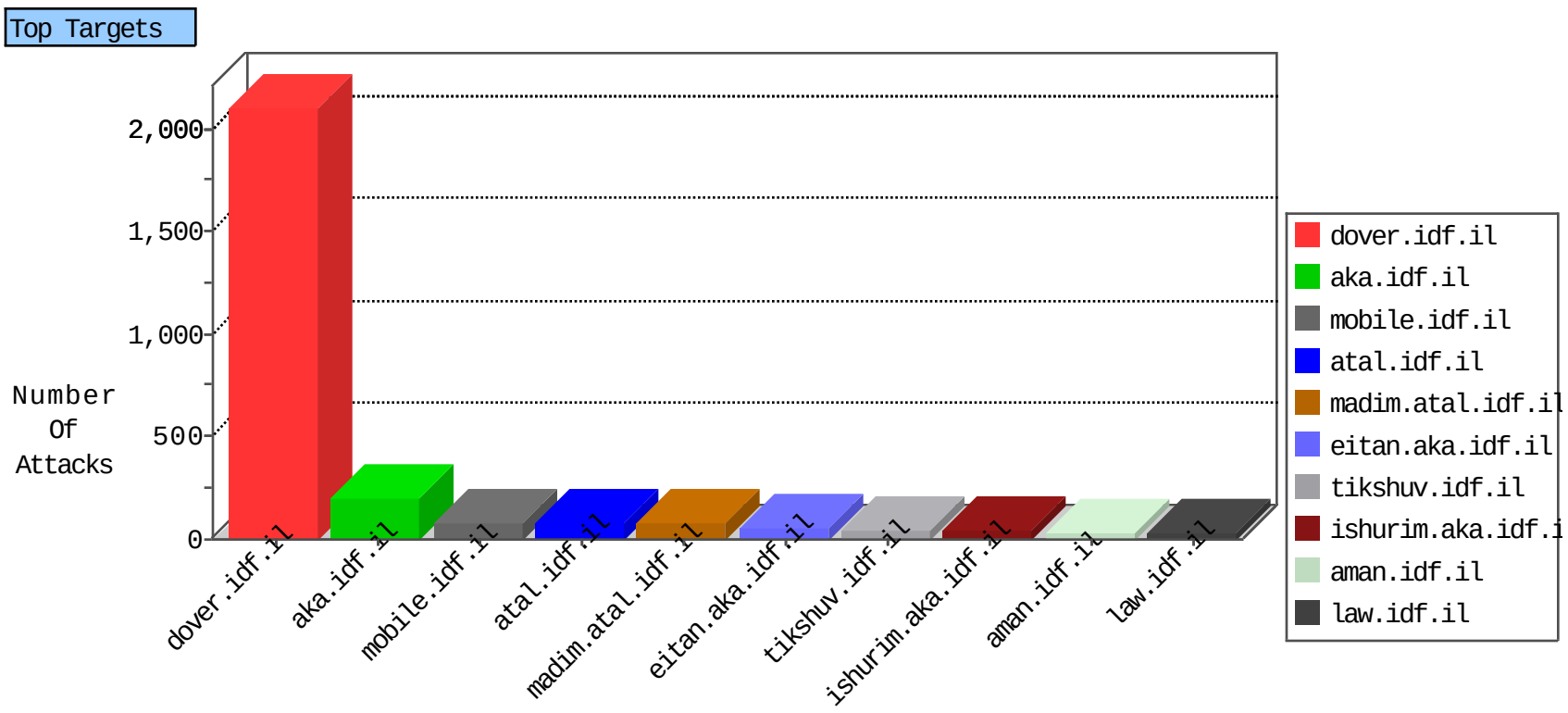
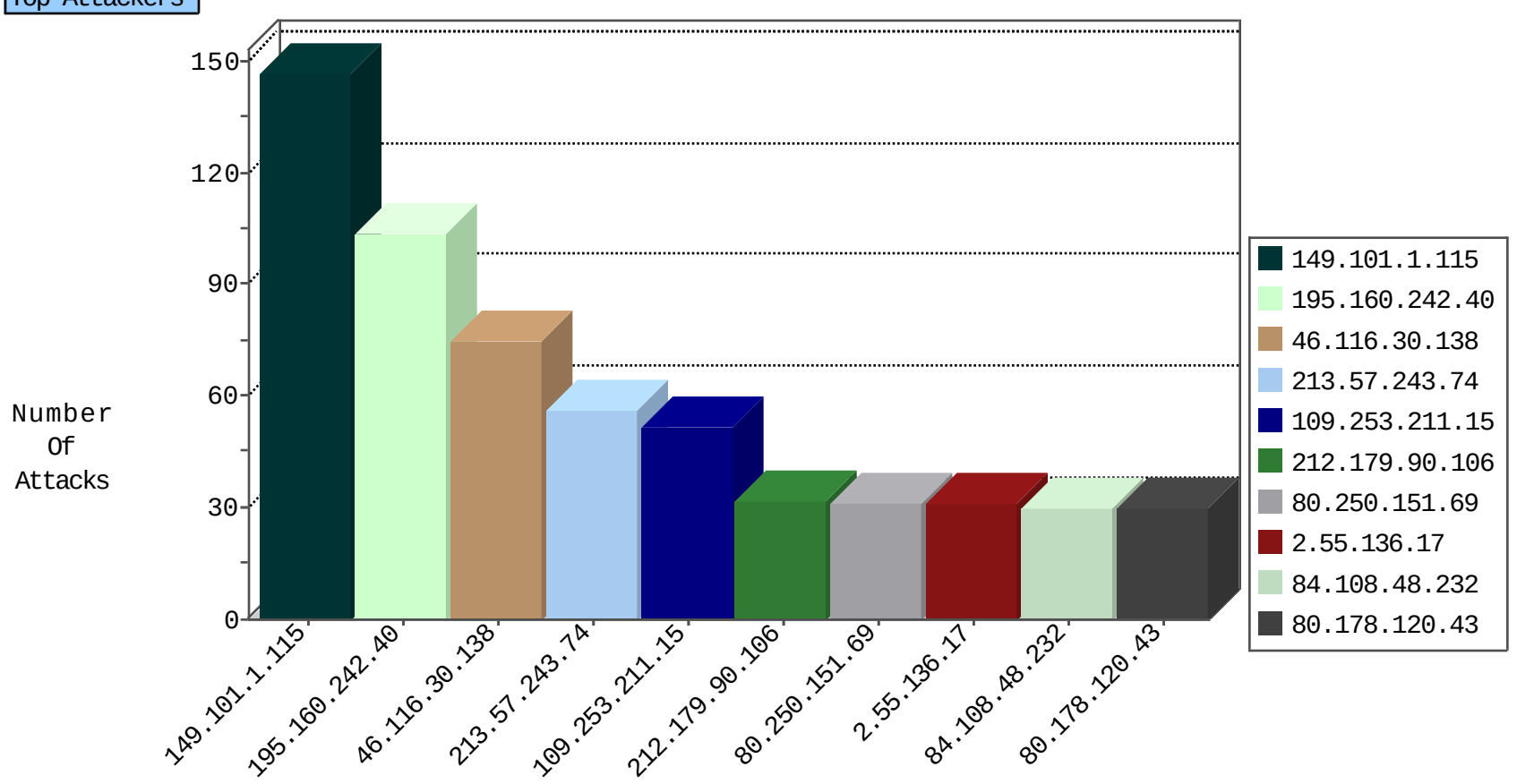
09-21-2016-14:04:00 to 09-21-2016-15:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-14:04:00 to 09-21-2016-15:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
2.55.136.17	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
37.26.148.172	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
176.13.8.152	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
109.65.3.2	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.139.247	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
80.246.137.81	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.169.89	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
80.246.137.183	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.55.56.25	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
80.246.136.205	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.12.220.83	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
79.177.121.105	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
63.141.242.194	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
204.12.220.84	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
80.246.136.11	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
62.210.15.54	France	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
109.253.197.163	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
5.29.211.183	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
63.141.231.196	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
198.204.224.237	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
149.101.1.115	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.26.146.241	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.32.179.164	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
109.66.184.167	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
63.141.231.197	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
173.208.197.204	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
85.250.254.217	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
217.132.54.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.204.224.234	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
109.253.194.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
5.29.122.205	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.204.224.234	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
69.30.193.253	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
109.66.134.60	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
80.246.136.177	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
84.108.192.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
69.30.226.220	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
208.110.84.70	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1

