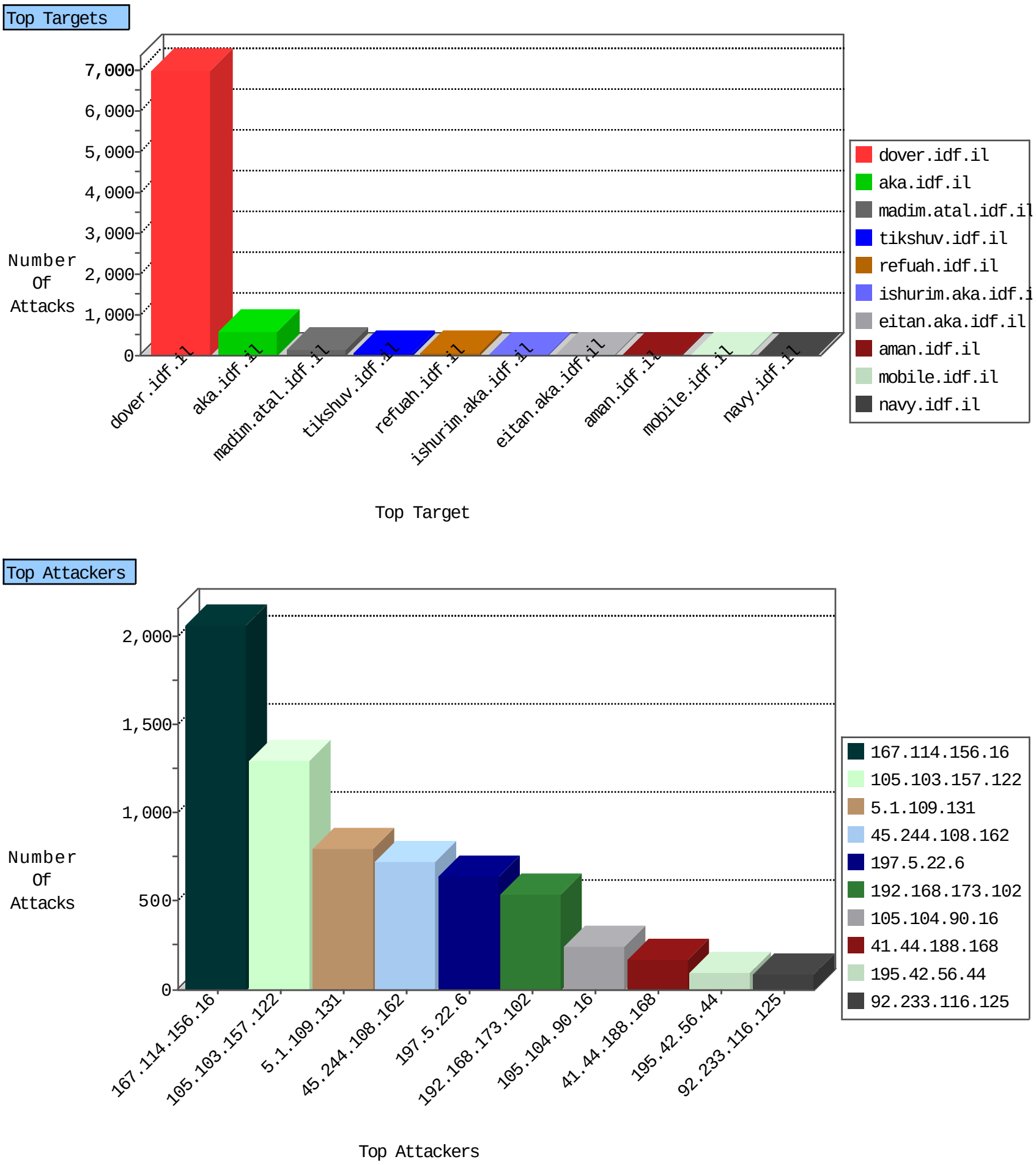
04-07-2016-18:04:07 to 04-07-2016-19:04:07

IDF Under Attack Daily Report



04-07-2016-18:04:07 to 04-07-2016-19:04:07

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	2065
105.103.157.122	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	1827
45.244.108.162	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	307
188.247.77.96	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	40
123.59.59.52	China	147.237.72.166	aka.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
41.44.188.168	Egypt	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
197.0.29.147	Tunisia	147.237.72.166	aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.103.252.96	Russian Federation	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
41.44.188.168	Egypt	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
37.8.119.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1

