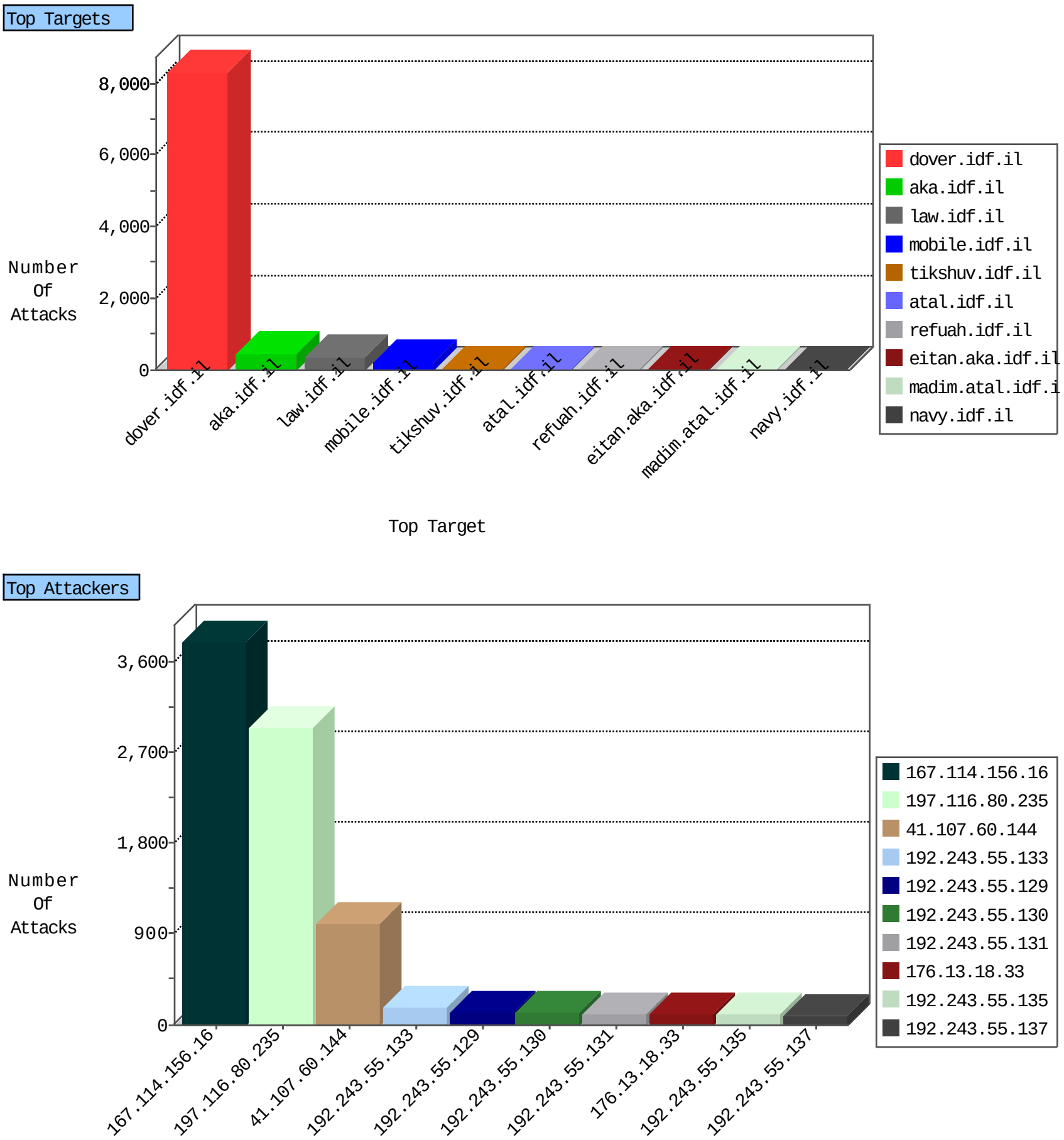
04-11-2016-22:04:06 to 04-11-2016-23:04:06

IDF Under Attack Daily Report



04-11-2016-22:04:06 to 04-11-2016-23:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	12136
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5173
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3794
83.130.99.162	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1917
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1153
109.67.111.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	994
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	703
74.206.99.126	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	677
46.117.43.97	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	644
185.3.144.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	432
37.26.147.216	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	283
77.125.160.127	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	149
192.243.55.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	126
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	69
2.54.135.236	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	48
79.182.144.51	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
192.243.55.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
89.217.14.202	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.85.243	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.111.191.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.3.146.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.173.248.138	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.246.137.107	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
173.252.74.99	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.68.12.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.133	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
109.64.26.201	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.166.73.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
89.138.214.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.179.54.35	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
41.111.97.43	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
205.203.135.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
76.9.96.138	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-11-2016-22:04:06 to 04-11-2016-23:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.54.35	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.182.173.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.67.111.179	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
61.135.189.99	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
5.8.45.2	Brazil	147.237.77.216	dover.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
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-11-2016-22:04:06 to 04-11-2016-23:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.8.45.2	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
163.172.140.23	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.115	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
108.61.19.5	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.115	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

04-11-2016-22:04:06 to 04-11-2016-23:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop		drop	264
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	240
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
176.13.18.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	78
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	65
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.52.168.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.4.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
5.102.195.144	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.130	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
84.229.28.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	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
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.130	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	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
79.176.104.8	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Anonymous DoSer Denial of Service Tool	reject	12
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.133	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.133	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
93.173.4.134	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
192.243.55.136	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.243	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.243	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.129	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
80.246.133.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.138	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.133	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.107.60.144	Block	170
192.243.55.130	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	10
192.243.55.135	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	6
46.19.85.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
192.243.55.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	5
95.35.74.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	4
192.243.55.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	4
217.65.199.87		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	3
199.30.24.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
5.22.131.41	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
157.55.2.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
217.65.199.84		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
192.243.55.129	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	3
199.30.25.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
192.243.55.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	3
109.253.139.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.103.64	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
109.253.196.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.243.55.129	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
109.65.21.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.125.80.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58438	Block	1
157.55.39.95	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
104.130.136.159	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59331&docid=64447	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
85.65.103.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.190	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
54.153.32.246	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
89.139.239.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1398-he/atal.aspx	Block	1
37.187.114.171	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /irj/portal	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
79.178.192.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17225-he/dover.asp	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/scriptresource.axd	Block	1
217.132.103.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.130.136.159	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
45.32.149.142	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	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
2.53.25.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteyerua	Block	1