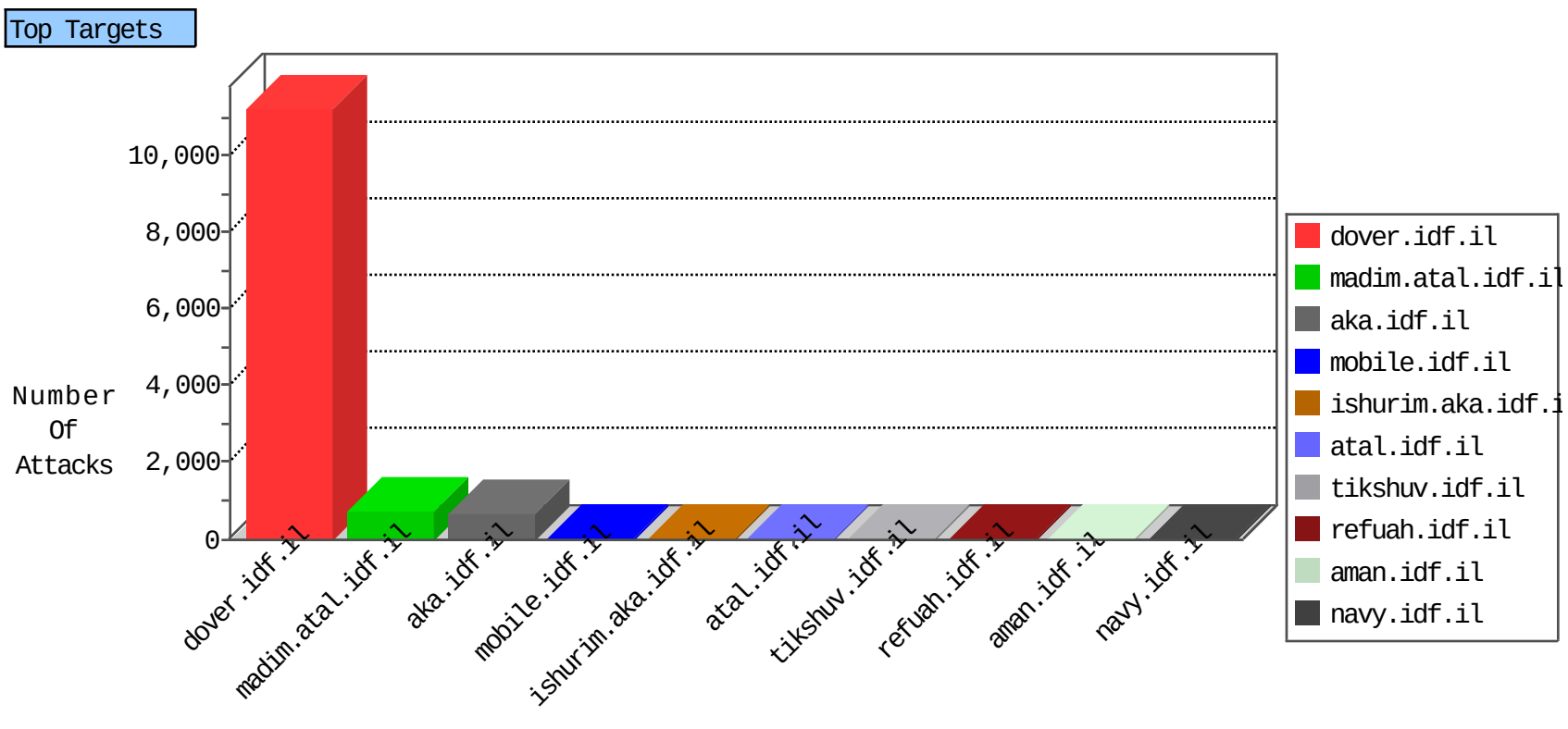
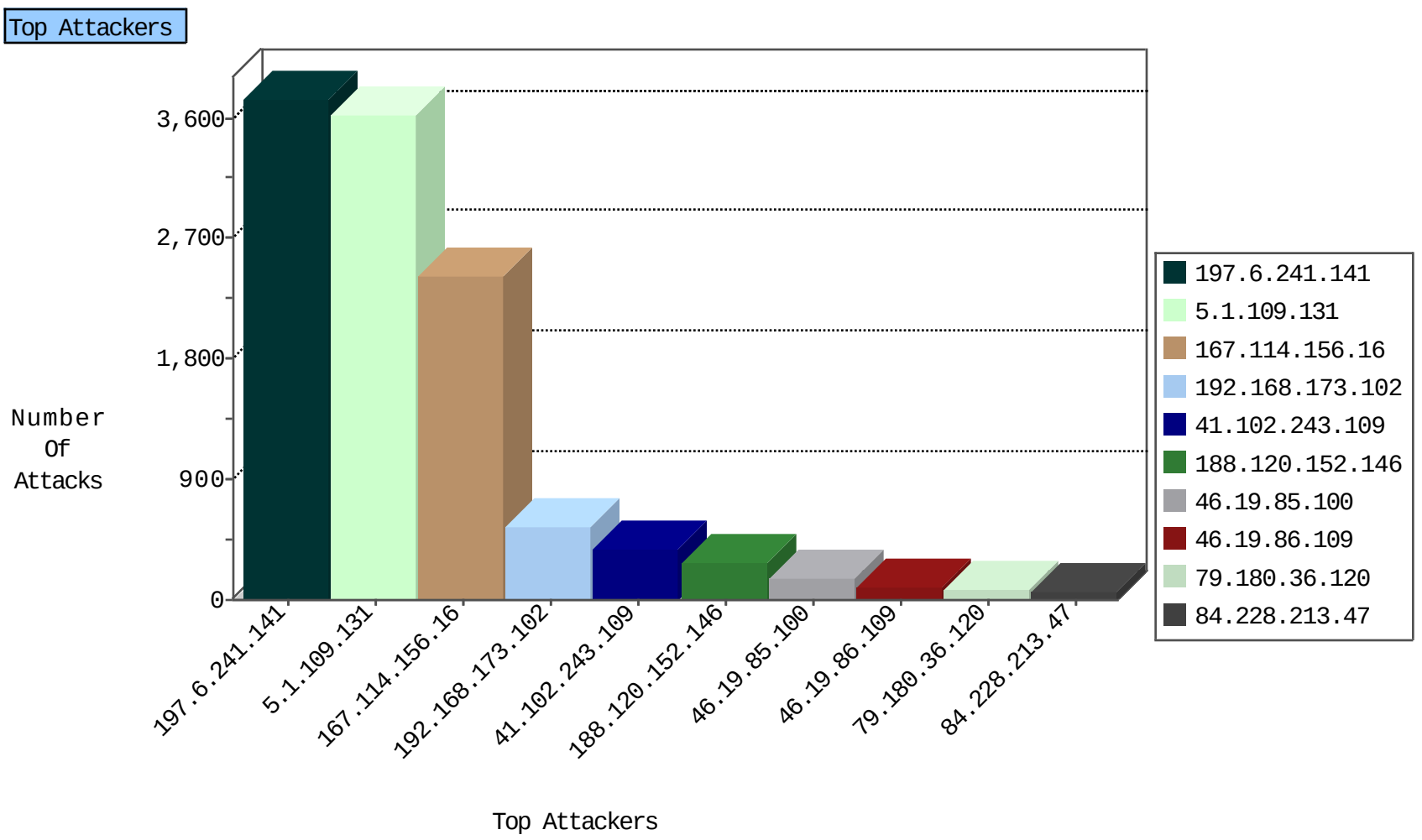
04-07-2016-20:04:08 to 04-07-2016-21:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-07-2016-20:04:08 to 04-07-2016-21:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9456
74.73.166.84	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4739
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2425
207.159.160.150	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2370
93.63.226.141	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1796
197.1.145.78	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1015
197.17.77.206	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	940
108.92.25.81	United States	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	892
197.6.241.141	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	576
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	142
66.67.116.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
120.132.50.135	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	4
46.120.79.253	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
197.6.241.141	Tunisia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
192.116.50.114	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
80.82.78.38	Netherlands	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
200.152.225.183	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
80.82.78.38	Netherlands	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
185.9.157.106	Turkey	147.237.77.205	prisha.idf.il	TCP handshake violation, first packet not syn	drop	2
109.67.187.79	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.44.119.35	Bulgaria	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
85.25.237.162	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
188.161.29.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
197.6.241.141	Tunisia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.44.119.36	Bulgaria	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.149.226	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.102.7.226	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.44.119.40	Bulgaria	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.102.7.233	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.70.184.164	Netherlands	147.237.76.38	e.e.meitav.idf.i	L4 Source or Dest Port Zero	drop	1

04-07-2016-20:04:08 to 04-07-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.241.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.121.115.4	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.78.234.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
149.78.168.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-07-2016-20:04:08 to 04-07-2016-21:04:08

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.108.132.58	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.37	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.71	147.237.77.233	United States	atal.idf.il	SERVER-WEBAPP JBoss web console access attempt	1
148.163.122.135	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
209.126.230.71	147.237.77.226	United States	www.chamatz.aka.idf.il	SERVER-WEBAPP JBoss web console access attempt	1
85.90.246.134	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.230.71	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP JBoss web console access attempt	1
80.178.13.95	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
