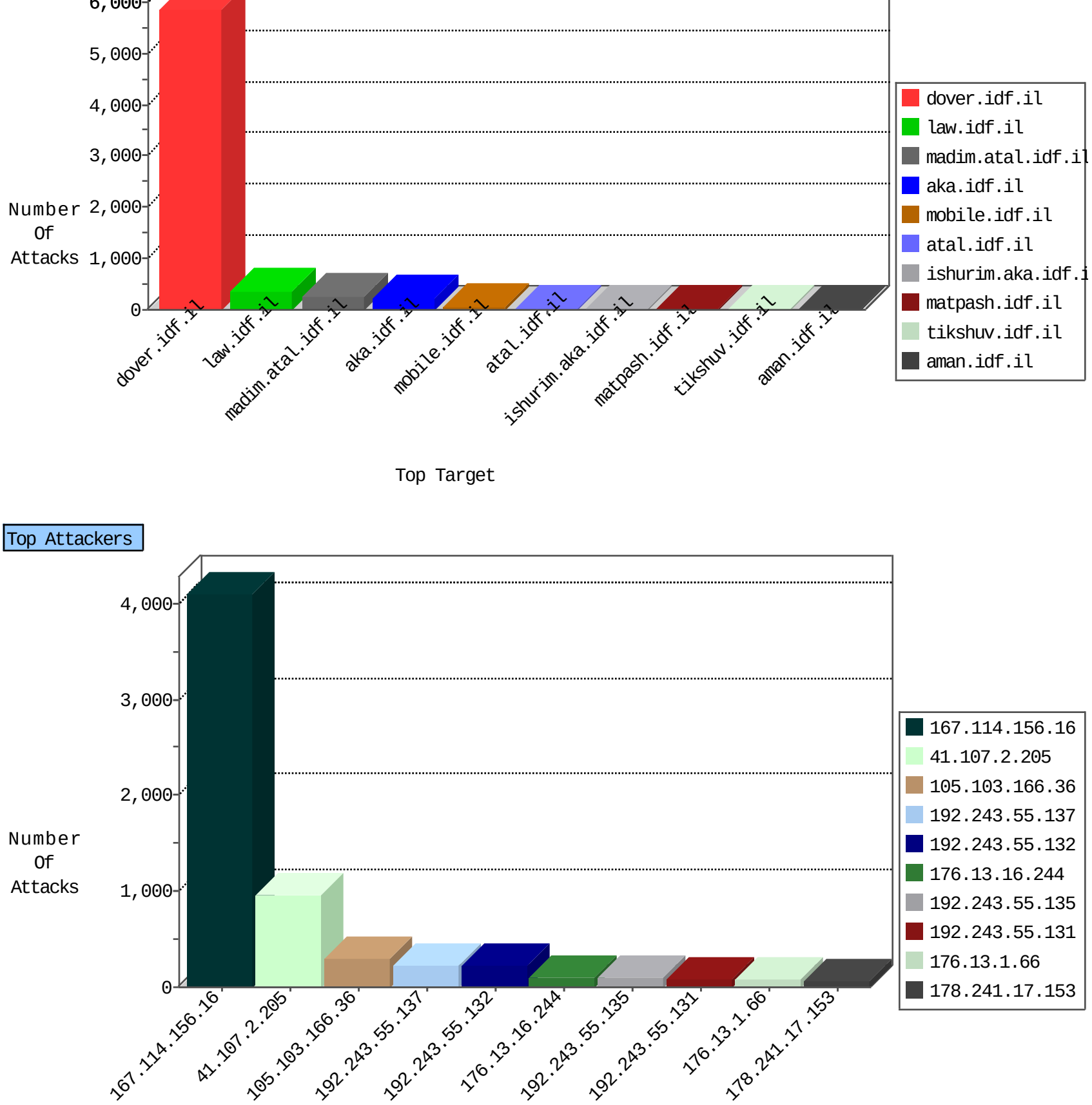
04-12-2016-20:04:04 to 04-12-2016-21:04:04

