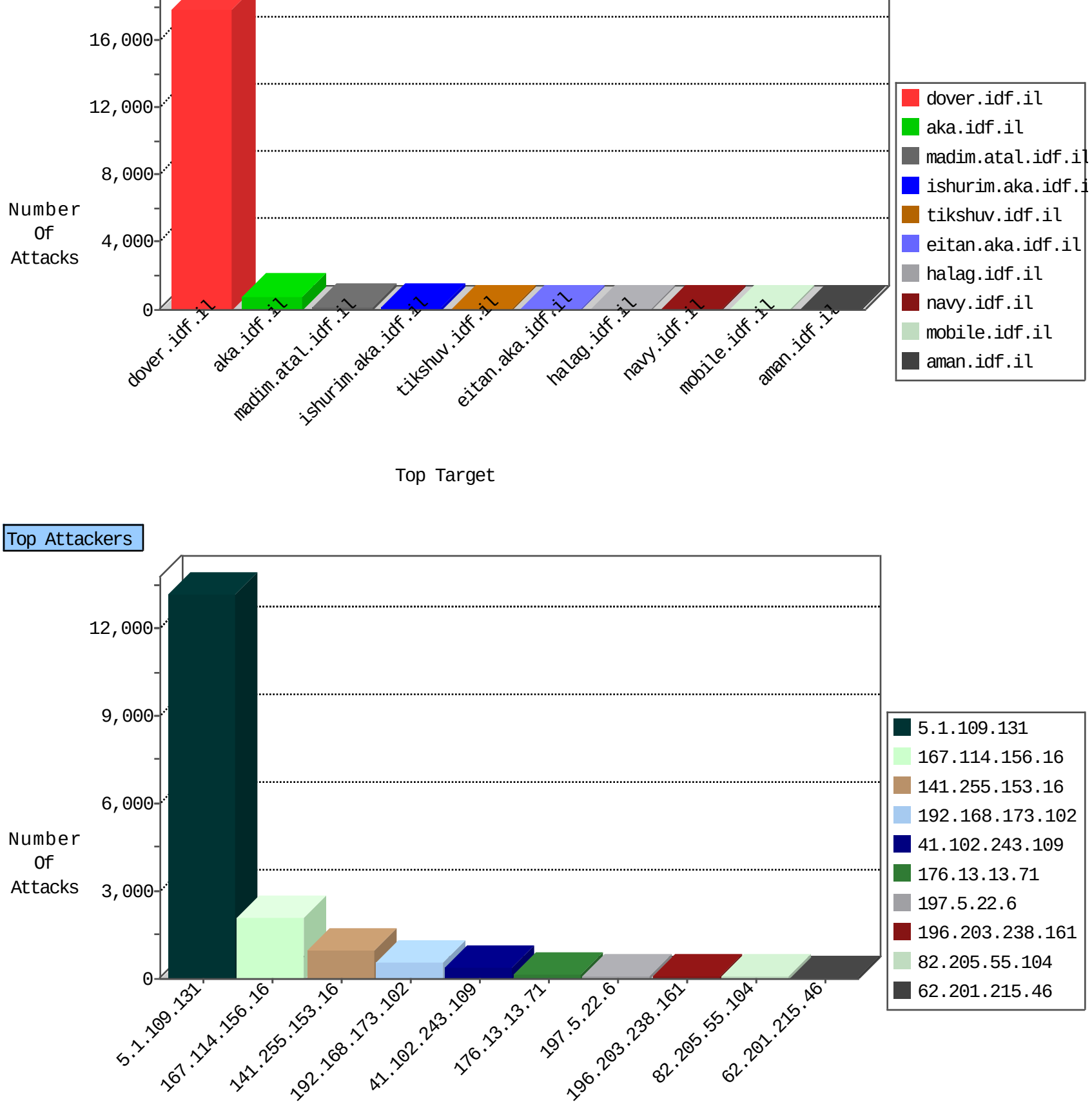
04-07-2016-19:04:07 to 04-07-2016-20:04:07

