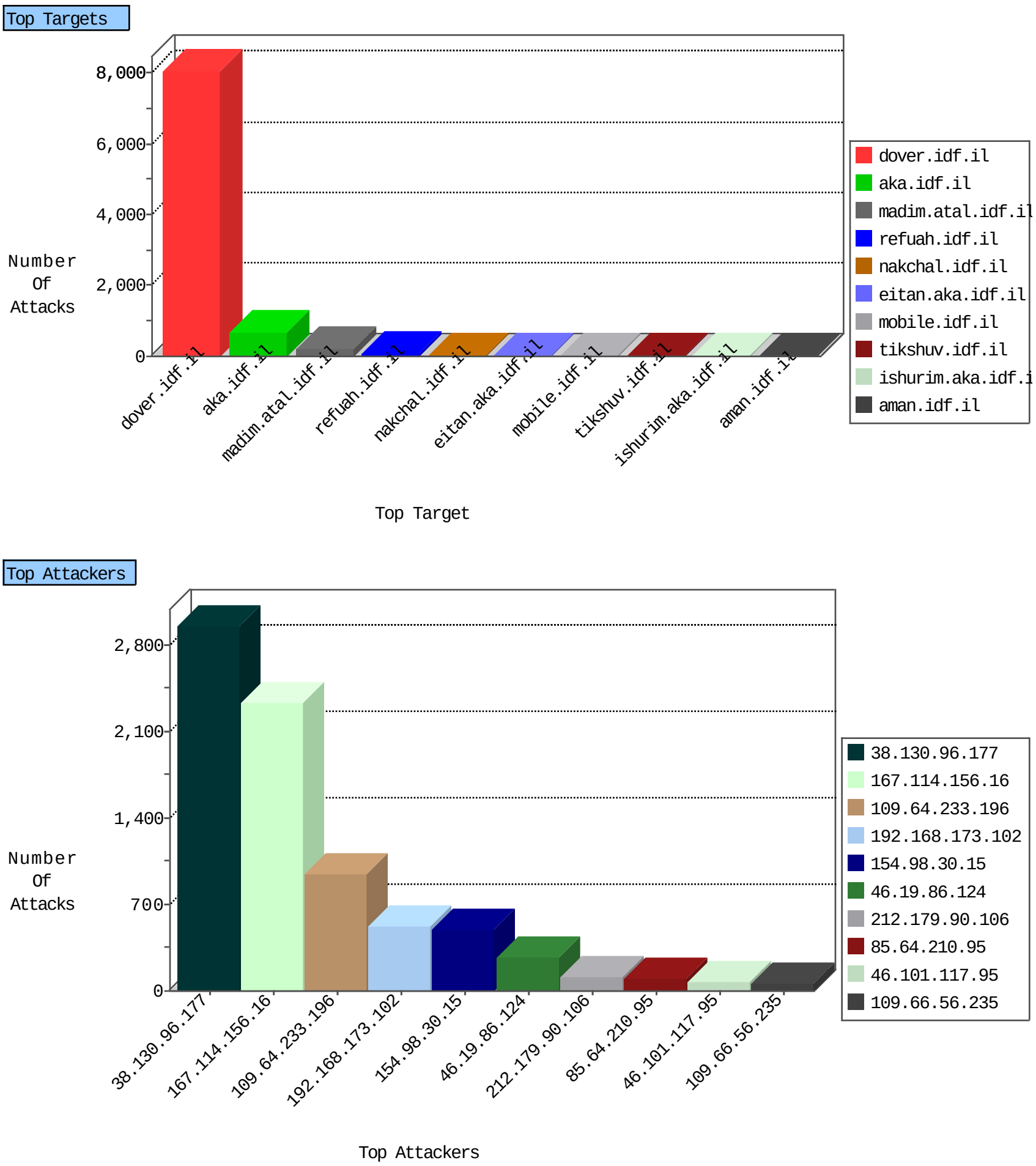
04-10-2016-19:04:07 to 04-10-2016-20:04:07