04-07-2016-18:04:07 to 04-07-2016-19:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.44.188.168	Egypt	147.237.77.216	dover.idf.il	20034: HTTP: HOIC Denial-of-Service Tool Usage	Block	92
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	16
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	C1000064: HTTP: Access to - admin.asp	Block	13
84.108.240.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
105.104.90.16	Algeria	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	9
213.8.204.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.64.202.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.109.232.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.130.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.56.110.176	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
80.246.133.32	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
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-07-2016-18:04:07 to 04-07-2016-19:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
197.5.22.6	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP login.htm access	19
197.5.22.6	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP adminlogin access	14
105.104.90.16	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP admin.php access	6
105.104.90.16	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP login.htm access	5
173.255.233.124	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
197.5.22.6	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP admin.php access	4
105.104.90.16	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP adminlogin access	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
176.13.2.107	147.237.0.19	Israel	madim.atal.idf.il	INDICATOR-SCAN myscan	2
173.255.233.124	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP TRACE attempt	2
132.66.231.124	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
176.13.2.107	147.237.0.19	Israel	madim.atal.idf.il	GPL SCAN myscan	2
173.255.233.124	147.237.77.216	United States	dover.idf.il	GPL WEB_SERVER TRACE attempt	2
197.0.29.147	147.237.72.14	Tunisia	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
197.0.29.147	147.237.72.14	Tunisia	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
80.246.137.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.248.129.181	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
216.227.58.7	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.85.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.227.58.7	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
2.53.30.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
166.62.85.153	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
197.0.29.147	147.237.72.166	Tunisia	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.37.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.0.29.147	147.237.72.156	Tunisia	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.0.29.147	147.237.72.14	Tunisia	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
80.246.138.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
59.184.158.84	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
216.227.58.7	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.148.3	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
168.235.207.154	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
166.62.85.153	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
119.93.197.195	147.237.76.42	Philippines	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
197.0.29.147	147.237.72.166	Tunisia	aka.idf.il	ET SCAN Potential SSH Scan	1

04-07-2016-18:04:07 to 04-07-2016-19:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
45.244.108.162	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	491
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	436
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	345
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	191
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	184
45.244.108.162	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	112
105.103.157.122	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	drop		drop	94
195.42.56.44	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
92.233.116.125	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	84
105.104.90.16	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	56
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	53
195.233.26.84	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
41.44.188.168	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	52
105.103.157.122	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
107.167.98.187	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
188.247.77.96	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	drop		drop	26
46.19.85.106	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
77.126.221.161	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
83.244.49.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
195.233.26.87	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.44.188.168	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.66.18.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
109.66.18.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
109.66.18.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
185.120.126.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.180	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.61	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
196.217.19.95	Morocco	147.237.77.216	dover.idf.il	drop		drop	8
109.134.175.191	Belgium	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
77.126.221.161	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.152.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
83.244.49.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.183.217.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.148.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.39.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.124.23.125	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
105.106.68.140	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
5.28.185.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.161.66.218	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.182.242.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	190
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.5.22.6	Block	174
105.104.90.16	Algeria	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	63
105.104.90.16	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.104.90.16	Block	61
85.64.115.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
197.5.22.6	Tunisia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	51
105.104.90.16	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	43
176.13.2.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
2.53.35.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
79.180.216.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
65.55.210.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
173.255.233.124	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 173.255.233.124	Block	3
46.120.142.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.169.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	3
173.255.233.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
157.55.39.161	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.161	Block	2
84.111.114.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.57.74.85	Kazakstan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1561-en/dover.aspx'	Block	2
5.29.162.249	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	2
149.88.209.87	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
2.55.0.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.140.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
2.53.30.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.55.45.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.140.123	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.50	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
123.59.59.52	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.ctrip.com/main/home/default.aspx	Block	1
46.19.85.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
101.226.33.204	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.130.44.115	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
177.206.121.89	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.181.169.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.169.113	Block	1
66.220.155.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.1.109.131	Iraq	147.237.77.216	dover.idf.il	NULL Character in Parameter Name /e[[#0]] in www.idf.il/ar	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
136.0.99.47	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.131.147.112	Block	1
2.53.39.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.179.28.34	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
157.55.39.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
2.52.169.26	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.52.169.26 (Open Mode)	None	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;DocID in www.aka.idf.il/giyus/leshakot/	None	1
173.255.233.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/404testpage4525d2fdc	Block	1
46.121.158.157	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
213.57.145.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
2.54.160.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
188.247.77.96	Jordan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on /	Block	1
80.246.140.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1