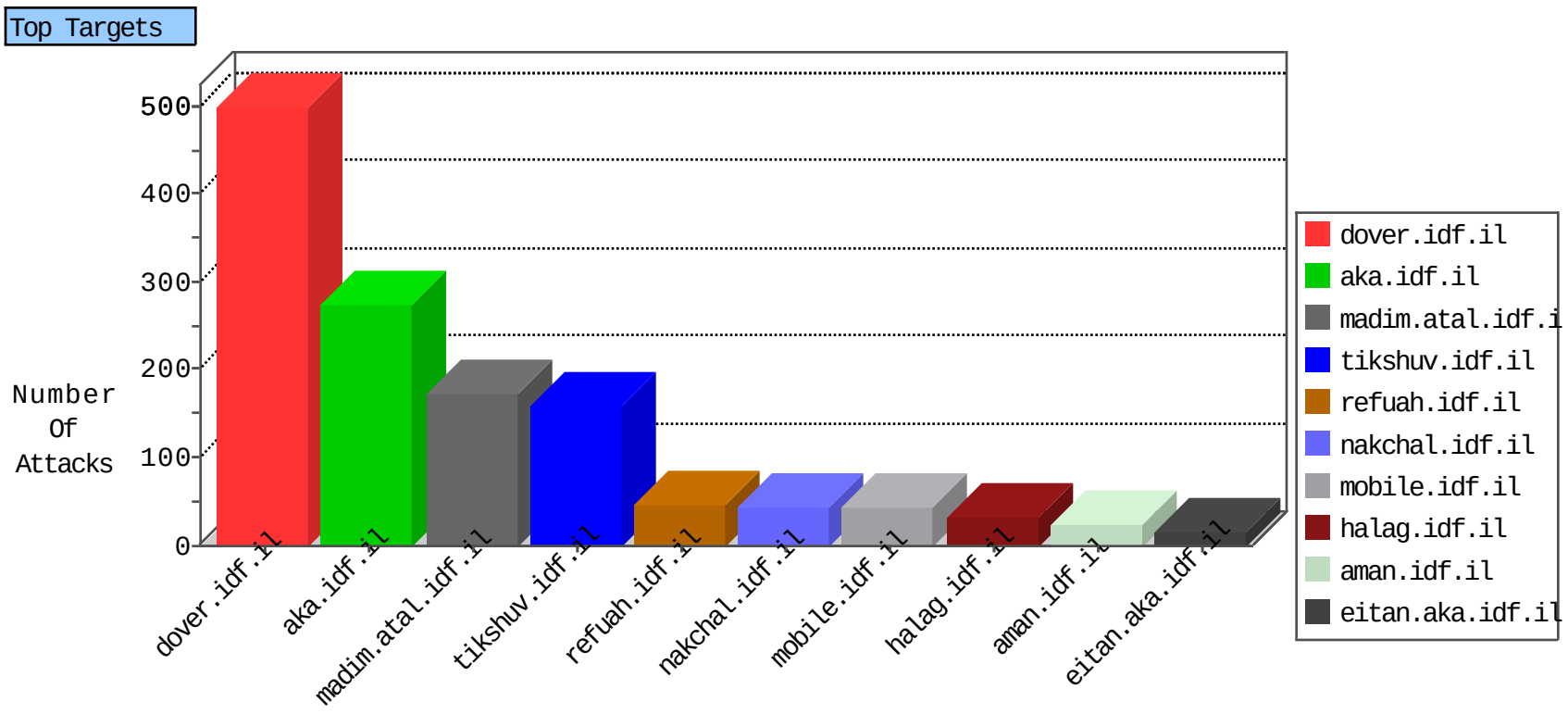
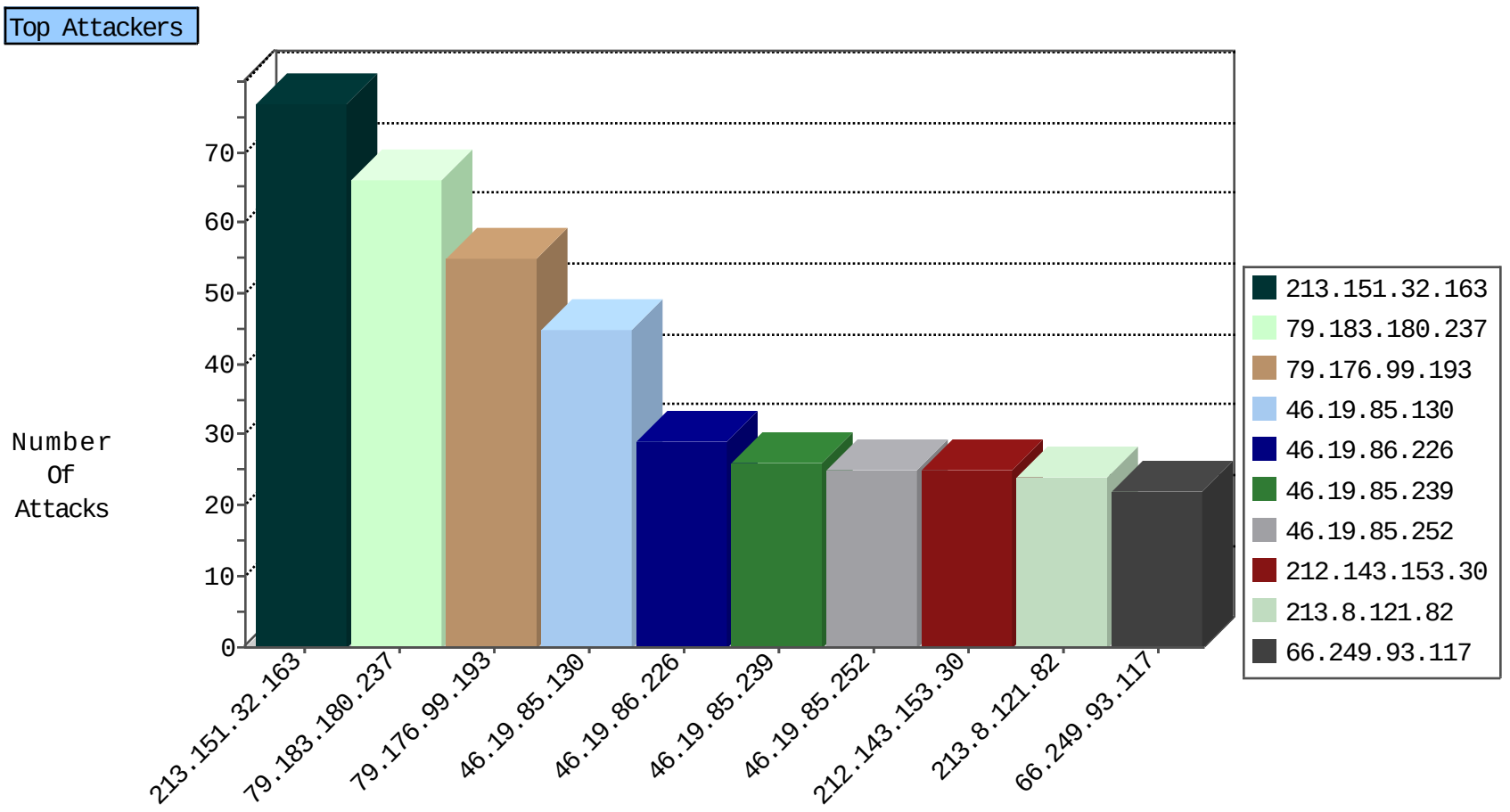
03-07-2016-15:04:08 to 03-07-2016-16:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-15:04:08 to 03-07-2016-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
2.54.135.135	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
2.52.58.242	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
46.19.86.116	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
5.22.130.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
209.126.105.33	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
1.34.207.31	Taiwan	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
209.126.105.33	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
209.126.105.33	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
1.34.207.31	Taiwan	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
209.126.105.33	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
198.48.92.104	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.50	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
209.126.105.33	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
209.126.105.33	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

03-07-2016-15:04:08 to 03-07-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.180.237	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	66
84.108.61.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.110.192.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.142.156.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
66.249.69.95	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.160	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.88.197.224	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.182.113.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
94.159.180.213	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
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
87.71.91.100	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-07-2016-15:04:08 to 03-07-2016-16:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
52.87.243.150	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
199.203.37.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.87.243.150	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.89.217.227	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.25.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.69.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.179.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.138.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.251.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.147.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.193.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.87.243.150	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.87.243.150	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
5.29.112.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.229.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.184.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.197.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.154.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.94.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.155.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.153.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.146.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-07-2016-15:04:08 to 03-07-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.130	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
212.143.153.30	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
213.8.121.82	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	18
87.69.205.163	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.130	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.248	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	10
84.95.232.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
