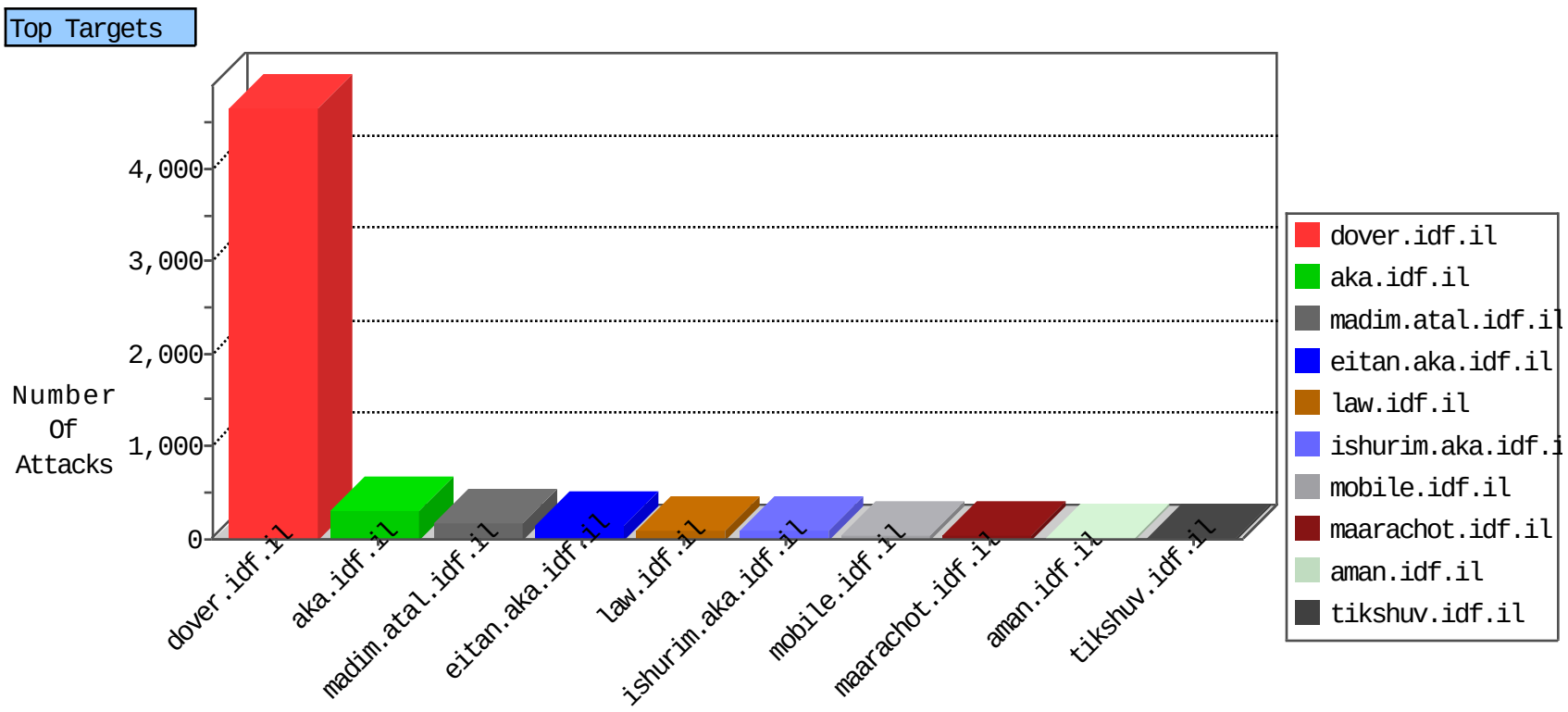
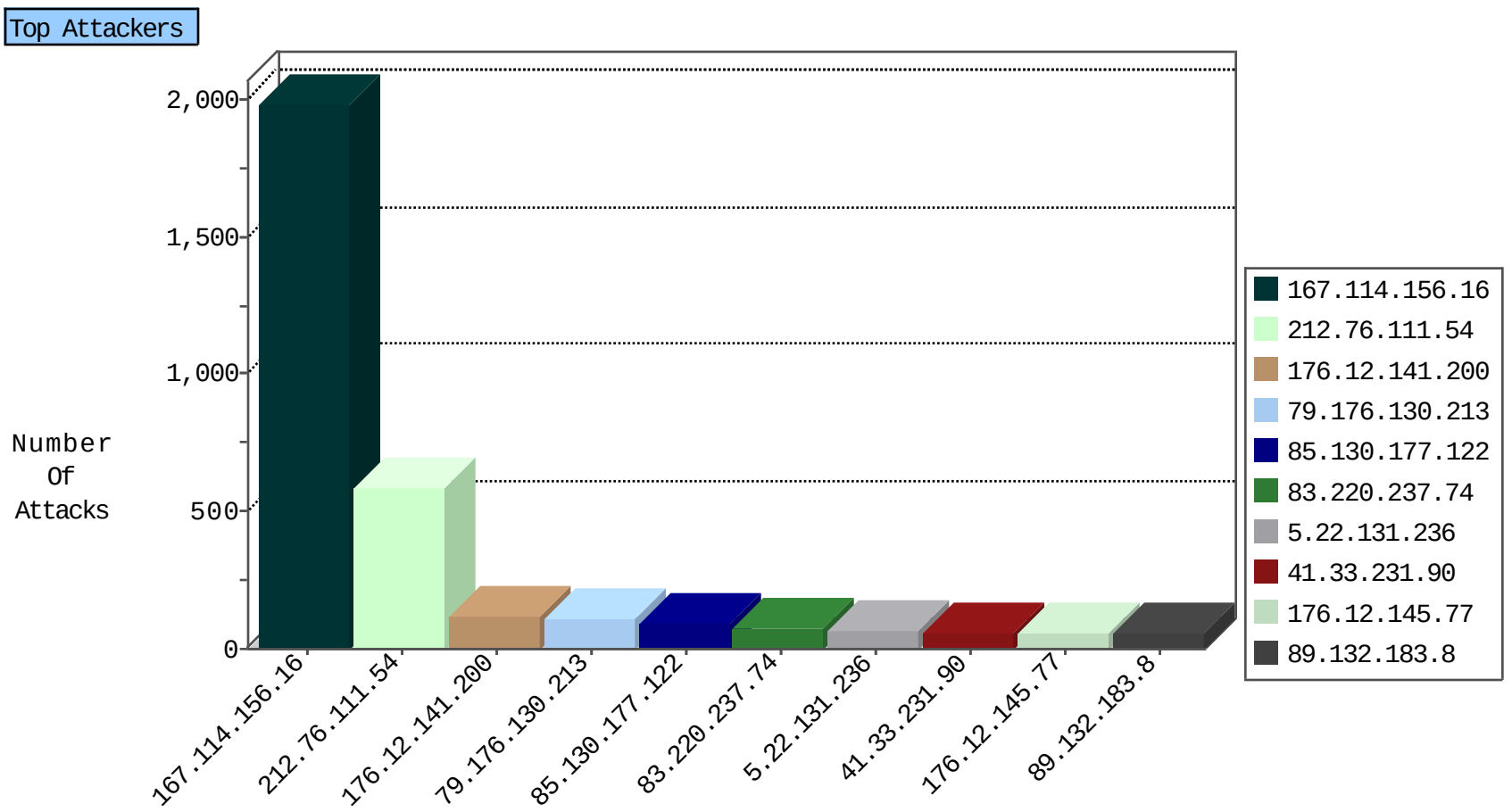
11-04-2015-21:04:07 to 11-04-2015-22:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-04-2015-21:04:07 to 11-04-2015-22:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	79274
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10092
37.26.148.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9674
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8413
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7488
37.26.148.188	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	7282
212.14.228.78	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4389
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3581
66.249.65.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3512
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3423
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3346
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2757
66.249.93.192	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2590
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2532
24.16.13.124	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2531
45.56.90.36		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2161
158.222.20.34		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2109
66.249.79.10	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1779
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1619
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1607
66.249.65.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1232
209.133.111.211	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	789
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	264
2.54.138.149	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	64
176.12.145.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	55
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	51
213.57.54.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
89.139.183.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
109.64.168.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
2.52.169.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
213.151.37.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
5.29.131.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
85.64.120.250	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
84.109.100.222	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
185.13.195.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
80.178.13.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
85.65.152.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.86.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.104.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
85.64.120.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
2.52.166.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
93.173.145.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
5.29.53.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
185.32.179.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
81.218.2.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.65.126.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.178.10.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.117.68.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6

