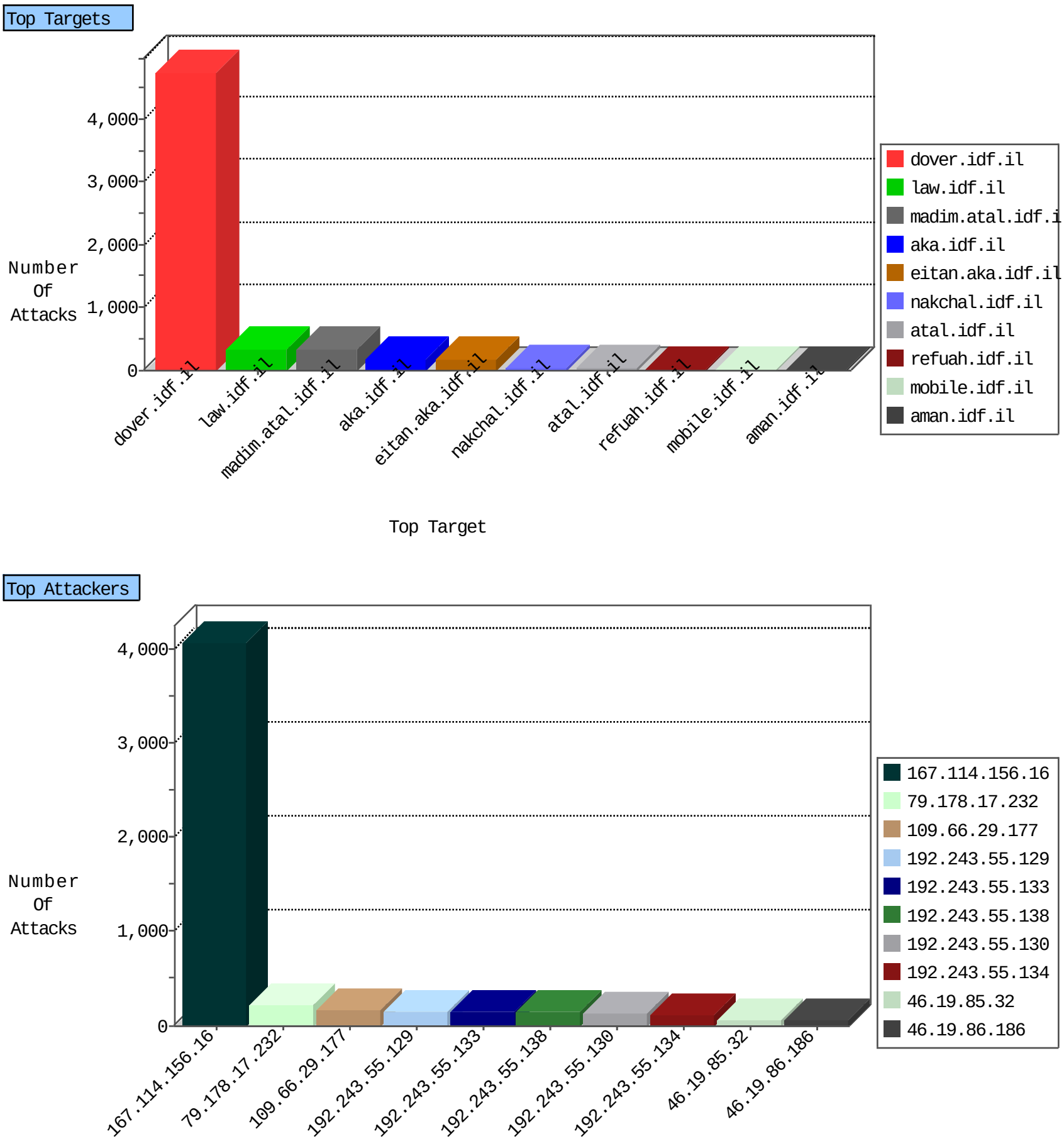
04-12-2016-18:04:01 to 04-12-2016-19:04:01

