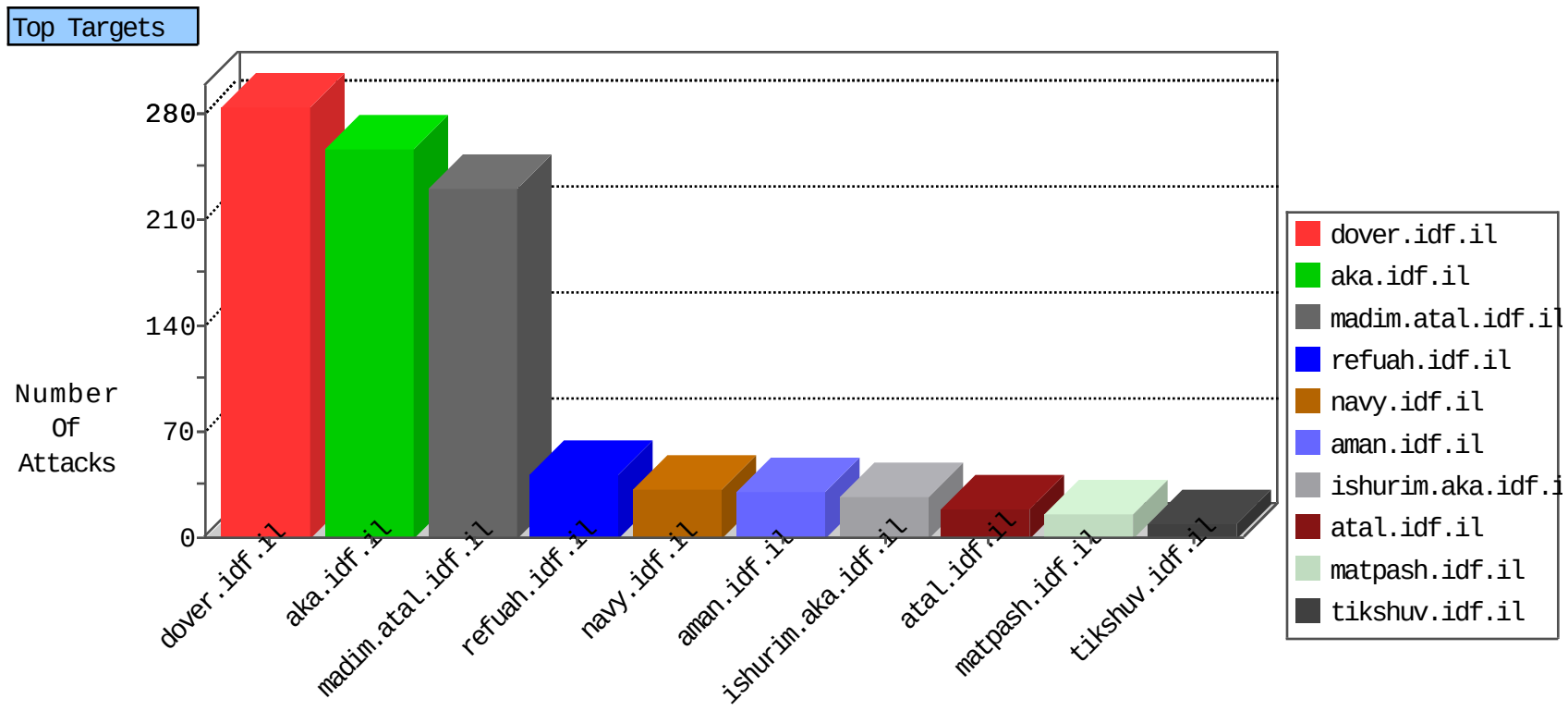
09-14-2016-15:04:07 to 09-14-2016-16:04:07

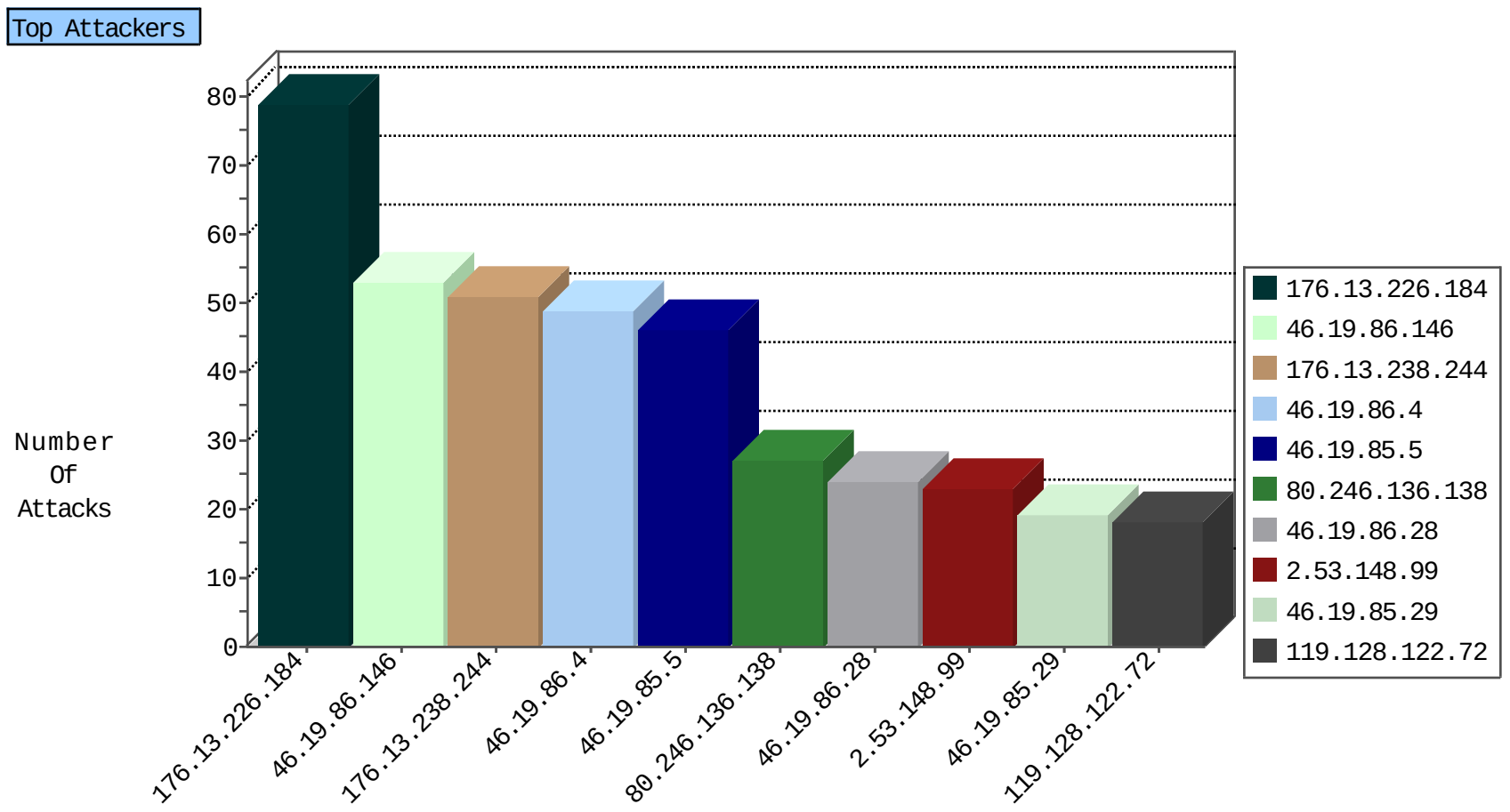
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-14-2016-15:04:07 to 09-14-2016-16:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	511
79.182.45.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
79.179.16.208	Israel	147.237.77.216	dover.idf.il	Black List	drop	6
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.32.84.160	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	4
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.110.84.66	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1
198.133.224.147	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.180	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
199.241.186.187	United States	147.237.72.217	e.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
69.30.193.253	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.253.241.62	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
208.110.84.66	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
198.204.224.234	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
142.54.174.85	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.193.253	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.150.117	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.110.84.70	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
198.204.224.237	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.12.220.85	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.150.117	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
198.204.224.238	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
63.141.242.198	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
156.56.250.227	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-15:04:07 to 09-14-2016-16:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.54.184.90	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-14-2016-15:04:07 to 09-14-2016-16:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
82.80.188.9	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
109.66.126.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
96.10.116.230	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
80.179.222.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
96.10.116.230	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
79.182.25.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
96.10.116.230	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
52.166.130.115	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
96.10.116.230	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.168.170.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.193.74.175	147.237.77.205	Gibraltar	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
212.227.55.94	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.53.54.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.129.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.241.186.187	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
84.109.214.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.201.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.102.169.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.48.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
