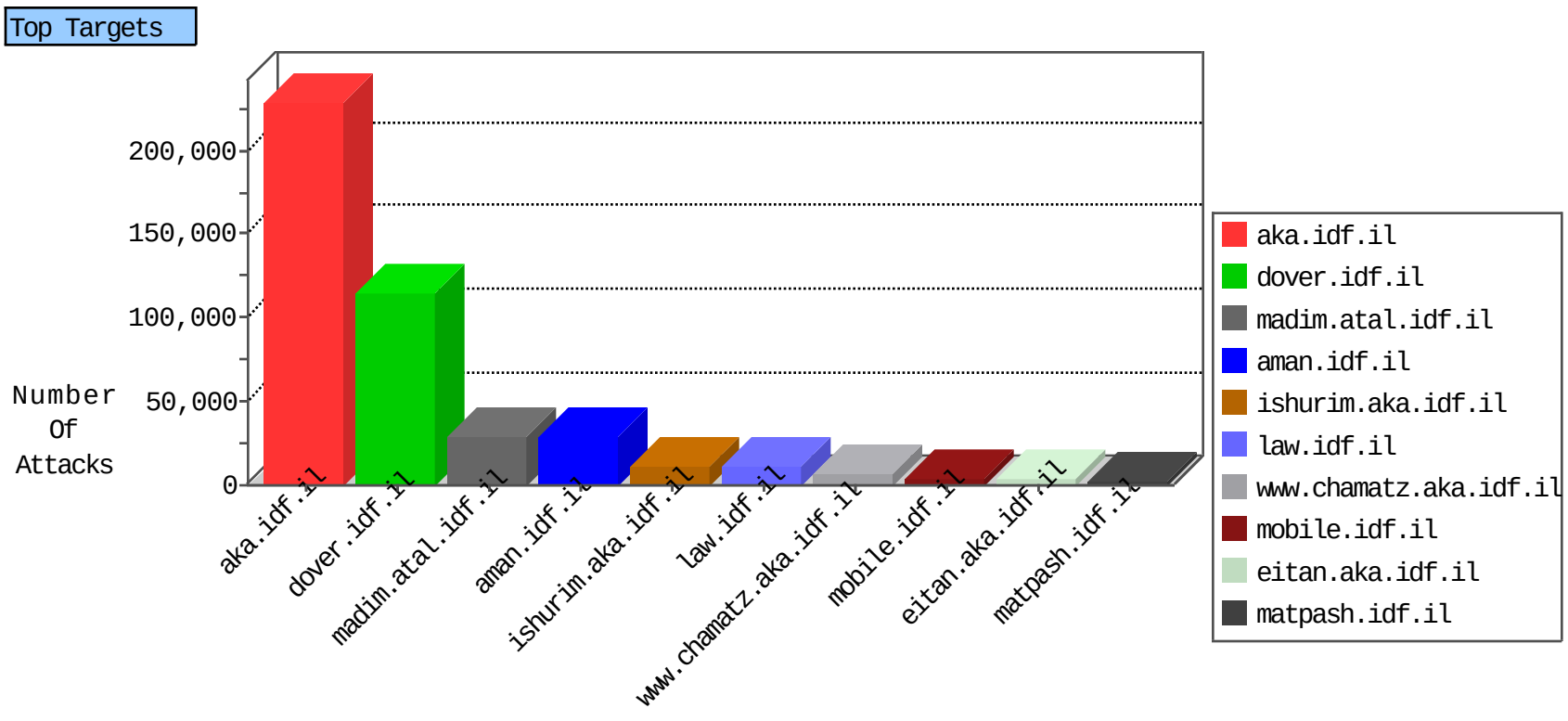
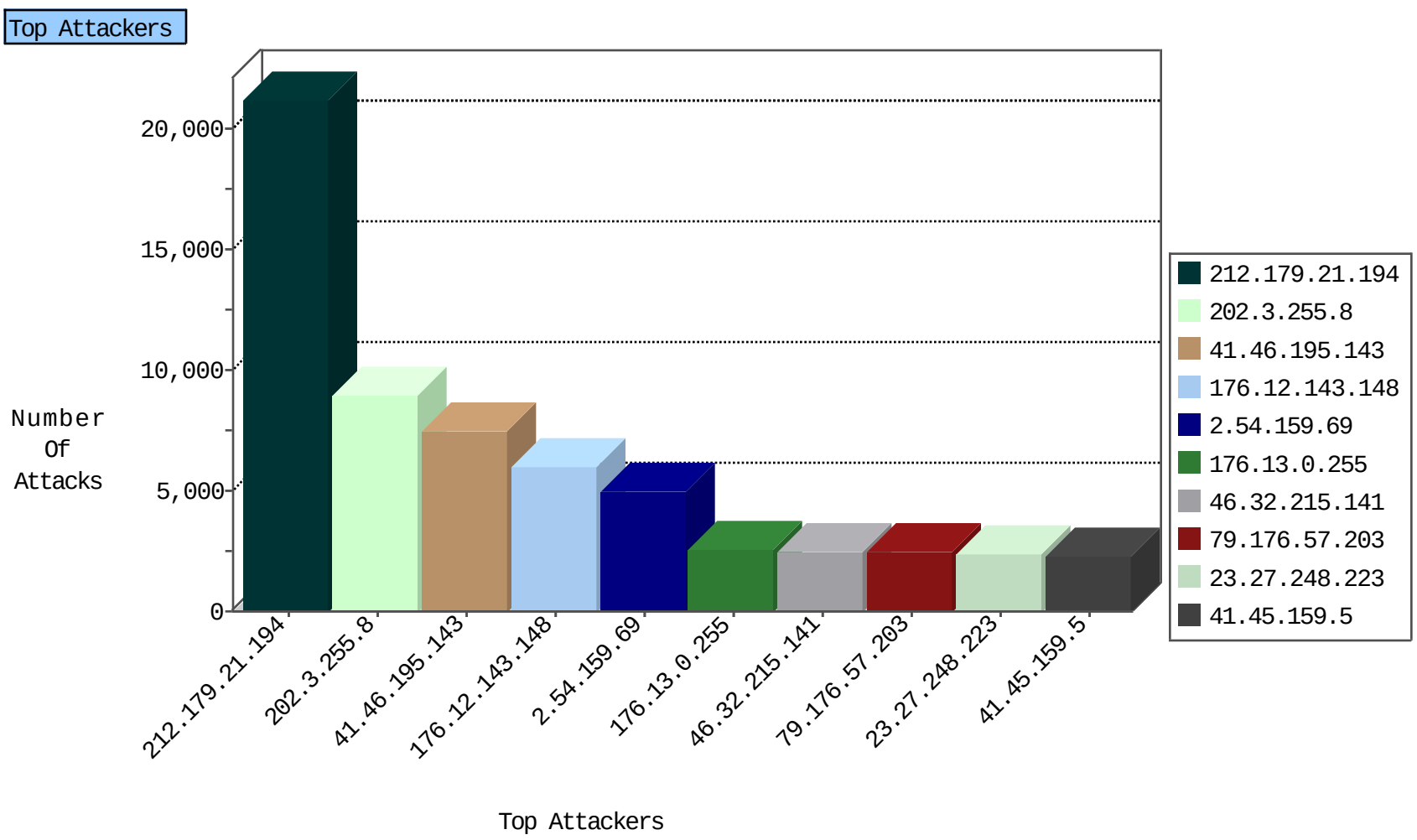
09-21-2015-00:00:09 to 09-22-2015-00:00:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2015-00:00:09 to 09-22-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	45761
176.223.83.97	Germany	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	14774
176.223.80.97	Germany	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	13246
66.249.67.208	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7972
93.127.140.136	Germany	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	7203
66.249.78.9	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6273
193.188.136.30	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5144
66.249.93.160	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4440
84.208.79.17	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3826
203.99.102.194	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3504
66.249.69.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3463
66.249.93.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3270
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3060
176.223.81.161	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2720
66.249.78.254	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2584
93.127.140.69	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2546
66.249.78.2	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2513
176.223.82.30	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1587
94.249.211.14	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1304
82.211.18.100	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	734
176.223.81.239	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	732
176.223.82.29	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	669
79.176.193.67	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	608
176.223.80.33	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	513
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	366
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	328
79.182.62.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	266
204.93.154.198	United States	147.237.76.31	nakchal.idf.il	TCP Scan (vertical)	drop	182
64.233.172.144	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	142
176.13.1.203	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	137
64.233.172.160	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	126
46.19.85.82	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	99
2.54.171.195	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	79
93.173.165.8	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	67
82.211.18.127	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	67
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
2.54.62.0	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	65
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	62
199.203.142.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	55
37.142.64.97	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	46
46.32.215.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41
5.28.180.142	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	35
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	30
199.203.142.65	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
62.90.70.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
2.52.142.125	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	28
31.168.51.194	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
2.54.21.227	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	25
87.68.45.182	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	25
185.32.179.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25

09-21-2015-00:00:09 to 09-22-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
104.155.193.30	United States	147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	11
104.155.193.30	United States	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	11
104.155.193.30	United States	147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	11
104.155.193.30	United States	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	11
94.23.17.208	France	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
81.218.116.129	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
23.91.127.130	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
67.216.79.204	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
74.86.47.2	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.245.88.135	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
81.218.59.82	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
62.210.225.135	France	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
105.158.242.147	Morocco	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	4
87.106.184.160	Germany	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
79.183.193.233	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
188.165.250.173	France	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
212.235.98.139	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.143.40.26	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
62.219.208.184	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.116.182.143	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
189.210.211.196	Mexico	147.237.77.74	law.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	2
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
140.237.23.26	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
212.150.37.22	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.26.147.189	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
198.143.164.221	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
212.199.97.194	Israel	147.237.72.166	aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	2