IDF Under Attack Daily Report



04-12-2016-18:04:01 to 04-12-2016-19:04:01

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	4071
37.38.138.254	Kuwait	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	387
46.19.85.32	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
46.117.69.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
212.117.136.8	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.85.189	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
217.132.142.9	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
82.145.222.91	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
46.117.34.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.165.214.165	Asia/Pacific Region	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.201.67.72	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
79.179.96.72	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.201.67.72	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
91.46.125.51	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.165.214.171	Asia/Pacific Region	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.201.67.72	Germany	147.237.0.19	madim.atal.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
93.201.67.72	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
192.165.214.172	Asia/Pacific Region	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
93.201.67.72	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
192.165.214.164	Asia/Pacific Region	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.201.67.72	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
63.141.247.218	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
192.165.214.172	Asia/Pacific Region	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
93.201.67.72	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1

04-12-2016-18:04:01 to 04-12-2016-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.248.252.113	Netherlands	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	3
77.248.252.113	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
5.9.63.149	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
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
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

04-12-2016-18:04:01 to 04-12-2016-19:04:01

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	4
88.204.187.90	147.237.76.30	Kazakstan	himush.idf.il	ET SCAN NMAP -sS window 3072	1
87.69.165.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.121	United States	e.navy.idf.il	ET DROP Dshield Block Listed Source	1
84.109.117.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.97.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
156.210.48.228	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.180.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.76.201	Turkey	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.103.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.84.148.3	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.77.179	Kazakstan	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
88.204.187.90	147.237.77.179	Kazakstan	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
87.70.82.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.109.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.255.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.8.14	Latvia	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.0.35	Israel	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
192.243.55.133	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.61.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.70.42.64	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.219.163.210	147.237.76.44	Israel	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.67.164.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.84.148.3	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
105.155.162.88	147.237.0.35	Morocco	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.29.93.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.77.179	Kazakstan	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1

04-12-2016-18:04:01 to 04-12-2016-19:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.29.177	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
109.65.24.162	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.32	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
192.243.55.129	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
192.243.55.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.138	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
192.243.55.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	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	16
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	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
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
46.19.85.32	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
192.243.55.133	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
109.253.204.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.18.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.17.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	217
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
37.26.149.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
174.47.33.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	3
80.246.133.186	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	3
149.50.34.198	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 149.50.34.198	Block	3
2.55.163.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.208	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
199.30.24.97	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.55.31.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authenticationservice.asmx/js	Block	1
213.8.204.16	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
46.19.85.25	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
2.53.21.104	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/newsservice.asmx/js	Block	1
192.243.55.133	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
149.50.34.198	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
79.177.188.156	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.66.163	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12715-he/dover.aspx	Block	1
213.8.204.32	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
46.19.85.25	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version __atuvc=1%7C13%2C0%7C14%2C1%7C15; __atuvs=570d1959cdaf5d9c000	Block	1
176.86.101.251	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/	Block	1
2.53.33.237	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9067-he/refuah.aspx	Block	1
37.26.147.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mavka	Block	1
79.177.188.156	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.66.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
213.254.241.4	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
185.82.68.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.25	Israel	147.237.76.42	refuah.idf.il	Malformed URL asp.net_sessionid=gnccxe55kxpjvu555heaic55;	Block	1
81.218.160.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14105505 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.75.76.165	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
199.30.25.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.153.33.233	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
157.55.39.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/authenticationservice.asmx/js	Block	1
185.120.126.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	1
46.19.85.25	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 1459093622.; in URL asp.net_sessionid=gnccxe55kxpjvu555heaic55	Block	1
109.65.24.162	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
213.8.44.133	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.102.9.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
40.77.167.40	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.133.75	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/styles/default	Block	1
192.243.55.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal	Block	1
46.19.85.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1