209.126.230.71	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.212.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.230.71	147.237.77.205	United States	prisha.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
67.219.95.53	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.230.71	147.237.76.86	United States	navy.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
66.249.69.124	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.18	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
213.57.143.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
148.163.122.135	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
209.126.230.71	147.237.77.233	United States	atal.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
85.105.74.172	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.230.71	147.237.77.226	United States	www.chamatz.aka.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
81.214.69.175	147.237.0.33	Turkey	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.230.71	147.237.77.216	United States	dover.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
80.82.78.38	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.71	147.237.77.205	United States	prisha.idf.il	SERVER-WEBAPP JBoss web console access attempt	1
67.219.95.53	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.230.71	147.237.76.86	United States	navy.idf.il	SERVER-WEBAPP JBoss web console access attempt	1
67.219.95.53	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.18	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-07-2016-20:04:08 to 04-07-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.6.241.141	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3734
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3271
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	335
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	245
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	202
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	145
160.176.35.17	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
45.216.202.121	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
84.95.252.59	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
70.155.28.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
54.89.135.66	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
54.89.135.66	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	17
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
54.89.135.66	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
188.161.29.12	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
216.191.95.14	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
185.3.147.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
109.253.202.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
89.139.145.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
64.233.172.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
109.253.198.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
84.95.252.59	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.27.105.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.32.97	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	11
197.9.226.54	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
132.74.244.142	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.80.170.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
64.233.172.171	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.18.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.23.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.70.13.47	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