11-04-2015-21:04:07 to 11-04-2015-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.50	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
109.67.145.42	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
23.91.70.50	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

11-04-2015-21:04:07 to 11-04-2015-22:04:07

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	9
23.91.70.50	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
66.249.79.16	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.67.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
80.241.251.218	147.237.77.235	Georgia	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
80.241.251.218	147.237.77.235	Georgia	sviva.idf.il	ET SCAN NMAP -f -sS	1
109.66.26.88	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
68.65.121.91	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
104.243.42.250	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
104.192.0.20	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
46.116.111.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.236.74.6	147.237.77.212	Poland	e.dover.idf.il	ET SCAN Potential SSH Scan	1
91.236.74.6	147.237.76.196	Poland	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.108.105.65	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.32	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.65.152.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.32	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.241.251.218	147.237.77.235	Georgia	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
183.233.162.70	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
68.65.121.91	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
104.243.42.250	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
104.243.42.250	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
46.151.52.8	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.236.74.6	147.237.77.227	Poland	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
91.236.74.6	147.237.77.121	Poland	e.navy.idf.il	ET SCAN Potential SSH Scan	1
91.236.74.6	147.237.8.28	Poland	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.32	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.68.67.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.32	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

11-04-2015-21:04:07 to 11-04-2015-22:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.111.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	582
79.176.130.213	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
85.130.177.122	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
83.220.237.74	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
5.22.131.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
89.132.183.8	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.12.145.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.85.112	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.177.171.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
79.180.218.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	23
31.25.76.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
158.222.20.34		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
2.54.104.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.180.55.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
193.201.224.32	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.166.22.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
92.201.113.208	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
141.0.14.196	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
38.122.227.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.64.168.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.186.103.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.178.106.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.109.186.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.150.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.210.191.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
96.91.243.195	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.88.8.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.180.141.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.177.172.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.32.179.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.26.148.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.52.169.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.66.173.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.108.204.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.46.118.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.67.132.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
209.53.180.111	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

11-04-2015-21:04:07 to 11-04-2015-22:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.141.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
176.12.141.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
2.54.9.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
5.29.94.171	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	16
5.29.94.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	16
46.19.86.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
40.77.167.88	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	4
109.64.211.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
89.139.58.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.57.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.173.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.102.243	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	2
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
176.13.14.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.167.44	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
109.67.132.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
79.181.167.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	2
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.44.139.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.179.210.71	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/110451.pdf	Block	2
95.86.102.243	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
79.180.55.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/2935.pdf	Block	1
109.66.170.79	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
5.29.53.39	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 5.29.53.39	Block	1
194.153.113.13	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.79.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
141.212.122.112	United States	147.237.77.176	matpash.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
37.142.68.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
85.65.98.228	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.67.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2921.pdf	Block	1
93.172.172.220	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
82.166.22.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
194.153.113.13	Germany	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
149.88.116.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
95.86.118.37	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	1
66.249.65.93	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.239.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
193.201.224.32	Ukraine	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/2905.pdf	Block	1
128.199.95.16	Singapore	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/l27.zip	Block	1
93.172.172.220	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/ajax/pages/fan_status.php	Block	1
85.64.191.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/displayallsoliders.asp	Block	1
194.153.113.13	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
159.203.134.182	United States	147.237.76.30	himush.idf.il	Unauthorized Method HEAD for chimush.atal.idf.il/	None	1
77.56.26.69	Switzerland	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.65.99	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1

11-04-2015-21:04:07 to 11-04-2015-22:04:07