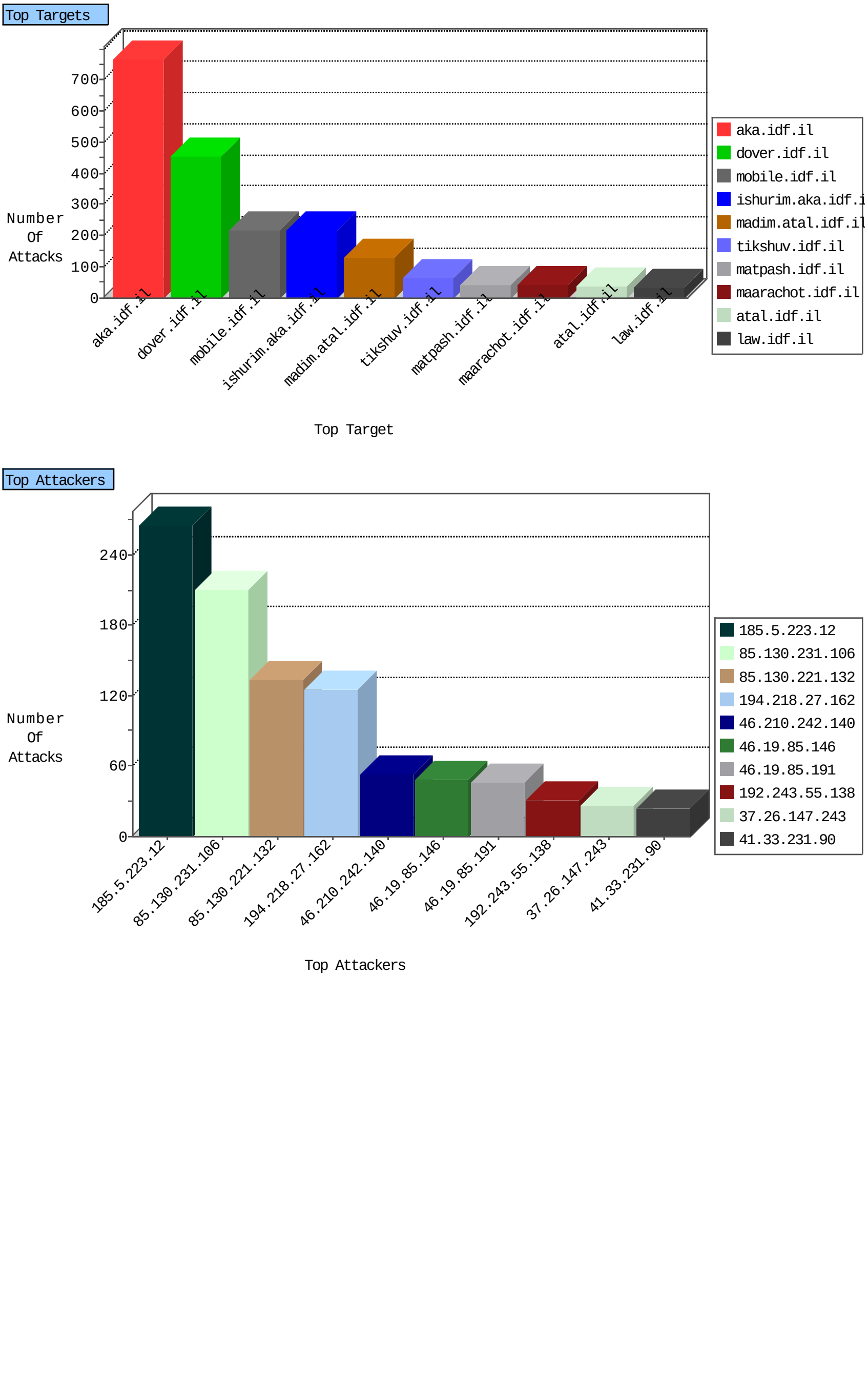
03-01-2016-12:04:08 to 03-01-2016-13:04:08

IDF Under Attack Daily Report



03-01-2016-12:04:08 to 03-01-2016-13:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.64.162	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
159.104.163.19	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
183.37.23.62	China	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
159.104.163.20	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.93.185.252		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
159.104.163.17	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.21	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
85.25.218.201	Germany	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
159.104.163.18	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.104.163.22	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.248.172.207	Netherlands	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-12:04:08 to 03-01-2016-13:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.129.204	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
5.29.86.179	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.214.46	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
194.90.25.90	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.9.151.22	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
80.246.133.113	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.86.126	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
174.34.135.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
61.160.195.5	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

03-01-2016-12:04:08 to 03-01-2016-13:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.113.111.134	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
193.106.54.36	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
192.114.91.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.179.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.12.209.58	147.237.72.166	Romania	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.44.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.11.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.31.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.156.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.209.37	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	portscan: TCP Distributed Portscan	1
207.232.18.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.97.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.41.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.30	United States	himush.idf.il	ET DROP Dshield Block Listed Source	1
87.68.34.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.138.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.81.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.118.28.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.132.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.153.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.144.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.48.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.1.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.118.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.50.77.34	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.0.15	Russian Federation	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
46.19.85.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
109.160.209.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.195.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.207.253.96	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.160.2	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
37.26.147.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.41.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.212.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-01-2016-12:04:08 to 03-01-2016-13:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	263
85.130.231.106	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	210
85.130.221.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	81
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	41
37.26.147.243	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
80.178.138.115	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	17
109.65.175.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
176.13.3.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.145.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.20.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.135.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.230.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.223.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
109.253.207.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.230.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
176.13.6.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.139.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
62.0.209.1	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
77.125.120.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.65.210.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.118.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.221.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.149.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.95		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.169.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.221.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.221.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.113.111.134	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
62.0.209.1	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
109.253.150.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.113.111.134	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.28.184.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.21.117	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

03-01-2016-12:04:08 to 03-01-2016-13:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
188.120.154.33	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

03-01-2016-12:04:08 to 03-01-2016-13:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.242.140	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.210.242.140	Block	52
46.19.85.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
109.253.129.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
5.102.219.207	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.102.219.207	Block	12
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	9
79.183.166.5	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 79.183.166.5	Block	7
37.26.146.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
31.154.5.110	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
176.13.9.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.183.166.5	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	4
109.253.135.110	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
31.154.5.110	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.154.5.110	Block	4
109.253.145.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
91.121.141.219	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	4
149.50.86.50	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.13.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.13.63	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
37.26.148.207	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.148.207	Block	3
87.70.26.48	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 87.70.26.48	Block	3
80.246.139.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.207.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.10.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.194	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.102.219.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
5.102.200.21	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.102.200.21	Block	2
176.13.6.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.28.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.70.26.48	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	2
80.246.137.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.20.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.215.243	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.139.15	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	2
109.253.221.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.142.64.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in aka.idf.il/main/sachar/payslips.aspx	None	1
80.246.133.54	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx	Block	1
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/drushim/contactus.aspx	Block	1
31.168.200.103	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.117.121.140	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
184.105.247.196	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
2.54.156.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
89.138.102.220	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

03-01-2016-12:04:08 to 03-01-2016-13:04:08