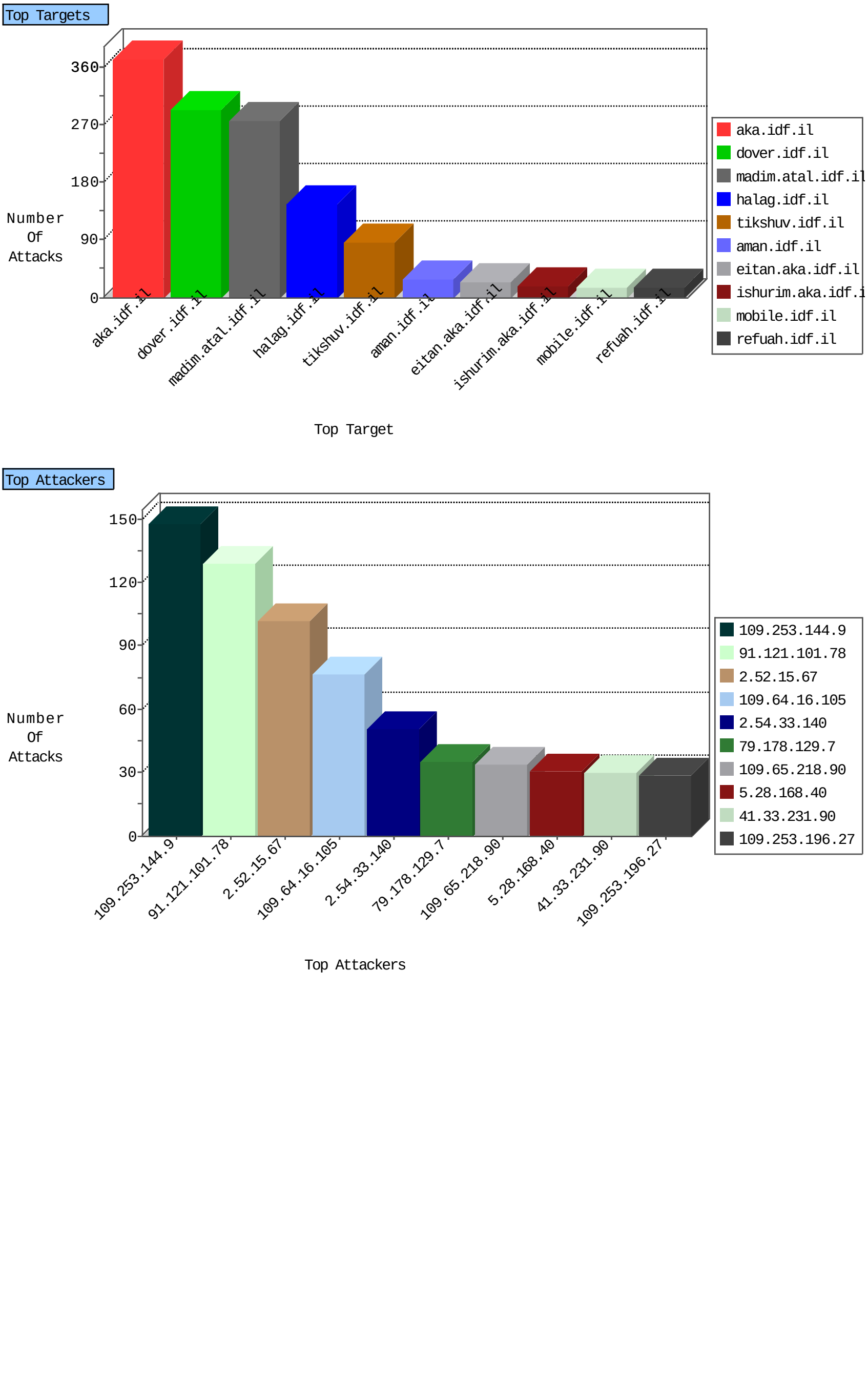
02-25-2016-19:04:07 to 02-25-2016-20:04:07