79.181.115.167	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.199.97.194	Israel	147.237.77.216	dover.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	2
83.142.167.109	Russian Federation	147.237.77.74	law.idf.il	20114: HTTP: PHP Malicious Archive File Transfer	Block	1
198.20.69.74	United States	147.237.77.227	e.hamaz.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
109.64.171.59	Israel	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
81.181.81.178	Romania	147.237.77.74	law.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
31.154.10.131	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.57.229.227	United States	147.237.77.216	dover.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
46.164.154.106	Ukraine	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
94.23.17.208	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
81.218.33.77	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
86.132.215.49	United Kingdom	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
157.55.39.122	United States	147.237.77.216	dover.idf.il	C1000158: HTTP(S): Hacked in the Payload	Block	1
46.172.71.251	Ukraine	147.237.77.176	matpash.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
41.185.31.40	South Africa	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
198.143.164.221	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
46.172.71.251	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
198.20.69.74	United States	147.237.76.198	e.yohalan.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-21-2015-00:00:09 to 09-22-2015-00:00:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.8	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	8178
213.247.63.11	147.237.77.176	Netherlands	matpash.idf.il	SQL Injection - Select From	293
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	64
50.59.103.190	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	27
46.19.85.5	147.237.76.42	Israel	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	23
50.31.134.53	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	19
62.210.225.135	147.237.77.74	France	law.idf.il	SQL Injection - Select From	12
87.106.184.160	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	12
67.216.79.204	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
94.23.17.208	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	11
74.86.47.2	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	11
188.165.250.173	147.237.77.74	France	law.idf.il	SQL Injection - Select From	6
23.91.127.130	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
198.143.164.221	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
94.245.88.135	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	5
176.12.146.116	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
176.12.143.148	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
171.250.100.141	147.237.0.34	Vietnam	tikshuv.idf.il	ET SCAN Potential SSH Scan	4
93.89.16.110	147.237.77.216	Turkey	dover.idf.il	SQL Injection - Select From	4
41.185.31.40	147.237.76.42	South Africa	refuah.idf.il	SQL Injection - Select From	4
171.250.100.141	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
80.246.136.41	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
50.62.58.201	147.237.76.86	United States	navy.idf.il	SERVER-WEBAPP backup access	3
176.13.6.206	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
218.87.111.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
50.59.103.190	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	3
218.87.111.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	3
171.250.100.141	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
66.249.93.253	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	3
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
66.249.75.227	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.100	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
92.252.167.222	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
50.31.134.53	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	2
218.87.111.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
54.224.149.230	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
37.8.105.90	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.100	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.23	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
54.72.144.153	147.237.77.216	Ireland	dover.idf.il	Tehila - Perl LWP with fake user agent	2
50.31.134.53	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	2
66.249.78.230	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
218.65.30.23	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
176.12.146.222	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
171.250.100.141	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.42	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2

09-21-2015-00:00:09 to 09-22-2015-00:00:09

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	20587
41.46.195.143	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7469
23.27.248.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2328
46.32.215.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2235
41.45.159.5	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2234
46.116.224.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1425
82.145.211.109	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1387
209.88.198.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1339
185.28.155.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1262
41.46.62.119	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1100
31.223.128.197	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1056
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1010
213.57.132.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	901
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	791
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	781