IDF Under Attack Daily Report



04-12-2016-20:04:04 to 04-12-2016-21:04:04

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	4097
41.107.2.205	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	970
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	621
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	179
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	103
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	61
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	35
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
85.76.32.118	Finland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
197.115.79.242	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
69.30.226.222	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
10.0.0.2		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
69.30.202.230	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.226.101	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
107.150.32.61	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
69.30.226.102	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
109.160.176.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
91.195.121.57	Ukraine	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1
124.105.57.58	Philippines	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
37.26.146.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.102.49.116	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
198.20.87.98	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
2.53.169.140	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1

04-12-2016-20:04:04 to 04-12-2016-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.124.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.94.67.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
213.251.184.38	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.148.247	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
80.246.133.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
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
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
91.121.101.78	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
157.55.39.215	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-12-2016-20:04:04 to 04-12-2016-21:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.215	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
176.13.4.137	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
61.94.23.143	147.237.77.216	Indonesia	dover.idf.il	Tehila - Perl LWP with fake user agent	2
176.13.4.137	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
203.197.205.118	147.237.76.176	India	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
79.182.26.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
203.197.205.118	147.237.76.176	India	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
50.193.61.77	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.57.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.172.147	147.237.76.196	Israel	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
175.184.203.44	147.237.77.234	Australia	halag.idf.il	ET SCAN NMAP -sS window 2048	1
31.168.172.147	147.237.8.24	Israel	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
175.143.36.222	147.237.0.35	Malaysia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.108.137.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.201	147.237.77.216	Israel	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
208.100.26.228	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.195.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.197.205.118	147.237.76.176	India	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
201.160.90.206	147.237.0.16	Mexico	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.120.27.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.218.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.172.147	147.237.76.200	Israel	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.172.147	147.237.76.34	Israel	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
175.184.203.44	147.237.77.234	Australia	halag.idf.il	ET SCAN NMAP -f -sS	1
5.102.228.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.103.166.36	147.237.77.216	Algeria	dover.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.76.30		himush.idf.il	ET SCAN NMAP -sS window 1024	1

04-12-2016-20:04:04 to 04-12-2016-21:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	60
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	39
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
2.53.8.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
105.103.166.36	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
192.243.55.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
84.111.130.135	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
192.243.55.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.135	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	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	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
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	12
176.13.15.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.135	United States	147.237.77.74	law.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	drop	First packet isn't SYN	drop	11
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	10
192.243.55.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
111.207.164.1	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.16.244	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.115.177.202	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.67.63.191	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	9
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
207.46.13.74	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	8
192.243.55.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.131	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8

04-12-2016-20:04:04 to 04-12-2016-21:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
176.13.1.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
79.183.39.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
108.66.123.100	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
37.26.149.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.18.29	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
118.193.175.5	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
46.19.85.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
5.28.181.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/resource/userfollowresource/create/	Block	1
77.127.163.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
193.138.219.234	Sweden	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/jpg/image.jpg	Block	1
61.94.23.143	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0 '	Block	1
128.232.110.28	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
37.142.64.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
104.131.21.195	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 104.131.21.195	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/scriptresource.axd	Block	1
46.19.85.176	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21744-ar/idfgdover.aspx	Block	1
109.65.106.134	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.39.222.159	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	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
207.46.13.43	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/giyus/[[#11]]general.aspx	Block	1
37.142.194.240	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
149.88.231.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
104.131.21.195	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
69.30.226.101	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
46.120.97.101	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
192.243.55.135	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
118.193.175.5	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 118.193.175.5	Block	1
207.46.13.43	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
40.77.167.37	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
107.150.32.61	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.ps780.com/	Block	1
69.30.226.102	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
192.243.55.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17060-en/dover.aspx>.	Block	1
54.153.33.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
31.210.176.141	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/צש|מ.דשביש׳ר	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/general.aspx	Block	1
2.53.31.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
108.40.60.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
69.30.226.222	United States	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1
193.138.219.234	Sweden	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/jpg/image.jpg	Block	1
61.94.23.143	Indonesia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 61.94.23.143	Block	1
118.193.175.5	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
85.250.115.136	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/webresource.axd	Block	1

04-12-2016-20:04:04 to 04-12-2016-21:04:04