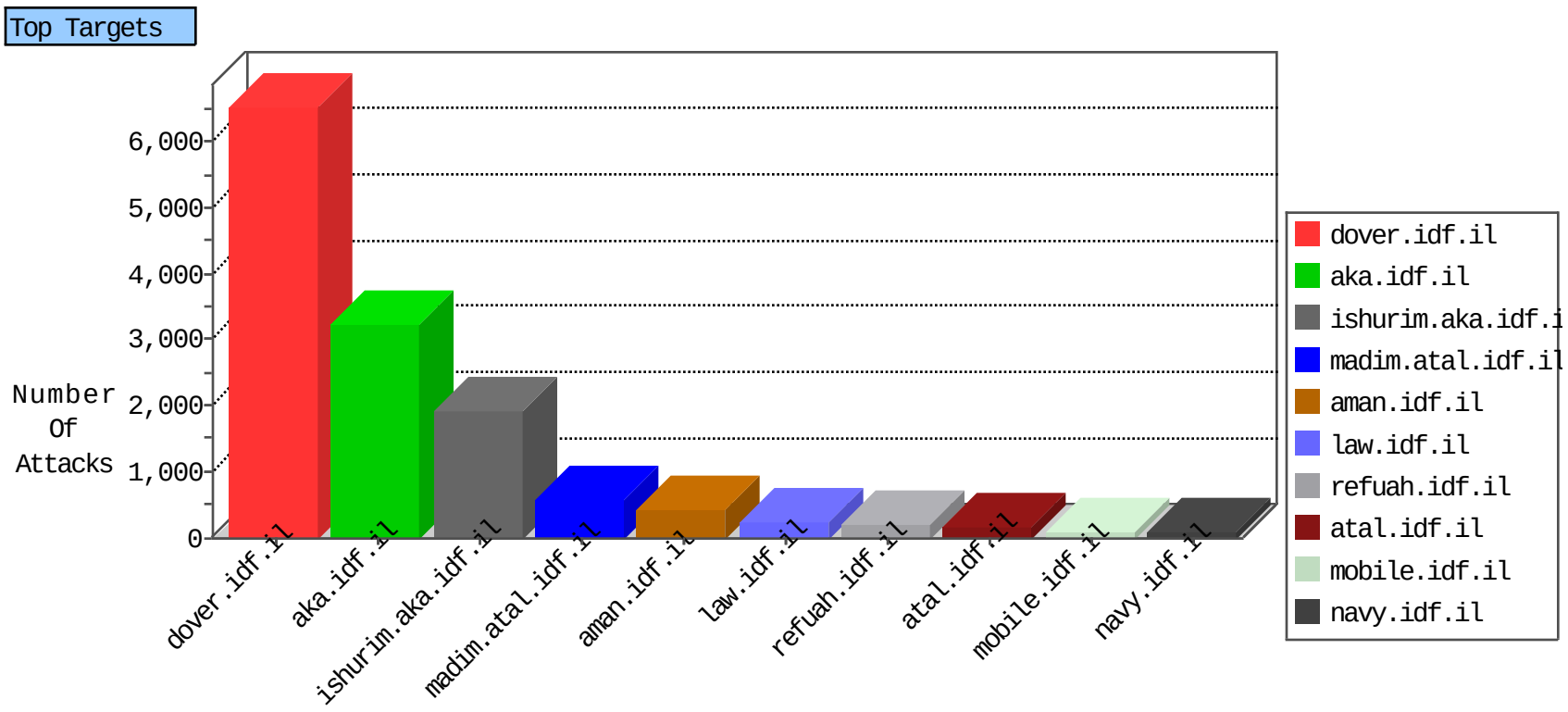
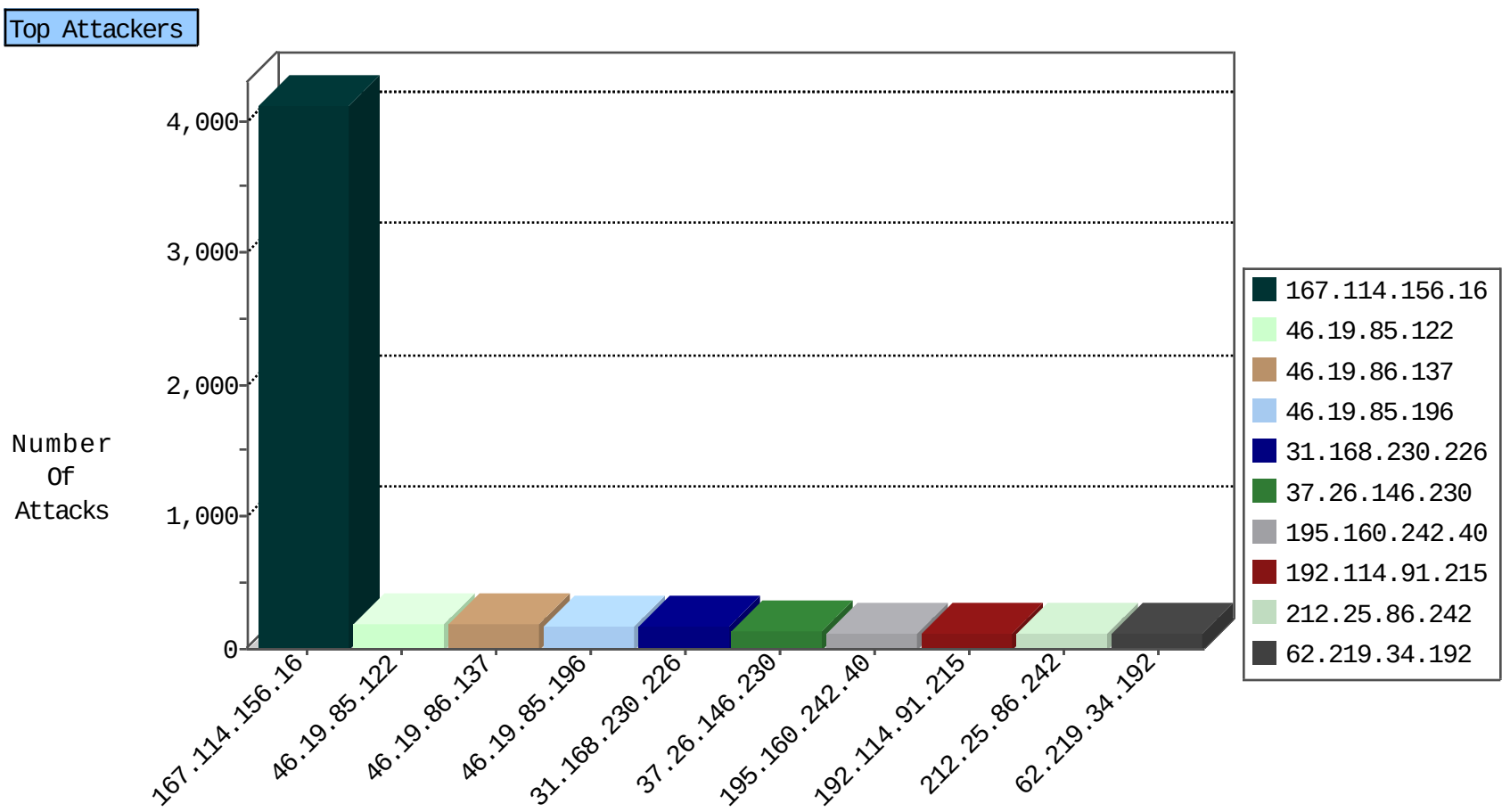
04-11-2016-13:04:01 to 04-11-2016-14:04:01

