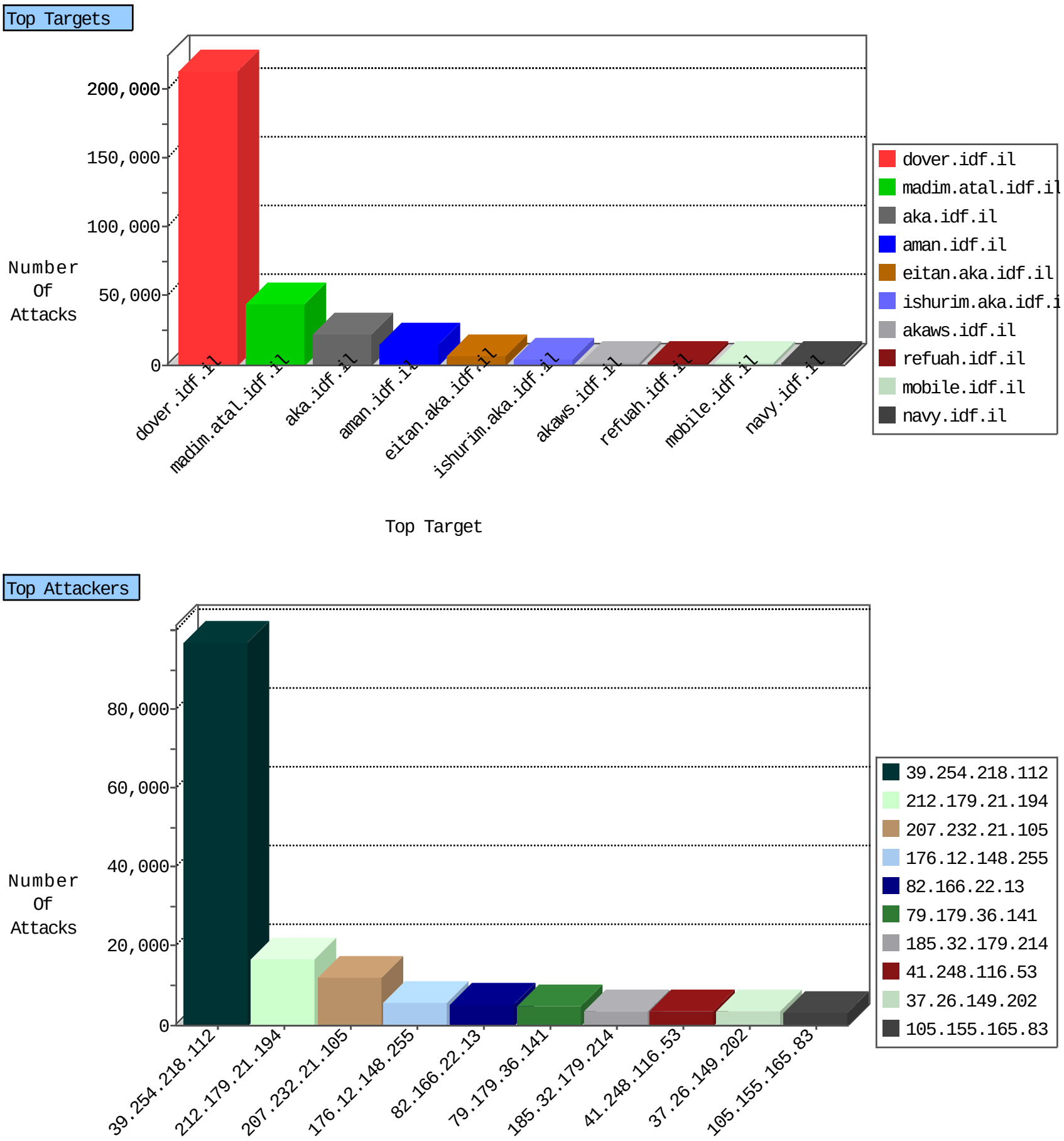
10-12-2015-00:00:02 to 10-13-2015-00:00:02

