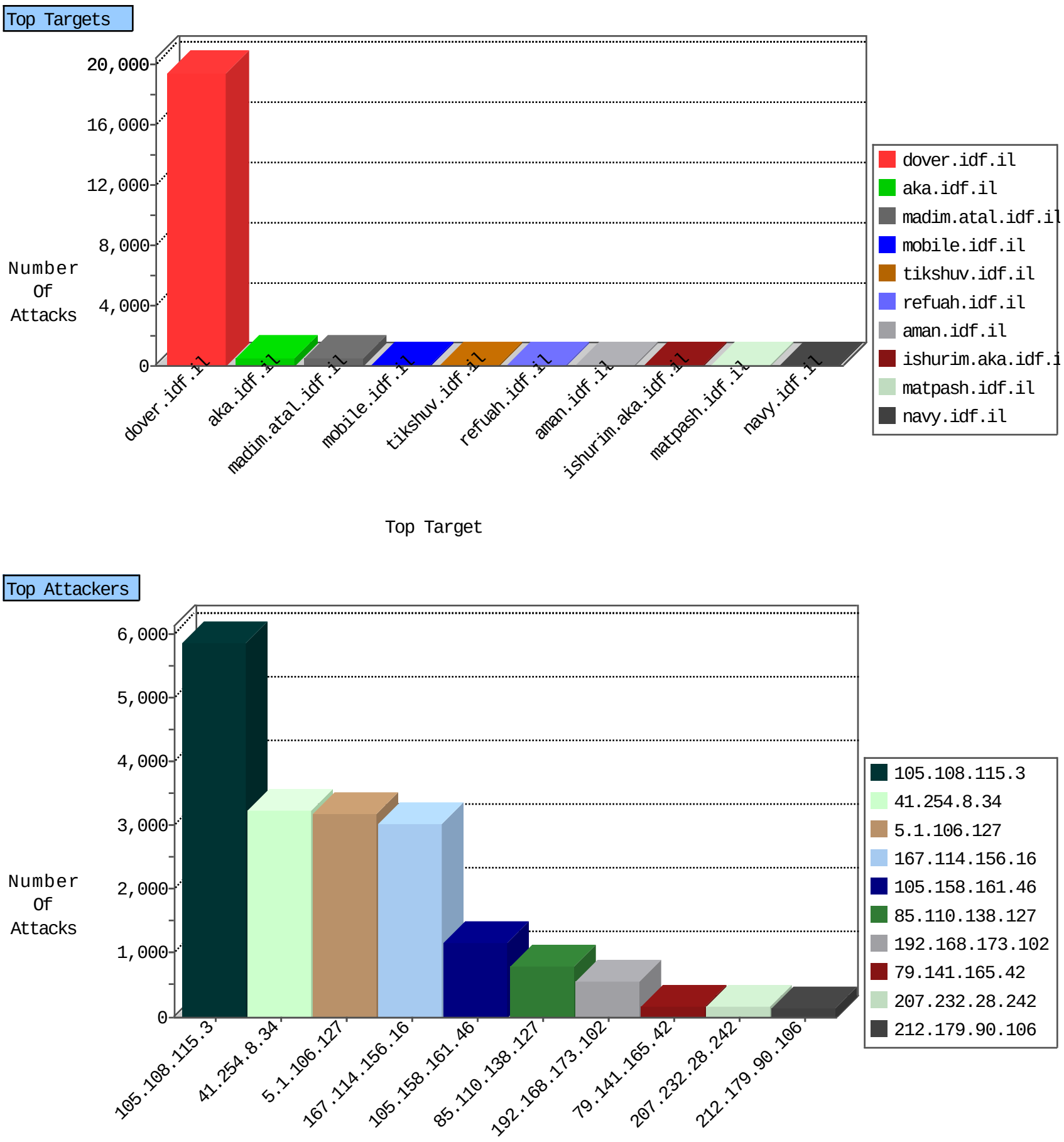
04-07-2016-14:04:00 to 04-07-2016-15:04:00

IDF Under Attack Daily Report



04-07-2016-14:04:00 to 04-07-2016-15:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.239.68.65	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5872
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3035
41.254.8.34	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	972
85.110.138.127	Turkey	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	811
108.61.208.140	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	181
79.141.165.42	Europe	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	173
185.120.125.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	94
79.179.149.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	86
105.158.161.46	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	17
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
105.158.161.46	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
81.96.83.130	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
105.108.115.3	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
92.114.41.197	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
176.13.8.13	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.253.209.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
94.249.90.145	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
5.102.233.101	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
37.239.68.61	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
62.90.167.46	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
37.239.68.65	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
37.239.68.65	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.46.38.69	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
37.239.68.61	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
109.253.195.28	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.176.42.132	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
46.20.222.201	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
177.92.60.81	Brazil	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
82.145.221.62	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
105.107.132.11	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
41.143.171.129	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
182.52.16.51	Thailand	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1

04-07-2016-14:04:00 to 04-07-2016-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.213.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.28.137.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.69.88.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.183.150.44	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.176.42.132	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
197.2.135.75	Tunisia	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.135.63.82	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.113	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-07-2016-14:04:00 to 04-07-2016-15:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.82.78.38	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.111	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
45.63.16.73	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 3072	1
212.76.97.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.44.118.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
92.114.41.197	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.219.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.79.172	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
66.102.9.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
31.168.75.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	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
151.237.79.36	147.237.77.234	Bulgaria	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.94.195.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-07-2016-14:04:00 to 04-07-2016-15:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.108.115.3	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5818
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3114
41.254.8.34	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2935
105.158.161.46	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1037
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	362
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	199
207.232.28.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	175
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
105.158.161.46	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	97
41.141.152.196	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	76
108.61.208.140	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
81.96.83.130	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.254.8.34	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	36
105.108.115.3	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
79.180.99.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
82.80.138.86	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
105.108.115.3	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
45.104.72.139	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
41.254.8.34	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
188.161.7.96	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
176.13.20.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
149.78.42.21	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.231.128.49	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
210.246.35.244	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.52.134.37	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
92.40.248.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
81.184.3.19	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.118.162.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
89.138.188.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
217.55.110.220	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.254.8.34	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
217.55.110.220	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.110.40.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.102.169.113	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
87.71.50.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.125.92.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

04-07-2016-14:04:00 to 04-07-2016-15:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.254.8.34	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.254.8.34	Block	224
109.253.202.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	132
2.52.164.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
2.53.38.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
213.151.35.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
2.53.3.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
46.19.85.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
5.1.106.127	Iraq	147.237.77.216	dover.idf.il	Multiple Post Request - Missing Content Type: 'none'	Block	19
176.13.21.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
79.176.42.132	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	9
80.74.116.135	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.216.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
81.1.147.105	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
81.218.46.131	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
81.1.147.105	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.1.147.105	Block	5
149.78.42.21	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.20.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.53.2.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
89.138.188.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.16.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.5.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.219.211.28	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.235.60.86	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.117.60.216	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.25.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
103.55.25.247	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/	Block	2
80.246.137.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
103.55.25.247	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 103.55.25.247	Block	2
62.128.48.126	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.150.178.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	2
103.55.25.247	Hong Kong	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
79.183.172.134	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
37.26.149.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.54	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 46.19.86.54 (Open Mode)	None	1
188.161.49.138	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
80.179.243.82	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
41.227.224.180	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
173.219.168.83	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/unit.aspx	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;DocID in www.aka.idf.il/giyus/leshakot/	None	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
5.28.190.122	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 5.28.190.122	Block	1
50.118.198.254	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1

04-07-2016-14:04:00 to 04-07-2016-15:04:00