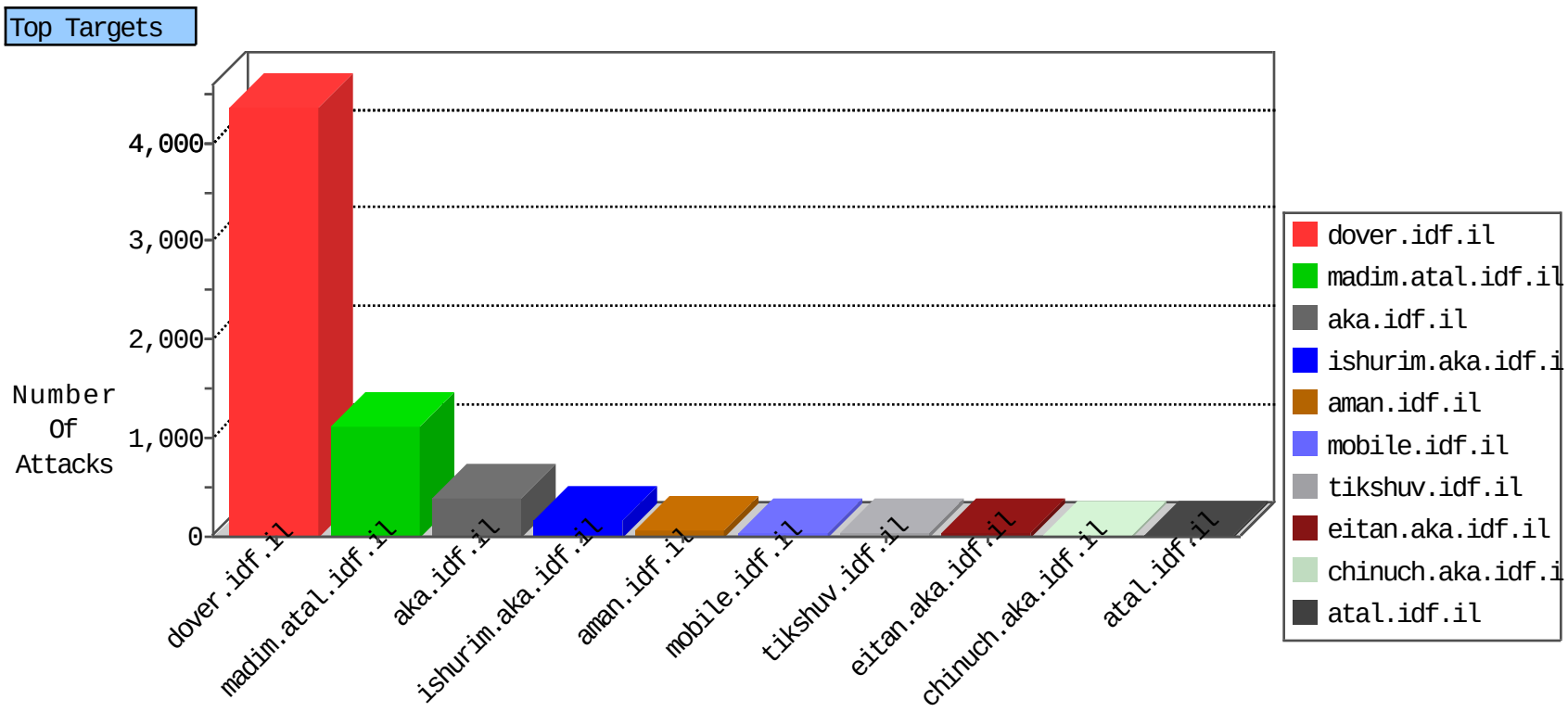
04-10-2016-11:04:02 to 04-10-2016-12:04:02

