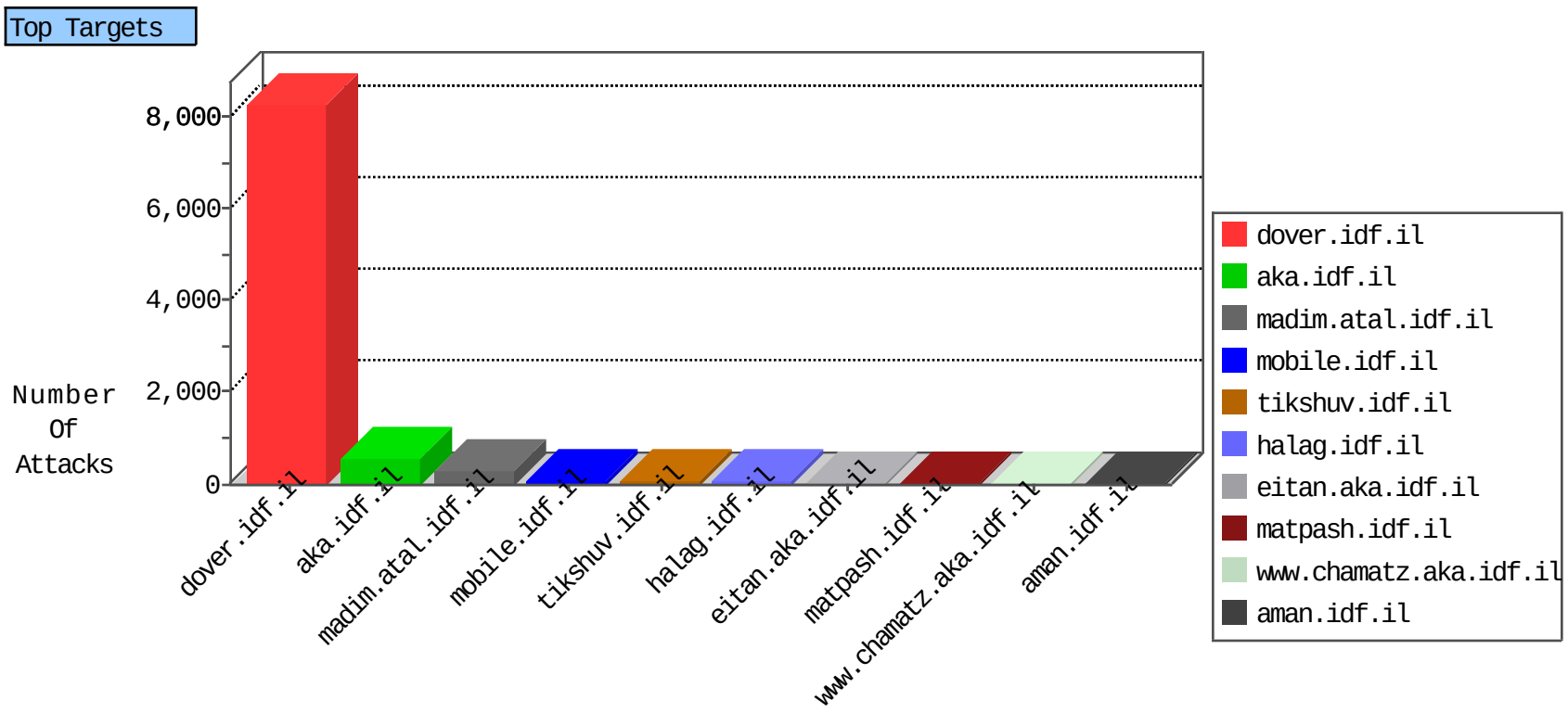
03-01-2016-11:04:09 to 03-01-2016-12:04:09

