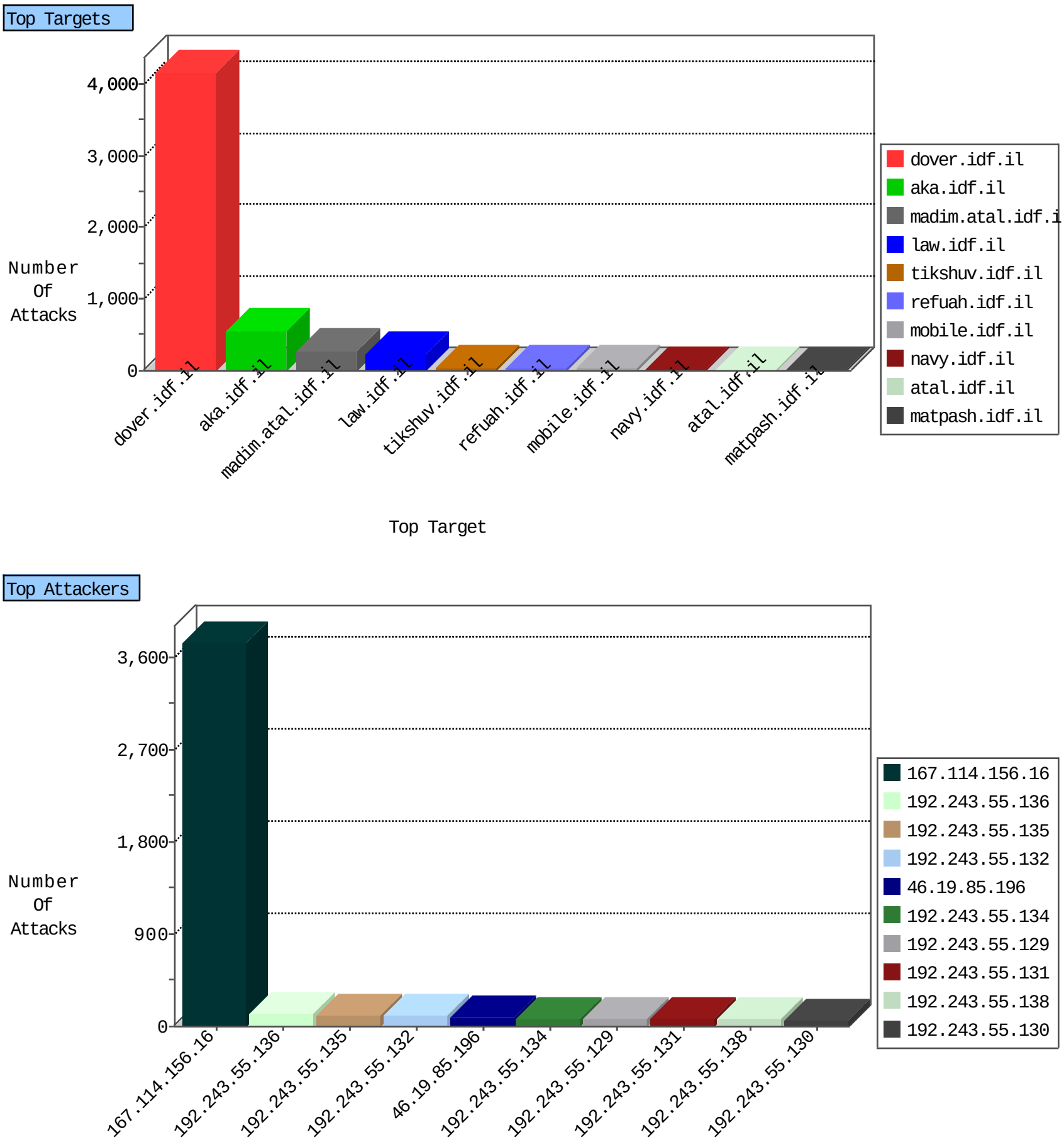
04-11-2016-14:04:02 to 04-11-2016-15:04:02

IDF Under Attack Daily Report



04-11-2016-14:04:02 to 04-11-2016-15:04:02

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	3739
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
213.57.212.74	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.228.156.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.106.92.47	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
123.59.59.52	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
5.100.248.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
124.232.150.230	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
202.88.1.10	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
179.43.141.194	Switzerland	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.13	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.50	Switzerland	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
152.178.71.13	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.50	Switzerland	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
62.138.2.122	Germany	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.50	Switzerland	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
202.88.1.3	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
179.43.141.194	Switzerland	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.9	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.50	Switzerland	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1

04-11-2016-14:04:02 to 04-11-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.132.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.229.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
185.106.92.47	Russian Federation	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
142.54.184.90	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
109.65.7.14	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.145.79	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
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.65.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
185.106.92.47	Russian Federation	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
23.254.153.202	United States	147.237.76.86	navy.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.77.176	matpash.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

04-11-2016-14:04:02 to 04-11-2016-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
195.216.176.244	147.237.77.234	Latvia	halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
192.243.55.136	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.129.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.23.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.19.0	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.131.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.182.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.3	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
87.71.22.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.214.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.0.15		kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
79.177.141.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.135	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
62.0.118.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.106.92.47	147.237.77.216	Russian Federation	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
46.19.86.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.203.2.233	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
5.229.199.111	147.237.77.176	Turkey	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.186.34.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.217.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.38.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.227.68.190	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.8.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-11-2016-14:04:02 to 04-11-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
82.166.221.34	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
192.243.55.136	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.134	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
217.194.205.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
192.243.55.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.132	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
212.179.21.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	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
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
109.65.7.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
37.26.147.218	Israel	147.237.76.31	nakchal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
147.236.34.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.136	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
151.80.138.19	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.114.91.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.2.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.136	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.179.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
85.250.22.245	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.137	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
82.81.34.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

04-11-2016-14:04:02 to 04-11-2016-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
2.53.11.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
176.13.12.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.52.166.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
192.243.55.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	7
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.243.55.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	5
192.243.55.134	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	5
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	4
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	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
192.243.55.132	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	4
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	4
192.243.55.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	4
192.243.55.130	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	4
192.243.55.135	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	3
37.26.148.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.146.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.221.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.135	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	3
46.116.160.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
2.53.11.74	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
176.13.14.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.130	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/general	Block	2
2.53.44.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.206.80	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	2
192.243.55.135	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/general	Block	2
109.186.190.138	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.186.190.138	Block	2
77.124.31.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
192.243.55.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
109.186.190.138	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
31.168.3.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/miluim/miluimnikpail/general.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
80.179.114.11	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
188.120.148.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
199.30.25.46	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
23.254.153.202	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/general	Block	1
89.138.106.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
66.249.73.245	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.	Block	1
2.25.118.198	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1393-en/dover.aspx	Block	1
46.120.47.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22449-he/	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Malformed URL	Block	1

04-11-2016-14:04:02 to 04-11-2016-15:04:02