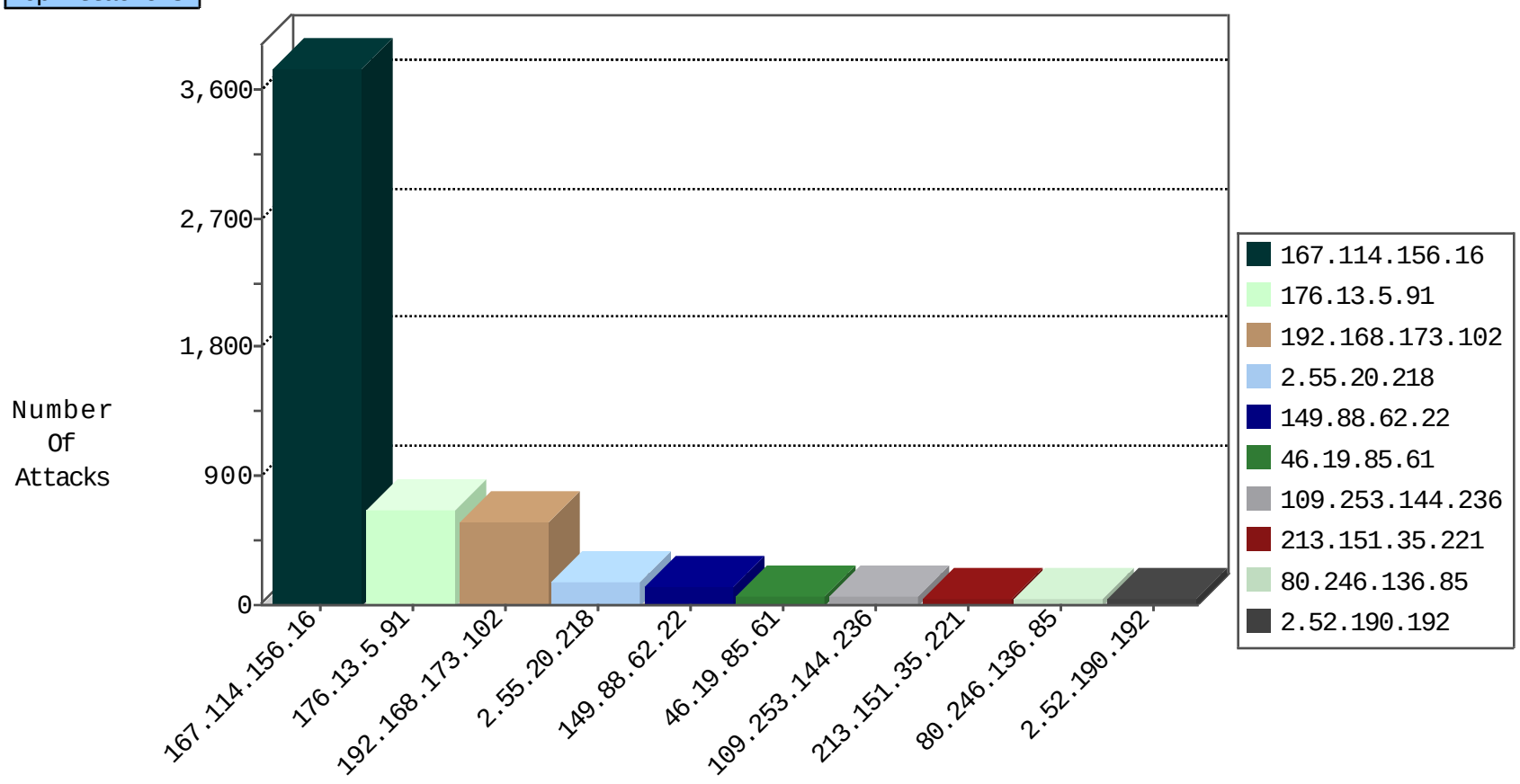
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-10-2016-11:04:02 to 04-10-2016-12:04:02

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	3760
80.246.137.177	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
123.59.59.52	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	4
109.64.204.115	Israel	147.237.72.166	aka.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
69.197.185.22	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	3
69.30.202.228	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
69.197.185.21	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
69.30.202.226	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
74.91.18.46	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
69.30.226.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
204.12.196.238	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
69.30.202.227	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2
74.91.20.194	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
69.30.226.102	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
69.30.198.146	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2
107.150.46.36	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
74.91.18.42	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
69.30.202.227	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
74.91.20.195	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
69.197.185.18	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
69.30.198.149	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
74.91.18.45	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	1
62.219.35.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.81	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
141.255.165.194	Switzerland	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.85	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
8.29.130.117	United States	147.237.77.74	law.idf.il	Invalid L4 Header Length	drop	1

04-10-2016-11:04:02 to 04-10-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.229.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	6
2.54.144.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.52.130.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
198.204.230.114	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	3
2.53.23.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.55.16.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
80.246.133.6	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
87.71.1.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.101	Israel	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
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
66.249.93.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-10-2016-11:04:02 to 04-10-2016-12:04:02

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	2
194.90.25.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.144.178.145	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.159.168.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.201.193.141	147.237.72.166	Bulgaria	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
213.151.53.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.91.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.118.30.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.45.110.218	147.237.77.216	Belarus	dover.idf.il	portscan: TCP Distributed Portscan	1
122.144.178.145	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
95.86.116.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.228.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.193.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.157.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.233.172.163	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

04-10-2016-11:04:02 to 04-10-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	374
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	209
149.88.62.22	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
213.151.35.221	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	43
192.114.163.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
2.54.155.61	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.220	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
109.67.80.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	10
62.90.161.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.54	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
217.194.203.52	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
217.194.203.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.150.37.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.52.162.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.53.48.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
185.106.92.47	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	6
89.138.119.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.46.16	Israel	147.237.76.197	e.himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.209.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.6.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
141.0.15.50	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
106.38.241.149	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.144.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
95.86.124.44	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.70.96.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.60.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.178.162.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.132.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.13.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.28.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.20.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.91.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.160.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.53.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.60.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.191.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-10-2016-11:04:02 to 04-10-2016-12:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.26.146.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.157.183	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.154	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	660
2.55.20.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
109.253.144.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.52.190.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
109.253.199.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
95.35.70.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
194.90.66.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	10
2.55.20.218	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	5
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	5
132.70.66.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	3
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.55.21.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.141.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.248	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
2.53.8.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.178.166.241	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	2
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.178.166.241	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/72288-he/	Block	2
2.54.182.153	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
2.55.28.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.207	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.250	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
74.91.20.195	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
69.30.202.228	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1
123.59.59.52	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.ctrip.com/894-he/dover.aspx	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/4/954.pdf	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
94.230.93.169	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	1
176.13.17.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
54.153.33.145	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
188.247.18.25	Syrian Arab Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.247.18.25	Block	1
94.230.93.131	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.250	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
69.30.226.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
94.230.93.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.183	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.228.43.89	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
74.91.18.45	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
2.54.155.61	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
69.30.198.149	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on www.app-softwares.com/	Block	1