IDF Under Attack
Daily Report



04-10-2016-19:04:07 to 04-10-2016-20:04:07

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	Block_Ip_Web_In	drop	2339
154.98.30.15	Sudan	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	979
79.177.85.153	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	881
212.179.90.106	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	594
154.98.30.15	Sudan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	584
38.130.96.177	United States	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	501
38.130.96.177	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	213
156.205.95.137	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	150
109.64.233.196	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	144
109.64.233.196	Israel	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	130
84.111.226.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	108
192.168.33.247		147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	45
192.116.210.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
154.98.30.15	Sudan	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	38
38.130.96.177	United States	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	23
38.130.96.177	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	21
109.64.233.196	Israel	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	18
46.19.85.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
10.0.0.8		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
38.130.96.177	United States	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	7
192.168.33.247		147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	6
109.67.202.246	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
5.22.131.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
194.187.168.204	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
69.175.127.10	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.16.69.121	Iran, Islamic Republic of	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.46.39.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.31.60.249	France	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
79.177.108.30	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.168.33.247		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.131.237	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.170	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
134.170.27.72	United States	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1

04-10-2016-19:04:07 to 04-10-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
178.63.86.11	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
212.47.253.128	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
84.228.226.57	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
178.63.86.11	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
212.47.253.128	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
212.47.253.128	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
178.63.86.11	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-19:04:07 to 04-10-2016-20:04:07

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	3
66.249.75.136	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.223	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
80.179.35.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.98.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.166.138.210	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
189.218.249.49	147.237.77.243	Mexico	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.88.225.181	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.111.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
139.162.150.131	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
5.28.159.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.83.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
1.189.209.194	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.65.54.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
1.189.209.194	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.42.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.111.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.138.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.103.252.98	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.235.207.151	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
45.79.137.87	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
139.162.150.131	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
31.168.80.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.155.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
1.189.209.194	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
87.69.207.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
1.189.209.194	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

04-10-2016-19:04:07 to 04-10-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
38.130.96.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2058
38.130.96.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	600
109.64.233.196	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	520
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	336
154.98.30.15	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	302
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	273
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	182
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
109.64.233.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
46.101.117.95	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
109.66.56.235	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
109.64.233.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	47
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
46.19.85.54	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.64.233.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
156.205.95.137	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
73.253.227.193	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.120.70.96	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
84.108.136.224	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
5.22.131.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
213.151.48.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.150.136	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.71.118.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.64.32.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.211.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.108.108.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
185.32.179.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.154	Israel	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	9
85.65.88.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
146.185.61.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.46.39.45	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
217.132.131.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
81.245.54.46	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.113.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.120.126.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.120.248.105	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.210.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
37.26.148.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
87.69.151.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
185.32.179.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
176.13.7.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
79.183.204.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.138.163.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
198.50.189.250	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.50.189.250	Block	2
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
131.253.25.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.71.43.52	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
198.50.189.250	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
46.19.86.126	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
141.212.122.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /x	Block	1
109.64.206.1	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
79.178.134.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
41.207.3.216	Cote D'Ivoire	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/faq.aspx	Block	1
181.137.221.232	Colombia	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
114.97.56.215	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 114.97.56.215	Block	1
87.71.43.52	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
200.74.240.180	Panama	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
37.187.157.108	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
149.88.40.133	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.64.206.1	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.64.206.1	Block	1
181.137.221.232	Colombia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
89.46.89.148	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
212.76.96.98	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/61622.jpg	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
157.55.39.109	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/tizmoret/news/<a href=	Block	1
109.65.35.224	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authenticationservice.asmx/getauthuser	Block	1
40.77.167.6	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
109.66.56.235	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
31.168.88.91	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
105.105.28.149	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
41.46.186.124	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
176.228.166.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
109.253.216.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1

04-10-2016-19:04:07 to 04-10-2016-20:04:07