167	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	488
81.17.31.214	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	480
109.67.248.100	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	435
5.82.97.216	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	432
89.138.220.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	415
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	405
147.236.28.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	392
37.236.228.5	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	384
31.154.176.153	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	378
105.158.33.219	Morocco	147.237.77.216	dover.idf.il	drop		drop	350
82.166.22.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	342
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	327
207.46.13.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	292
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	276
81.17.31.214	Switzerland	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	260

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.252.230.59	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.252.230.59	Block	476449
79.176.0.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	163056
2.54.186.252	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.186.252	Block	5925
85.250.100.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2569
5.29.83.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2078
176.12.146.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1906
37.26.146.200	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.200	Block	1783
79.181.168.221	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.168.221	Block	1621
89.139.178.172	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.178.172	Block	1458
79.177.62.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1430
37.252.230.59	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/	Block	1374
79.177.50.163	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 79.177.50.163	Block	1221
93.172.174.216	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.172.174.216	Block	1174
149.88.62.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1099
95.86.124.76	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 95.86.124.76	Block	957
79.177.62.130	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.62.130	Block	869
31.168.196.32	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 31.168.196.32	Block	847
75.126.122.176	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	691
176.13.5.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	605
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	462
41.142.214.53	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.142.214.53	Block	398
121.100.143.14	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.100.143.14	Block	363
125.107.185.204	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 125.107.185.204	Block	319
121.100.143.14	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 121.100.143.14	Block	319
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	303
62.0.101.97	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.0.101.97	Block	296
46.19.85.167	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	286
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	264
46.19.85.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	264
37.26.147.191	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter RepeatPassword	Block	249
37.252.230.59	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-he/	Block	242
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	240
31.154.176.153	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 31.154.176.153	Block	231
109.67.150.174	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	231
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	218
37.26.149.195	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.149.195	Block	198
85.250.139.98	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	187
176.13.15.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	176
109.67.248.100	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.67.248.100	Block	176
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	165
37.252.230.59	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	165
46.19.85.21	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	154
37.252.230.59	United Kingdom	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 37.252.230.59	Block	153
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	143
37.252.230.59	United Kingdom	147.237.77.216	dover.idf.il	Multiple Double URL Encoding from 37.252.230.59	Block	143
81.17.31.214	Switzerland	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	143
80.178.202.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	132
176.12.139.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	132
176.12.142.251	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	110
37.26.148.128	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	110