IDF Under Attack Daily Report





04-11-2016-13:04:01 to 04-11-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4114
207.232.27.5	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	120
176.13.17.27	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	99
192.249.66.247	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	89
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	53
31.168.194.95	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
62.0.244.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
141.0.14.146	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
212.179.73.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
79.182.148.141	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.179.73.146	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	2
46.120.236.141	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
82.166.198.205	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
2.55.26.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
193.43.246.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
109.65.193.86	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
192.243.55.134	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.144.50	Switzerland	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
2.53.7.152	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.168.24.162		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.31.60.249	France	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
109.65.1.31	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
212.179.46.16	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1

04-11-2016-13:04:01 to 04-11-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
46.19.86.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
109.253.156.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.146.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
80.179.243.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.146.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
132.74.145.226	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.190	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
194.105.250.18	Iceland	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.28.152.58	Poland	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-11-2016-13:04:01 to 04-11-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.146.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.194.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.54.0	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.70.84.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.1.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.145.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.123.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.134	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.39.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.20.72.19	147.237.76.201	Italy	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.19.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.131.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.20.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.11.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.102.169.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.226.192	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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.131	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.39.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.20.72.19	147.237.8.14	Italy	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

04-11-2016-13:04:01 to 04-11-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.122	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
31.168.230.226	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	82
37.26.146.230	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
31.168.230.226	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	75
31.168.26.98	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
212.25.86.242	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
141.0.14.146	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
192.114.91.215	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
37.26.148.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
80.74.100.131	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
62.219.34.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
80.74.100.131	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	49
79.183.13.66	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
5.22.135.221	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
192.55.54.40	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
62.219.167.243	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
79.182.11.51	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.85.122	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
176.13.17.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
5.29.0.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.86.33	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
5.29.0.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	36
46.19.85.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
5.29.0.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
46.19.86.120	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
2.55.42.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	32
62.219.34.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
2.55.42.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
37.26.146.230	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
185.27.105.119	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	28
168.235.206.48	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
37.26.147.143	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
5.22.135.221	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
192.114.91.215	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
168.235.206.48	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
157.55.39.234	United States	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
149.50.65.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	23
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
132.70.66.12	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
109.64.48.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23

04-11-2016-13:04:01 to 04-11-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	181
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
2.53.24.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
37.26.147.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.53.26.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
5.102.237.140	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.102.237.140	Block	34
185.32.179.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
195.93.234.9	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	5
62.90.77.127	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
195.93.234.9	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/	Block	3
109.253.205.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	2
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
195.93.234.9	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.93.234.9	Block	2
80.246.139.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.102.237.140	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/trans.not	Block	2
192.243.55.134	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	2
192.243.55.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
83.244.113.166	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
185.120.125.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1367-8722-he/atal.aspx	Block	1
217.69.133.246	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/glyus	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
40.77.167.21	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
199.203.8.2	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Malformed URL	Block	1
5.22.135.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/jius	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/giyus/kiosk/	None	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
176.13.5.193	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
212.199.224.24	Israel	147.237.76.147	chinuch.aka.idf.i	Unknown Parameter wb48617274 in www.chinuch.aka.idf.il/style/shared/text.css	None	1
194.105.250.18	Iceland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
79.180.49.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/resources/styles/showbigstyle.css	Block	1
217.69.133.247	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giy.com	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
46.19.85.31	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
209.88.196.250	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	1
109.253.209.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$comboQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59333&docid=68029	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
70.39.157.197	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.254.241.5	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

04-11-2016-13:04:01 to 04-11-2016-14:04:01