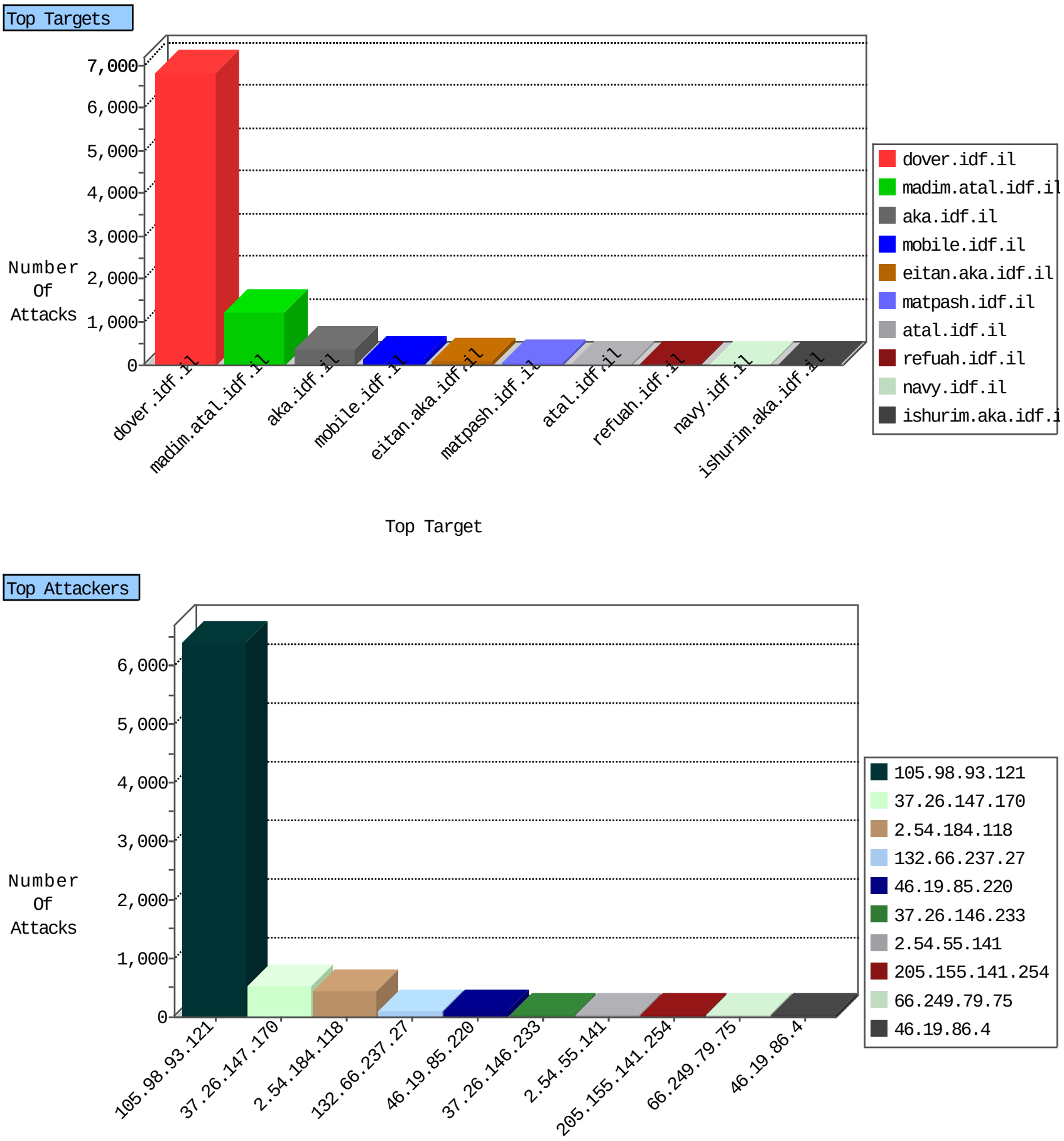
02-09-2016-19:04:08 to 02-09-2016-20:04:08

IDF Under Attack Daily Report



02-09-2016-19:04:08 to 02-09-2016-20:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	6922
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3100
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	503
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	229
66.249.79.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	30
66.249.79.77	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
104.131.226.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
105.224.174.217	South Africa	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
69.171.230.98	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
217.31.54.202	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
157.55.39.39	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
173.252.88.94	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
31.13.112.121	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
157.55.39.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
31.13.112.121	Ireland	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
173.252.74.110	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.0.100.226	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
157.55.39.209	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.145.57.38	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
157.55.39.113	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
165.139.83.106	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
142.54.169.163	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
173.252.90.228	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
31.13.97.104	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
173.252.88.94	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
157.55.39.113	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
31.13.112.121	Ireland	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
165.139.83.106	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
142.54.160.214	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
78.52.103.15	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

02-09-2016-19:04:08 to 02-09-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.125.125.79	China	147.237.77.216	dover.idf.i	C103: HTTP: User Agent Sogou+web+spider	Block	1
105.98.93.121	Algeria	147.237.77.216	dover.idf.i	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	1

02-09-2016-19:04:08 to 02-09-2016-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.147.170	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
31.168.78.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
109.186.189.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.194.202.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.66.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.128.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.160.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.57	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
82.81.75.147	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.201.227.57	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
79.183.191.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
165.91.48.186	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
77.85.35.211	147.237.77.243	Bulgaria	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
125.65.165.215	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.142.68.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.77.176	Canada	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
217.132.10.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.178.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.85.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.22.129.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.193.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.57	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
79.183.202.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.57	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.177.215.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
77.85.35.211	147.237.77.243	Bulgaria	mobile.idf.il	ET SCAN NMAP -f -sS	1
125.65.165.215	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
37.142.147.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-09-2016-19:04:08 to 02-09-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4065
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	228
132.66.237.27	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Attack		reject	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
205.155.141.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.13.10.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.154.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
85.250.103.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.235.22.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
37.26.147.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
95.35.202.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.49.175	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.134	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
94.230.86.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.117.120.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.139.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
205.155.141.254	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.177.128.216	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.166.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.242.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.22.129.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.193.249.95	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.22.135.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
216.81.81.80	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
130.193.51.64	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
80.179.119.22	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.67.130.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
74.57.147.88	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.222.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.19	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.240.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.132.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
130.193.37.23	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
31.210.191.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.111.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.144.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
149.78.242.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.10.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-09-2016-19:04:08 to 02-09-2016-20:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.183.14.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.184.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	269
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.170	Block	263
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
2.54.184.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.147.170	Block	118
46.19.85.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
37.26.146.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
2.54.55.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
2.54.184.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	46
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.10.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
128.194.131.235	United States	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	6
2.52.24.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	5
37.142.217.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu	Block	4
37.26.147.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.154.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
158.69.2.11	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	3
2.54.156.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.132.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.21.209	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
158.69.2.11	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
85.64.122.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	3
85.250.103.192	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.108.154.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
89.138.166.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.243	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
46.19.86.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.52.183.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.5.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.236.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.139.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.45.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
165.91.48.186	United States	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	2
37.26.149.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.229.197.249	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/miluim.aspx	Block	1
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
79.182.165.123	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/994-8447-he/himush.aspx×™×©×¨	Block	1
212.235.22.119	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.35.253.161	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
84.108.95.115	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
5.39.222.159	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/rom-0	Block	1
217.132.59.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/phpmyadmin	Block	1