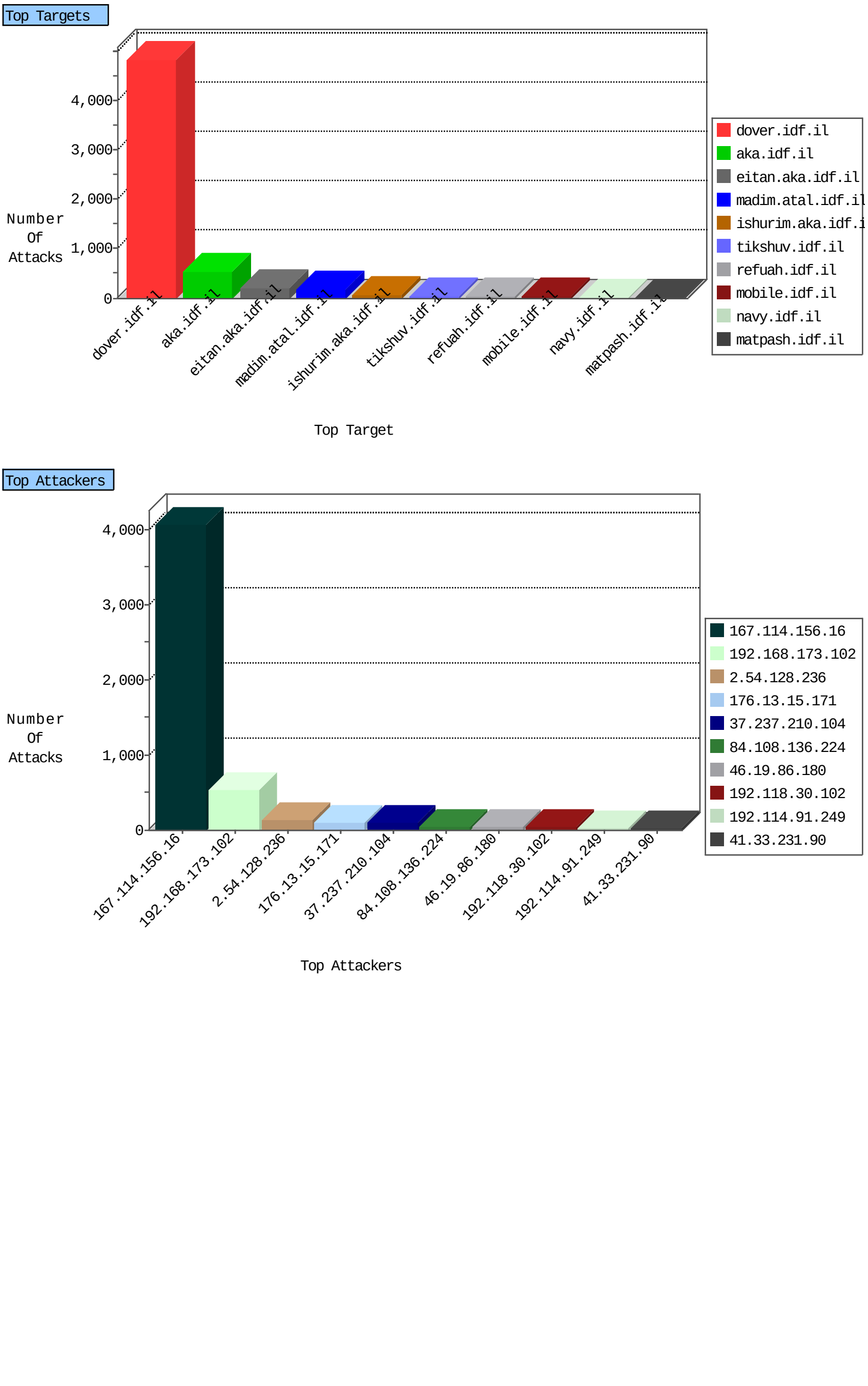
04-10-2016-14:04:02 to 04-10-2016-15:04:02

IDF Under Attack Daily Report



04-10-2016-14:04:02 to 04-10-2016-15:04:02

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	4063
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	411
37.237.210.104	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	22
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
62.219.196.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
204.12.196.234	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
69.30.226.102	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
173.208.197.252	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
69.30.226.220	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
69.30.198.150	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
107.150.32.62	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
192.114.23.211	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
69.30.226.100	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
74.91.20.196	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
105.155.0.34	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1
5.39.0.222	France	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
185.24.206.57	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.199.9.225	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
74.82.47.57	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
82.145.216.141	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	1
62.138.2.83	Germany	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
88.150.206.225	United Kingdom	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1

04-10-2016-14:04:02 to 04-10-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.57.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
80.74.110.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
212.150.125.221	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
149.78.206.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
31.168.123.247	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
31.168.216.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.93.101	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.93.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
46.19.85.19	Israel	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

04-10-2016-14:04:02 to 04-10-2016-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.62.41.72	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.132.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.76.34	Italy	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
109.226.27.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.146.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
202.152.10.104	147.237.0.35	Indonesia	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.117.30.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.72.14	Latvia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
40.84.148.3	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
185.120.126.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.85.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.225.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.205.152.52	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.141.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.158.255.194	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.78.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.99.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.168.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.99.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.26.147.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.89.217.228	147.237.72.166	Netherlands	aka.idf.il	portscan: TCP Distributed Portscan	1

04-10-2016-14:04:02 to 04-10-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	359
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	186
176.13.15.171	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
46.19.86.180	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	49
84.108.136.224	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
37.237.210.104	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	28
37.237.210.104	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.86.108	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	23
207.241.229.223	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
192.114.91.249	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
207.241.229.222	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
31.154.16.68	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.103	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
46.19.86.220	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	15
37.26.148.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.237.210.104	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.221	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	11
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.93.101	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
105.105.83.175	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.241.229.225	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.31.98.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
5.102.227.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.102.227.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
5.102.227.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.114.91.249	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.133.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.73	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
213.8.123.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.37.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.245.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.137.69.143	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.150.25.79	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.237.210.104	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.194.203.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
81.218.165.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.244.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.238.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.62.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.117.195.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.150.201.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.32.190	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.195.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.66	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.154.31	Israel	147.237.72.166	aka.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
2.54.128.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
109.253.202.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
37.26.149.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	13
185.32.179.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.26.147.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
91.227.164.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.53.39.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.128.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.160.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.50.39.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
91.227.165.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.199.9.225	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.20.23	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
176.13.6.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl37 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.64.10.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
37.236.136.140	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Cookie Tampering on cookie wb48617274: Expected 7A40C6FE, Observed 6D71F8BB	None	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
178.154.149.6	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1460288781706	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/30012011masaiyot.aspx	Block	1
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1460288775587	Block	1
37.237.158.144	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.255.253.14	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1460288787686	Block	1
69.30.198.150	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.app-softwares.com/	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl57 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
152.62.109.203	Europe	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
109.67.53.235	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
37.236.136.215	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.6.11	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
185.3.147.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal/site/templates/controller.asp	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.237.210.104	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
141.212.122.129	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /x	Block	1
31.168.50.46	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
69.30.226.102	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
169.229.3.90	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/rec.dat	Block	1
37.236.137.71	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.136.216	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.254.241.7	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
87.70.125.233	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
41.107.97.131	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
141.212.122.129	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1