IDF Under Attack Daily Report



10-12-2015-00:00:02 to 10-13-2015-00:00:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.153	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	19099
85.17.29.97	Netherlands	147.237.0.19	madim.atal.idf.il	TCP Scan (vertical)	drop	15353
54.244.22.103	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	11653
157.55.39.152	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8594
66.249.93.196	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8178
66.249.65.95	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7446
155.56.68.214	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7324
37.26.148.226	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6352
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5734
66.249.78.160	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4571
39.254.218.112	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3494
195.110.146.226	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2006
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	789
66.249.78.146	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	546
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	438
185.32.179.70	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	380
2.52.8.63	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	329
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	292
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	290
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	235
66.249.69.109	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	222
66.249.69.101	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	150
2.54.32.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	142
217.132.238.47	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	135
5.22.129.181	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	129
46.19.85.163	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	121
37.26.147.172	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	110
80.246.137.109	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	109
2.54.190.69	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	107
192.116.94.223	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	97
62.219.183.196	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	84
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	81
66.249.64.151	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	76
2.54.189.4	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	69
80.246.137.240	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	61
2.54.53.10	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	60
79.183.224.30	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	56
46.19.86.78	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	55
37.26.146.226	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	54
132.64.25.131	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	53
5.28.163.253	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	53
84.108.42.199	Israel	147.237.77.243	mobile.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	50
2.54.179.160	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	46
109.64.96.230	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	45
46.19.86.43	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	45
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	44
37.26.147.217	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	43
66.249.64.143	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	42
176.13.3.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	41
46.19.85.206	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	41

10-12-2015-00:00:02 to 10-13-2015-00:00:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.116.173	Israel	147.237.77.216	dover.idf.il	C017: HTTP: Malicous UserAgent FOCA	Block	66
194.177.16.3	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	22
84.108.220.49	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
74.63.228.226	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
146.185.24.133	United Kingdom	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
81.218.116.129	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.17.29.97	Netherlands	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	5
189.38.90.189	Brazil	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
208.90.95.197	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
93.172.172.118	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
91.142.253.133	Netherlands	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
192.115.252.2	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
149.202.112.62	Germany	147.237.77.216	dover.idf.il	13033: HTTP: Ruby on Rails YAML Deserialization Memory Corruption Vulnerability	Block	2
73.179.208.124	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
198.20.69.74	United States	147.237.8.28	e.mobile-ks.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
149.202.112.62	Germany	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	2
149.202.112.62	Germany	147.237.77.216	dover.idf.il	2023: HTTP: Cross Site Scripting in GET Request	Block	2
79.178.101.147	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
84.109.0.197	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
149.202.112.62	Germany	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	2
212.235.10.42	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.179.176.218	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
216.172.189.115	United States	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
198.20.69.74	United States	147.237.8.27	e.madim.atal.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1
212.96.109.86	Russian Federation	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
149.202.112.62	Germany	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
217.65.214.167	Russian Federation	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
2.94.19.99	Russian Federation	147.237.77.216	dover.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
31.168.232.194	Israel	147.237.72.166	aka.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
91.142.253.133	Netherlands	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
212.199.97.194	Israel	147.237.72.166	aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	1
117.241.208.174	India	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
198.20.69.74	United States	147.237.77.227	e.hamaz.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
46.116.134.117	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
93.89.16.110	Turkey	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
85.17.29.97	Netherlands	147.237.0.34	tikshuv.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
149.202.112.62	Germany	147.237.77.216	dover.idf.il	3999: HTTP: Cross Site Scripting Attack in HTTP Header	Block	1
93.89.16.110	Turkey	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