62.219.226.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.0.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.136.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
58.161.132.20	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.57.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.220.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.182.226	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.247.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.126.41.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.126	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.188.227	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.166.136.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.117.134.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.4.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
217.132.23.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.157.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

03-07-2016-15:04:08 to 03-07-2016-16:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
79.176.99.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.18.57	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	8
65.208.151.118	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.118	Block	6
80.178.157.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
80.179.96.89	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.179.96.89	Block	4
65.208.151.113	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.113	Block	4
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
31.168.193.208	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.208.151.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.117	Block	3
65.208.151.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	3
46.19.86.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.7.69.34	France	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	3
81.218.101.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.192.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
65.208.151.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	3
131.253.25.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
77.158.88.42	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	2
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
65.208.151.119	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.119	Block	2
46.19.85.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
94.230.93.16	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
94.230.93.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
27.55.175.61	Thailand	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.136.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.208.151.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	2
109.67.14.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $74 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
185.89.217.234		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.38.37	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
95.86.106.230	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 95.86.106.230	Block	2
109.67.14.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $117 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.8.204.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
94.230.93.48	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
67.131.60.94	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
185.89.217.228		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.5.151	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
222.164.224.34	Singapore	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.124.164	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/s	Block	1
37.142.203.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	1
66.249.69.11	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
203.127.96.201	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
24.105.137.142	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-07-2016-15:04:08 to 03-07-2016-16:04:08