77.125.72.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
109.253.202.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.46.39.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.8.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
64.233.172.163	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.137.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.210.187.188	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.254.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.120.152.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	269
46.19.85.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	148
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
79.180.36.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
84.228.213.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
95.35.204.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
46.210.152.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	16
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	12
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.52.168.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
89.139.145.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
54.89.135.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.89.135.66	Block	4
131.253.25.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.137.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.18.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.193.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
54.172.101.71	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.172.101.71	Block	2
54.209.250.192	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.209.250.192	Block	2
54.165.111.78	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.165.111.78	Block	2
79.180.24.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.223	Block	1
149.202.239.134	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.65.94.133	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.66.97	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sidebar/sidebar.js	Block	1
85.64.7.222	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter &bc in aka.idf.il/main/giyus/captcha.ashx	None	1
209.126.230.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /web-console/serverinfo.jsp	Block	1
54.89.135.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1383-he/-	Block	1
77.125.72.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
46.19.86.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/scripts/general.js	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
37.59.111.20	France	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/changelog.txt	Block	1
95.70.21.225	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
80.82.78.38	Netherlands	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
201.234.199.242	Ecuador	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/es	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1672	Block	1
52.91.236.246	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 52.91.236.246	Block	1
159.203.4.15	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
109.65.94.133	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	1
2.54.148.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.70.13.47	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
65.254.33.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1