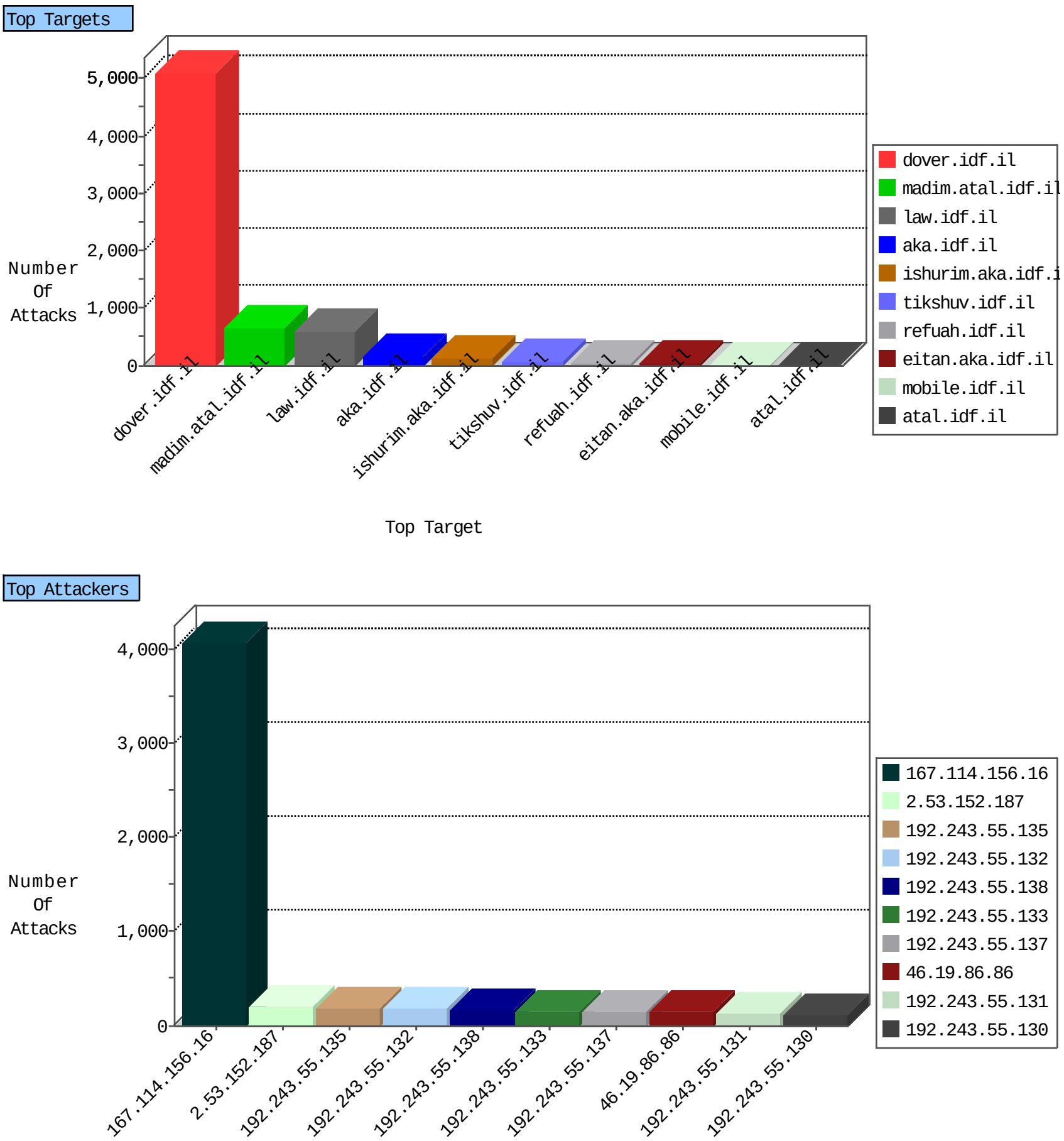
04-12-2016-13:04:07 to 04-12-2016-14:04:07

IDF Under Attack
Daily Report



04-12-2016-13:04:07 to 04-12-2016-14:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.105.118.160	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	5071
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4074
199.203.83.190	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1237
162.243.37.178	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	813
31.168.4.242	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	714
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	92
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	73
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26
46.19.85.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
192.243.55.133	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
192.243.55.134	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
192.243.55.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
192.243.55.138	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
195.160.242.40	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.117.158.34	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
213.151.58.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
5.28.190.107	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.42.253.130	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
66.240.219.146	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
194.90.134.251	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.130	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.81.81.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.211	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.3.144.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.139.47.142	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
41.105.118.160	Algeria	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
192.243.55.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
79.177.136.149	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.127	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
62.138.3.98	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
192.116.94.110	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.152	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-12-2016-13:04:07 to 04-12-2016-14:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.40.43	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
31.154.41.17	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
144.76.29.66	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
144.76.29.66	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.202	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
84.228.220.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.29.66	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.31.179	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.107	France	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.158	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-12-2016-13:04:07 to 04-12-2016-14:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.181.9.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.205.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.165.143.42	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
5.102.240.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.130	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.162.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.222.225.138	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
93.63.226.141	147.237.77.216	Italy	dover.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.76.147	Kazakstan	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
80.246.137.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.85.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.127	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
2.53.184.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.129	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.55.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.114.157.12	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 4096	1
122.3.135.145	147.237.8.28	Philippines	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.138.109.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.188.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-12-2016-13:04:07 to 04-12-2016-14:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.20.86	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
82.81.13.178	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	53
212.179.132.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
107.167.99.225	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
192.243.55.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
192.243.55.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
192.243.55.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.138	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
192.243.55.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	13
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13

04-12-2016-13:04:07 to 04-12-2016-14:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.152.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	212
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
89.139.172.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.13.21.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
176.13.17.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
79.180.105.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.149.218	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 37.26.149.218	Block	23
176.13.5.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
109.253.128.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
212.143.163.172	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.143.163.172	Block	15
80.178.28.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.13.16.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.178.28.129	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	7
192.243.55.132	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	4
46.19.86.211	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
212.143.163.172	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	3
37.26.146.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.6.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
147.236.232.36	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	3
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.148.131	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	2
199.30.25.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
141.212.122.161	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.67.180.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
52.10.45.138	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
192.243.55.129	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
82.81.193.82	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.152.187	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** **********	None	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
54.213.220.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
124.106.155.106	Philippines	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
94.230.93.143	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an...	Block	1
5.22.134.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
54.173.106.255	United States	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
192.243.55.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.111.20.108	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
77.72.150.241	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
176.13.7.212	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
54.229.110.44	Ireland	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to 147.237.76.39/	Block	1
94.230.93.146	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.211	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
192.243.55.138	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
5.28.183.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
178.23.141.106	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
157.55.39.120	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1

04-12-2016-13:04:07 to 04-12-2016-14:04:07