IDF Under Attack
Daily Report



02-25-2016-19:04:07 to 02-25-2016-20:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.211.122	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
212.179.54.237	Israel	147.237.77.216	dover.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	3
123.130.244.18	China	147.237.76.148	gqcenter.aka.idf.il	Invalid TCP Flags	drop	2
118.213.224.138	China	147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	2
198.23.190.39	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
118.232.250.160	Taiwan	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
198.23.190.39	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
199.26.90.15	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
198.23.190.39	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
202.3.176.43	Taiwan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

02-25-2016-19:04:07 to 02-25-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.101.78	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	90
79.181.201.206	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
10.0.0.11		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
149.78.87.96	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
77.125.143.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.180.149.131	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.57.153.213	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
69.30.213.18	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
46.117.162.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.178.148.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
62.210.97.48	France	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Block	2
176.9.131.69	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.97.48	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
176.9.131.69	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
5.29.151.233	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.97.48	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.88.163.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.97.48	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
162.210.196.100	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.97.48	France	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Block	2
217.132.111.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2

02-25-2016-19:04:07 to 02-25-2016-20:04:07

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	4
62.0.73.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
38.105.146.70	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.76.30	Italy	himush.idf.il	ET SCAN NMAP -sS window 3072	1
128.127.0.45	147.237.76.30	Italy	himush.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.193	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.175.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.210.69.71	147.237.76.30	France	himush.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
38.105.146.70	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
198.20.69.74	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
193.105.134.220	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.76.30	Italy	himush.idf.il	ET SCAN NMAP -sS window 2048	1
120.55.90.163	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.61.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.79.104	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

02-25-2016-19:04:07 to 02-25-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.52.15.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
109.64.16.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	77
91.121.101.78	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	38
79.178.129.7	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
109.65.218.90	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.116.145.189	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.117.67.124	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
62.128.48.50	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
87.68.159.153	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.8.13	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
37.46.38.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.168.93.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.134.229	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
77.125.75.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.145.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.237.234.4	Slovakia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.39	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.7.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.130.237.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
95.35.181.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.237.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
87.69.248.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.130.237.234	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
87.69.248.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.25.111	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.125.152.234	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
94.230.86.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.107.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.43	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.176.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.93	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.211.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.242.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.106.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.143.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.242.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.66	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
172.58.32.228	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.15.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.66.99.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.64.14.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-25-2016-19:04:07 to 02-25-2016-20:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.126.169.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-25-2016-19:04:07 to 02-25-2016-20:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.144.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
2.54.33.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
5.28.168.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
109.253.196.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.250.149.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
107.77.64.92	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	3
85.65.38.41	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 85.65.38.41	Block	3
46.117.40.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
38.106.194.199	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
107.107.187.97	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.130.15	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
198.57.247.217	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
149.50.104.145	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
46.19.86.138	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.217.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
79.178.129.7	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
201.247.229.225	El Salvador	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.229.201	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.61	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
109.253.134.229	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
185.89.217.235		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
46.19.86.183	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
113.85.27.73	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
107.77.64.92	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.181.186.115	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.199.65.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.2.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.241	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/site/links.aspx	Block	1
40.77.167.98	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
85.65.38.41	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/6_s3_	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
198.20.69.74	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
46.116.145.189	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
148.251.21.227	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
213.151.48.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/faq.aspx&sa=u&ved=0ahukewjk3yfotpplahud1ywkhz8daeiqfggkmae&usg=afqjcnefysu6yi5sb7zbjwsjmdbowklaxw	Block	1
176.12.160.5	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.65.248	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
46.19.85.43	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.145.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.69.248.130	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
148.251.21.227	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.65.218.90	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.39.222.159	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/rom-0	Block	1
185.82.200.91		147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.138.68.53	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
79.178.104.59	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1

02-25-2016-19:04:07 to 02-25-2016-20:04:07