10-12-2015-00:00:02 to 10-13-2015-00:00:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	90
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	36
189.38.90.189	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	12
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
87.242.112.35	147.237.77.216	Russian Federation	dover.idf.il	SQL Injection - Select From	10
149.202.112.62	147.237.77.216	Germany	dover.idf.il	SERVER-WEBAPP awstats access	6
91.142.253.133	147.237.76.86	Netherlands	navy.idf.il	SQL Injection - Select From	6
66.249.69.101	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
73.179.208.124	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
54.209.60.63	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
93.95.207.36	147.237.77.216	Jordan	dover.idf.il	SERVER-WEBAPP adminlogin access	3
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
66.249.69.109	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
66.249.65.92	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
23.95.82.74	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	2
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
5.22.129.94	147.237.76.30	Israel	himush.idf.il	GPL SCAN myscan	2
66.249.64.168	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
79.177.132.132	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
23.95.82.74	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
23.95.82.74	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	2
85.17.29.97	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
94.102.48.194	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	2
192.198.151.45	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
149.202.112.62	147.237.77.216	Germany	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
149.202.112.62	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	2
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
27.185.202.92	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
149.202.112.62	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER Possible CVE-2013-0156 Ruby On Rails XML YAML tag with !ruby	2
93.89.16.110	147.237.76.42	Turkey	refuah.idf.il	SQL Injection - Select From	2
5.22.129.94	147.237.76.30	Israel	himush.idf.il	INDICATOR-SCAN myscan	2
66.249.64.161	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
31.210.176.60	147.237.72.166	Israel	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
85.17.29.97	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	2
23.95.82.74	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
66.249.78.74	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
212.76.96.199	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.78.45	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
193.105.134.220	147.237.77.216	Sweden	dover.idf.il	ET SCAN NMAP -sS window 1024	2
85.250.59.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.11.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.44.62.78	147.237.77.121	Egypt	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.86.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.1.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.152.92.89	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
95.185.104.39	147.237.77.216	Saudi Arabia	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.4.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.50.197.147	147.237.8.27	Australia	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
190.124.35.115	147.237.8.27	Nicaragua	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1

10-12-2015-00:00:02 to 10-13-2015-00:00:02

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	16820
39.254.218.112	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5972
82.166.22.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5401
105.155.165.83	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3267
41.248.116.53	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2886
36.70.27.86	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2559
199.203.247.180	Israel	147.237.0.35	akaws.idf.il	drop		drop	2223
149.202.112.62	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2052
172.56.39.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1111
213.8.114.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	977
31.154.27.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	898
37.142.232.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	876
2.54.16.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	809
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	805
79.176.148.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	803
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	798
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	783
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	766
66.249.65.92	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	759
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	741
66.249.65.89	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	734
66.249.65.95	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	720
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	674
79.182.15.137	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	654
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	608
79.181.129.48	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	570
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	564
46.117.59.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	561
85.250.59.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	547
2.52.185.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	466
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	447
185.18.206.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	430
37.26.146.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	413
77.125.126.180	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	411
95.86.74.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	407
179.214.236.147	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	406
85.130.187.233	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	402
188.165.15.126	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	401
37.60.45.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	399
84.94.116.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	386
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	383
2.54.30.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	355
2.52.139.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	348
88.8.175.150	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	336
62.219.128.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	320
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	318
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	317
46.19.86.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
37.26.149.211	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	297
114.176.31.136	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	277

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
39.254.218.112	Indonesia	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90969
207.232.21.105	Israel	147.237.72.156	aman.idf.il	Too Many of the Same Response Code (404) in Session from 207.232.21.105	Block	12117
176.12.148.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5750
79.179.36.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5023
185.32.179.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3756
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.149.202	Block	3487
176.13.15.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2827
46.116.92.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2772
185.32.179.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2686
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2059
217.132.211.208	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 217.132.211.208	Block	1977
80.246.137.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1872
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1824
149.78.200.146	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1608
46.19.86.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1302
79.182.15.137	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.15.137	Block	1295
2.54.139.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1259
176.12.140.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1064
85.64.5.161	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	984
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	684
41.248.116.53	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.248.116.53	Block	568
185.24.207.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	516
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.89	Block	492
2.54.9.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	453
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	360
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.95	Block	348
85.130.187.233	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.130.187.233	Block	348
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.51	Block	348
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.92	Block	348
80.246.136.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	336
77.125.126.180	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.126.180	Block	276
37.26.148.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	264
80.246.136.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	252
80.246.136.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	252
62.219.147.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	216
176.13.2.98	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.2.98	Block	216
212.199.97.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.97.194	Block	204
2.54.1.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	192
85.17.29.97	Netherlands	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 85.17.29.97	Block	180
39.254.218.112	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	180
75.126.122.176	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	168
80.246.136.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
2.52.0.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	156
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	156
84.108.220.49	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.220.49	Block	144
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	144
185.5.154.224	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	144
5.102.254.209	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	144
176.12.150.189	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Parameter Type Violation on m.my-kosher-kravi.idf.il/templates/training/training.aspx parameter ctl00$ContentPlaceHolder1$txtAreaRemarks	Block	143
2.54.149.127	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	132