09-21-2016-14:04:00 to 09-21-2016-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.200.154.34	United States	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	8
195.8.208.80	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

09-21-2016-14:04:00 to 09-21-2016-15:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.229.41.66	147.237.0.34	Israel	tikshuv.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	21
195.8.208.80	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	13
91.193.51.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.63.28.189	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
212.76.100.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.83.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
206.246.150.226	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.119.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.44.143.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.52.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.130.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.92.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.223.94.123	147.237.76.197	Bolivia	e.himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.178.238.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.244.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.38.253	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
132.73.199.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
47.88.4.204	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
109.64.85.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
212.84.169.225	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.202.218.245	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.3.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
211.149.244.79	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.81.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
206.246.150.226	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.133.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.99.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.255.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.37.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.15.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.19.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.44.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.184.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.183.223.228	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN Potential SSH Scan	1
95.86.110.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-21-2016-14:04:00 to 09-21-2016-15:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.101.1.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
109.253.211.15	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
213.57.243.74	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	32
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.178.120.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
62.0.227.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
213.57.243.74	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
46.19.86.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.116.30.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
109.253.137.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.116.30.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.116.30.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.116.30.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
46.116.30.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
46.19.85.191	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
80.178.203.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
199.203.152.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.53.174.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
217.33.23.250	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.248.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.108.48.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.149.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
188.120.154.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.225.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.250.151.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
109.65.3.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.150.145.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.131.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.149.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.137.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.252	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.148.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.139.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.250.151.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
5.28.181.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.192	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.136.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.117.14.243	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.25.102.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

09-21-2016-14:04:00 to 09-21-2016-15:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.140.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.221.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
82.81.4.86	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
104.200.154.34	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.200.154.34	Block	4
80.246.139.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.21.47	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	3
185.120.124.25	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.120.124.25	Block	3
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.231.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
104.200.154.34	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 104.200.154.34	Block	2
2.53.49.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.176.15.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
111.93.113.149	India	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
87.69.158.127	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
104.200.154.34	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
80.246.139.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.65.127.77	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
78.6.227.132	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method	Block	1
111.93.113.149	India	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.210.138.194	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
46.19.85.1	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method l in URL	Block	1
212.235.64.96	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.76.102	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.67.14.246	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.154.81.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
52.16.137.212	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.58	Israel	147.237.77.233	atal.idf.il	Malformed URL	Block	1
2.53.180.233	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.243.74	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Method þ	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.168.96.254	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
80.246.137.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.120.124.25	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
147.235.236.1	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 147.235.236.1	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
46.19.85.58	Israel	147.237.77.233	atal.idf.il	Unknown HTTP Request Method 3vt5fsab2z in URL	Block	1
2.55.21.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.35.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
82.166.212.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in URL	Block	1
89.138.169.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
40.134.145.86	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
80.246.139.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1

09-21-2016-14:04:00 to 09-21-2016-15:04:00