IDF Under Attack Daily Report



04-07-2016-19:04:07 to 04-07-2016-20:04:07

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	2120
141.255.153.16	Netherlands	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1988
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	230
62.201.215.46	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	43
41.102.172.135	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.205.55.104	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
70.39.187.165	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
82.205.55.104	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
41.102.172.135	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	3
41.102.172.135	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
41.102.172.135	Algeria	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
70.39.187.165	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
82.205.55.104	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
70.70.1.2	Canada	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	2
123.151.42.61	China	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
41.44.188.168	Egypt	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
52.53.222.9	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.70.184.164	Netherlands	147.237.8.45	e.eitan.idf.il	L4 Source or Dest Port Zero	drop	1

04-07-2016-19:04:07 to 04-07-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.130.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
149.78.150.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.109.24.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
77.125.129.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
64.31.44.6	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.246.49.97	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.143.34.37	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
196.203.238.161	Tunisia	147.237.77.216	dover.idf.il	C1000064: HTTP: Access to - admin.asp	Block	3
84.108.240.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
185.118.27.8	Lebanon	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	C1000064: HTTP: Access to - admin.asp	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
123.126.113.22	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
197.5.10.131	Tunisia	147.237.77.216	dover.idf.il	C1000064: HTTP: Access to - admin.asp	Block	1

04-07-2016-19:04:07 to 04-07-2016-20:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
63.143.34.37	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	8
213.246.49.97	147.237.77.74	France	law.idf.il	SQL Injection - Select From	6
64.31.44.6	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
196.203.238.161	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP admin.php access	3
196.203.238.161	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP login.htm access	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
61.241.82.125	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
61.241.82.125	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.241.82.125	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
45.63.7.151	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
104.44.133.108	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
45.63.7.151	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
104.44.133.108	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
84.200.15.174	147.237.77.205	Germany	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
202.67.237.220	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN Potential SSH Scan	1
70.39.187.165	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
61.241.82.125	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.241.82.125	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
149.78.110.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.241.82.125	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
45.63.7.151	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
104.44.133.108	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
85.90.246.134	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
197.5.10.131	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP login.htm access	1

04-07-2016-19:04:07 to 04-07-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	8027
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3787
141.255.153.16	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	896
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	524
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	341
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	250
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	213
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	205
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	152
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	122
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	115
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	88
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
176.13.22.54	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.219.131.163	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	27
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	24
82.205.55.104	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
82.205.55.104	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	21
89.139.157.65	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
82.205.55.104	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
70.39.187.165	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
185.120.126.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
109.65.195.52	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.157.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
80.178.150.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.108.147.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
12.129.255.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.61.219	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.13.71	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.200	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.177.88.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
149.78.4.59	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
41.252.82.51	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
213.8.204.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.65.26.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
70.70.1.2	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.49.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.46.41.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.111.155.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.222.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.16.210	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
149.78.4.59	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
149.78.4.59	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
196.203.238.161	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 196.203.238.161	Block	52
197.5.10.131	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.5.10.131	Block	32
188.120.148.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
196.203.238.161	Tunisia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	13
149.78.23.55	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.23.55	Block	13
176.13.2.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
196.203.238.161	Tunisia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	7
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
197.5.10.131	Tunisia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
176.13.7.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.115.190.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
89.138.241.84	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	3
5.28.183.47	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 5.28.183.47	Block	3
109.253.205.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.200	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.47	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucFaqControl$txtSearch in www.refua.atal.idf.il/1762-he/refuah.aspx	Block	2
109.67.139.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.148.253	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
119.74.233.23	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
82.205.55.104	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
207.46.13.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
59.97.236.67	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
153.129.11.252	Japan	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
41.102.243.109	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
5.22.129.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
105.111.96.153	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
46.19.86.98	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/935-4489-	Block	1
37.26.148.253	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 37.26.148.253	Block	1
87.71.21.224	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
212.34.12.113	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
59.97.236.67	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.113	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
41.252.82.51	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
5.28.183.47	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
213.57.205.222	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ israel export institute –	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
46.19.86.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
176.13.22.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
137.254.4.9	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
37.26.148.253	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
212.34.12.113	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version Build/KTU84P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.105 Mobile Safari/537.36	Block	1
62.128.35.132	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/faq/	Block	1
46.19.85.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
197.5.10.131	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/siteadmin/index.asp	Block	1
46.116.45.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1