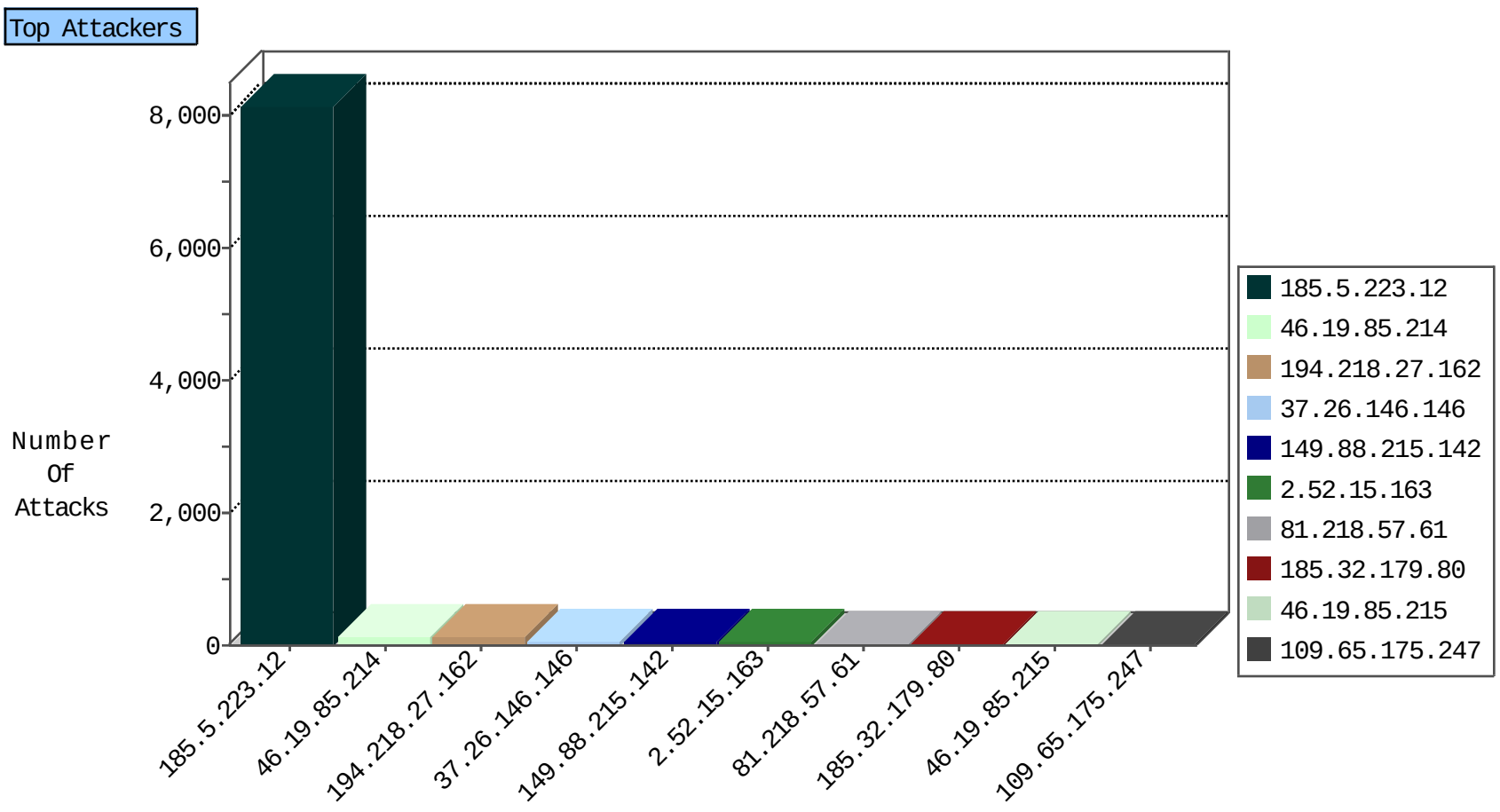
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-01-2016-11:04:09 to 03-01-2016-12:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	7805
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3563
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	255
209.126.122.20	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	5
209.126.122.20	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	4
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	2
89.248.172.207	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.235	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
41.178.246.157	Egypt	147.237.77.216	dover.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	1
185.94.111.1		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
1.34.18.227	Taiwan	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.110	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
1.34.18.227	Taiwan	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
209.126.122.20	United States	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.219	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
1.34.18.227	Taiwan	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1

03-01-2016-11:04:09 to 03-01-2016-12:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.193.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
79.176.30.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.64.125.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
173.234.153.122	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
5.102.220.231	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
69.30.215.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
81.218.151.130	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
213.57.218.226	Israel	147.237.76.86	navy.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

03-01-2016-11:04:09 to 03-01-2016-12:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.184	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	26
37.26.147.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.155.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.51.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.108.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.182.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.65.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.190.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.106.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.190.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.41.29.238	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 2048	1
188.120.148.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.117.149.78	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.74	Russian Federation	law.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.172.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.120.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.28.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.87.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.193.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.135.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.235.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.101.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
41.41.29.238	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -f -sS	1
183.3.202.115	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1

03-01-2016-11:04:09 to 03-01-2016-12:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1315
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	78
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	43
149.88.215.142	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
81.218.57.61	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
109.65.175.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.229.65.183	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	13
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack		reject	12
85.130.240.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.163.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.117.250.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.71.54.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.123.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.200.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.206.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
85.65.24.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.159.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.235.113.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.137.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.13.78	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.211	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.143.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.183.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.24.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
82.80.61.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.13	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
94.230.86.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.109.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.148	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
2.52.182.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.181.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.130.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-01-2016-11:04:09 to 03-01-2016-12:04:09

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.52.130.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.113.125.11	Romania	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
2.54.130.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.163.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
37.26.146.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.52.15.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
185.32.179.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.23.38	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter RepeatPassword	Block	8
176.13.9.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
149.88.63.114	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	4
37.26.147.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.26.146.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.197.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.52.32.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.13.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.163.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
109.253.200.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.52.14.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.178.157.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.199.57	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.199.57	Block	3
87.68.255.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.23.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
176.13.18.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.140.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.162.212	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	2
176.13.1.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.56.12.108	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.221.59.27	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.140	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
54.213.103.226	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ajax/updatestatus.php	Block	1
2.54.156.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.86.116.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in www.aka.idf.il/main/haredim/maslulimlist.aspx	None	1
46.19.86.206	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
73.181.130.85	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.203.214.2	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
109.253.131.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.66.96	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;popid in www.aka.idf.il/lomdim/tochen/	None	1
54.152.253.154	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
185.32.179.230	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.143.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
93.113.125.11	Romania	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
109.253.199.57	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
54.229.27.70	Ireland	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1