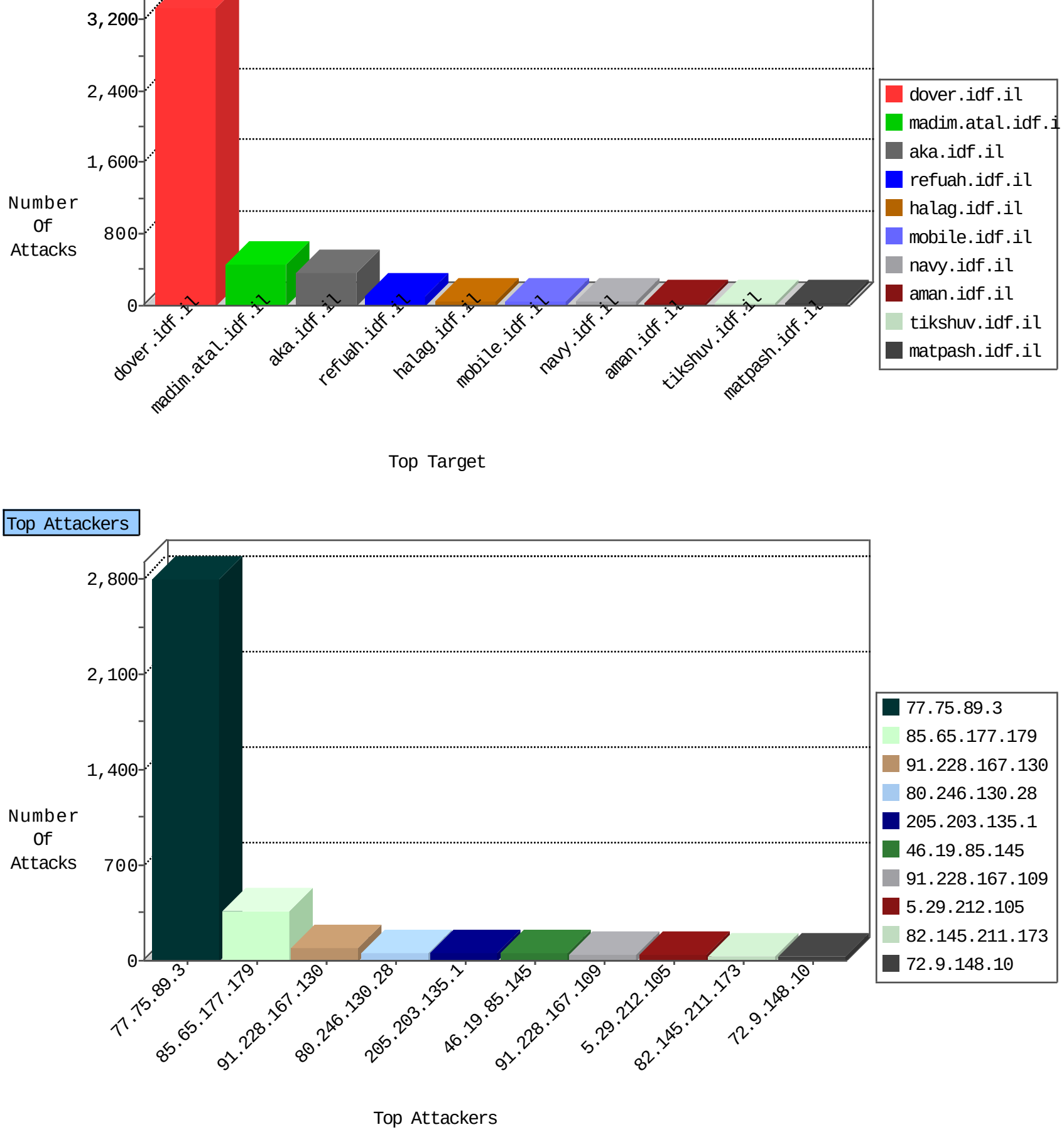
03-08-2016-19:04:09 to 03-08-2016-20:04:09

IDF Under Attack Daily Report



03-08-2016-19:04:09 to 03-08-2016-20:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.75.89.3	Lebanon	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	133
82.145.211.173	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	31
79.176.197.214	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
77.75.89.3	Lebanon	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.181.3.229	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.67.25.102	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
77.75.89.3	Lebanon	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.142		147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.218	Germany	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.142		147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
52.74.130.32	United States	147.237.76.38	e.e.meitav.idf.il	Invalid L4 Header Length	drop	1
71.6.216.61	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
78.152.21.90	Poland	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1

03-08-2016-19:04:09 to 03-08-2016-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.50.97.138	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.22.130.89	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
85.64.240.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
131.253.25.240	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.148.246	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.44	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.214.249.145	Romania	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-19:04:09 to 03-08-2016-20:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.93.117	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
5.39.222.253	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.203.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.255.137.113	147.237.76.30	Belgium	himush.idf.il	ET SCAN NMAP -sS window 2048	1
84.109.226.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.54.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.255.137.113	147.237.0.17	Belgium	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
79.178.205.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.255.137.113	147.237.0.17	Belgium	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
79.178.122.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.115.206.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.102.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.70.160.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.184.198.210	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
109.65.183.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.184.198.210	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.5.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.163.145.38	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
5.39.222.253	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
85.250.85.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.137.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.255.137.113	147.237.76.30	Belgium	himush.idf.il	ET SCAN NMAP -f -sS	1
80.246.136.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.255.137.113	147.237.0.17	Belgium	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
79.178.142.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.159.18.242	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
42.159.244.127	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
109.253.198.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.184.198.210	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
31.184.198.210	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.72.217	Austria	e.idf.il	ET SCAN NMAP -sS window 1024	1

03-08-2016-19:04:09 to 03-08-2016-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.75.89.3	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2641
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
80.246.130.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
5.29.212.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
77.75.89.3	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
31.210.189.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.26.149.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
2.54.19.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.65.193.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.109.212.229	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.34.196.95	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.183.34.163	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
17.78.79.134	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.199	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.195	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.108.164.86	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
93.184.12.100	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
181.166.221.201	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.184.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.153.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.164.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.152.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.161.71	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
185.32.179.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.31.55.69	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.176.207.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.45	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.128.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.134.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
88.255.245.248	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.164.42	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.180	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
84.228.155.163	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.132.175	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
149.88.165.2	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.139.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.244.100	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.177.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	368
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
176.13.3.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.65.193.218	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	5
87.71.9.229	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.71.9.229	Block	4
109.253.196.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.131.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.124	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.3.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.123.188	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
176.13.21.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.193.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
5.102.242.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	3
31.168.123.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.192.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/shachar	Block	2
46.19.86.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.238.240.40	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
87.70.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	1
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/shared/usercontrols/headerupper/	Block	1
80.246.130.28	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.236.24.52	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
93.172.162.104	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
84.228.155.163	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
217.132.43.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
185.32.179.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.211.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.70	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluiml	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
85.64.32.242	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
185.99.32.3		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.100.59	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
140.115.111.127	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter amp in www.aka.idf.il/brothers/skira/default.asp	None	1
2.52.153.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
92.99.19.63	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/kamlar/contact/	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
37.26.148.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.1.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.243.55.134	Dominica	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/110539.pdf,	Block	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
140.115.111.127	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter service in www.aka.idf.il/brothers/skira/default.asp	None	1
5.29.212.105	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
92.99.19.63	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.108.136.80	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/resource/userfollowresource/create/	Block	1
207.46.13.127	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdfg2=whvq9jgvov3igm-oflegda	Block	1