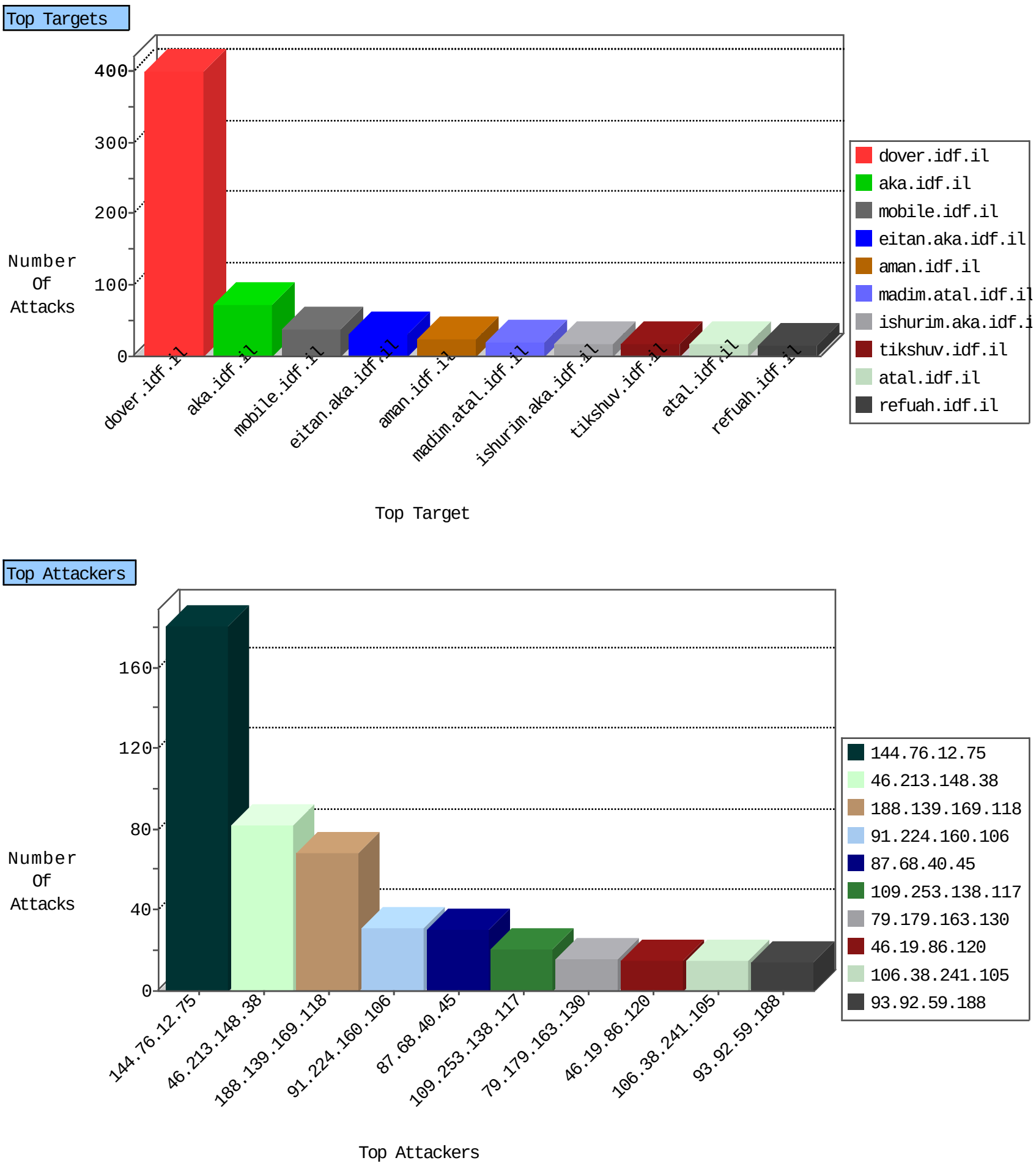
09-16-2016-20:04:09 to 09-16-2016-21:04:09

IDF Under Attack Daily Report



09-16-2016-20:04:09 to 09-16-2016-21:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	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
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-16-2016-20:04:09 to 09-16-2016-21:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	179
144.76.12.75	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-16-2016-20:04:09 to 09-16-2016-21:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
112.25.62.3	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
91.224.160.106	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.242	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
91.224.160.106	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.77.176	Indonesia	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
113.251.130.224	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.160.106	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
112.25.62.3	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
77.127.23.231	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
91.224.160.106	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.166	Netherlands	aka.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
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
185.129.148.230	147.237.8.14	Latvia	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
133.242.4.52	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

09-16-2016-20:04:09 to 09-16-2016-21:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.213.148.38	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
46.213.148.38	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	41
188.139.169.118	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	34
188.139.169.118	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
87.68.40.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.138.117	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.102.219.40	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.179.163.130	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	8
217.132.150.183	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.179.163.130	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.145.222.76	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
93.92.59.188	Hungary	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
46.19.85.85	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
159.220.74.2	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.26.148.217	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		monitor	4
46.19.86.202	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
93.92.59.188	Hungary	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.92.59.188	Hungary	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.178.37.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.236.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.121.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.148.181	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.40.139.39	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
46.19.86.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.217	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
186.103.235.124	Chile	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.226.217.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
93.157.82.130	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	2
37.142.9.144	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.148.217	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	alert	2
159.220.74.2	United Kingdom	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
37.26.149.245	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.228.83	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.183	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
93.92.59.188	Hungary	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
208.70.120.26	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.121.70.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.46.39.157	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
37.26.148.217	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
2.53.62.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.139.58.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.228.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-16-2016-20:04:09 to 09-16-2016-21:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.122.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
77.138.85.139	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	6
96.83.209.97	United States	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	4
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.236.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
96.83.209.97	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 96.83.209.97	Block	2
96.83.209.97	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/	Block	2
89.139.58.164	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/994-he/refuah.aspx	Block	2
84.108.67.18	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
77.139.171.156	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	2
77.139.231.3	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/navy/navy/general.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/chamatz/home/default.asp	Block	1
5.102.242.176	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
85.64.134.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.52.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=fbd9591fdc1af96e.1474048707.1.1474048707.1474048707.;	Block	1
79.181.5.131	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/112933.pd	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
5.102.253.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mai/giyus	Block	1
185.12.186.44	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized Method POST for 147.237.77.216/	Block	1
85.65.131.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
77.138.159.134	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.159.134	Block	1
213.186.78.86	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/library/generaldoc.asp	Block	1
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method %3A%2F%2Fm.facebook.com%2F%22%5D; in URL _pk_id.20.8afc=fbd9591fdc1af96e.1474048707.1.1474048707.1474048707.	Block	1
68.180.228.251	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1110-he/nakhal.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
207.46.13.166	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
77.138.159.134	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunpersonalquestionnaire.aspx	Block	1
136.243.16.208	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
77.138.66.125	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
213.8.204.45	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
96.83.209.97	United States	147.237.0.34	tikshuv.idf.il	Unauthorized HTTP Method	Block	1
46.19.86.120	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx	Block	1
2.53.129.207	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.29	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
84.111.110.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.77.55	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
213.8.204.45	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1

09-16-2016-20:04:09 to 09-16-2016-21:04:09