96.10.116.230	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.178.72.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
96.10.116.230	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
96.10.116.230	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.35.152.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.172.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.164.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.136.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.241.186.187	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
85.64.39.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.248.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-14-2016-15:04:07 to 09-14-2016-16:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
46.19.86.146	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
62.0.200.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
79.180.205.144	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
80.246.136.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
176.13.245.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
109.253.200.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
62.114.202.72	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
62.0.219.129	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	10
176.13.248.43	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
80.246.136.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.86.146	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
31.154.17.106	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.55.35.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.86.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.51	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.22.161	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.90	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.55.35.110	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
176.13.22.161	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
80.246.136.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.51	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
130.37.186.115	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.200.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
93.172.212.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.233.16	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.146.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
130.37.186.115	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.16.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.190.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.241.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.130.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.218.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.117.6.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.55.35.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.236.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
62.0.212.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

09-14-2016-15:04:07 to 09-14-2016-16:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.226.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
176.13.238.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
2.53.148.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
119.128.122.72	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 119.128.122.72	Block	11
79.177.72.135	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
80.246.140.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
119.128.122.72	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
2.53.171.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
192.116.142.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
176.13.225.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.117.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.120.148.79	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.13.228.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
159.203.71.236	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
46.19.85.105	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
105.102.87.84	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
81.218.104.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
159.203.100.247	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
145.132.105.78	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.102.6.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
89.241.136.206	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
31.168.8.110	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	1
174.17.251.21	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method i[[#0]][[#0]][[#0]]BôYÀÛÀm[[#18]]™k‰b=œ[[#19]][[#15]]í[[#27]]S•Ã[[#3]][[#5]][[#6]]¶Á[[#11]]MwÌl'¾[[#20]]TAÎ.ZLÌ[[#5]]É!*k›M"›ºã[[#26]]úÙøÚ{ô;h½örP‡[[#20]]Y,üÊoõÎ4œ^¾Hßø.Þr¼[[#4]]ÖÙ1ãg{H[•}() in URL	Block	1
159.203.75.185	United States	147.237.77.170	maarachot.idf.il	Unauthorized Method HEAD for 147.237.77.170/	Block	1
66.249.66.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.19.85.149	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/bottomcap.gif	Block	1
109.67.50.247	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
82.81.140.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.3.147.254	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.177.72.135	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
159.203.104.0	United States	147.237.0.34	tikshuv.idf.il	Unauthorized Method HEAD for 147.237.0.34/	Block	1
147.210.63.234	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/print.css	Block	1
104.236.43.72	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.26.149.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
159.203.79.95	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
84.108.5.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
2.53.37.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.46.214.61	Switzerland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
79.177.72.135	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.177.72.135	Block	1
174.17.251.21	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
159.203.71.236	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1

09-14-2016-15:04:07 to 09-14-2016-16:04:07