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	734
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	732
79.180.27.103	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	624
192.249.64.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	606
46.19.86.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	581
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	573
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	557
170.252.248.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	556
31.168.171.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	552
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	534
37.8.61.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	533
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	532
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	506
79.177.55.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	500
2.54.184.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	499
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	492
37.236.228.25	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	474
85.31.3.11	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	451
193.188.156.18	Sweden	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	444
94.249.211.142	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	420
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	407
176.223.80.77	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	403
176.223.84.67	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	382
82.211.18.138	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	381
176.223.81.161	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	380
82.211.18.123	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	372
94.249.211.60	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	358
37.26.146.200	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	342
105.158.178.255	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	341
89.138.220.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	336
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	331
82.211.18.69	Germany	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	330
46.248.223.12	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	327
176.223.82.30	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	322
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	315

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.143.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5971
2.54.159.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4945
176.13.0.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2519
79.176.57.203	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.57.203	Block	2430
2.54.22.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1919
80.246.136.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1710
80.246.136.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1665
185.32.179.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1307
176.12.151.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1179
176.13.18.74	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.18.74	Block	1179
176.12.140.191	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.140.191	Block	1059
79.180.27.103	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	691
176.13.3.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	648
80.246.136.20	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.20	Block	601
109.65.124.173	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	586
87.69.17.251	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.17.251	Block	513
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	405
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	396
66.249.78.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	378
66.249.78.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	341
157.55.39.237	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	333
207.46.13.182	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	333
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	324
66.249.78.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	315
66.249.67.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	306
176.13.16.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	306
66.249.67.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	297
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	297
157.55.39.231	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	288
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	270
68.180.229.239	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	243
46.19.85.32	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.32	Block	207
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	207
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	198
66.249.93.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	189
176.12.141.188	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.141.188	Block	189
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	189
66.249.78.141	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	180
54.187.55.213	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	171
66.249.78.134	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	171
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	171
59.174.166.143	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 59.174.166.143	Block	153
66.249.78.148	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	153
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	153
84.94.180.91	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	153
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	152
66.249.93.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	144
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	135
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	135
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	135