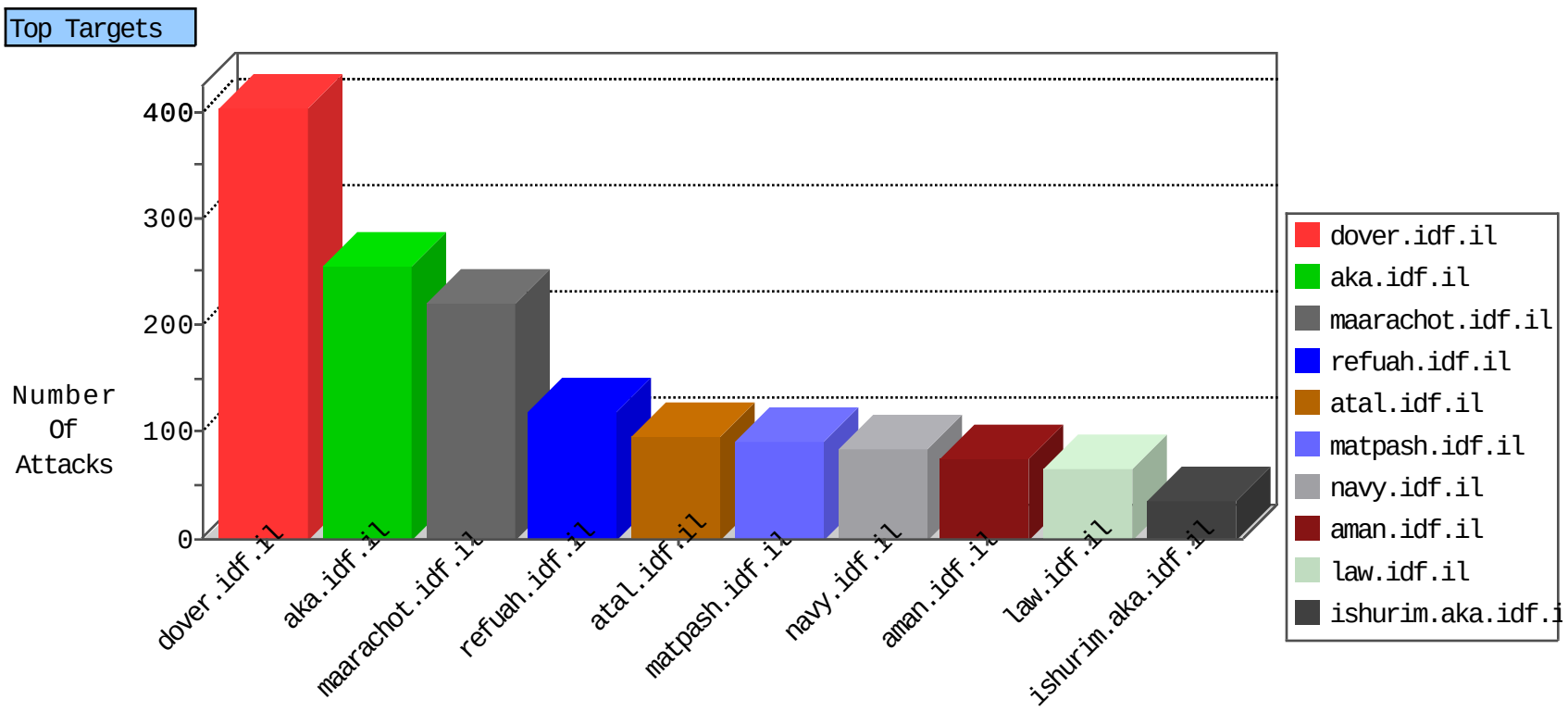
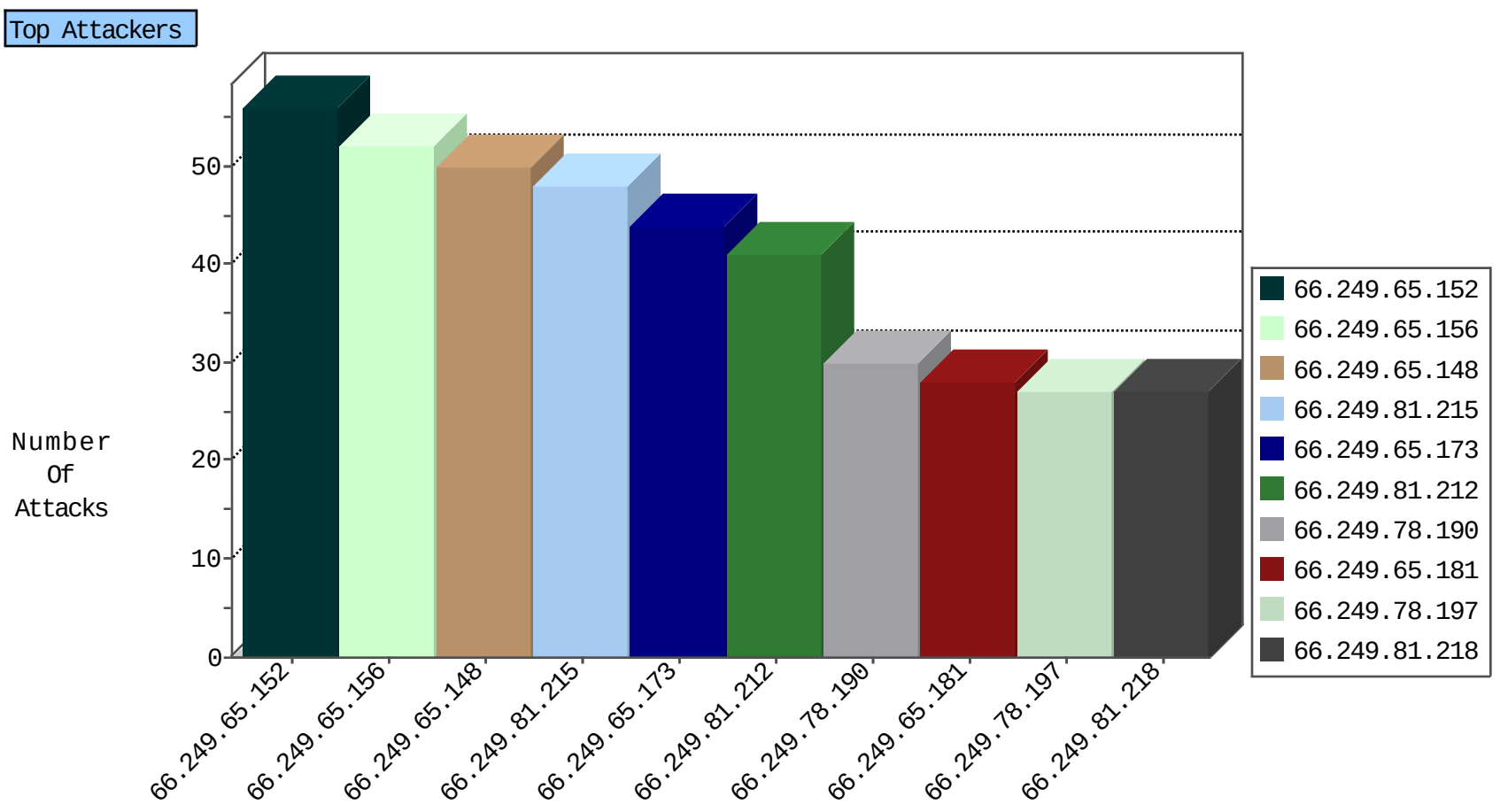
04-05-2015-12:03:04 to 04-05-2015-13:03:04

IDF Under Attack
04-05-2015-12:03:04

Top Targets



Top Attackers



04-05-2015-12:03:04 to 04-05-2015-13:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
85.64.195.229	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
87.69.119.83	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	56
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	50
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	50
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	48
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	44
66.249.81.212	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	41
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	30
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	28
66.249.81.218	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	27
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	26
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	25
66.249.93.203	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	22
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.93.207	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.93.213	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	18
66.249.79.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	18
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	17
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	17
82.102.141.254	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	17
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.75.39	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	10
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.90.82	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	9
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.81.144	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.213	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.134	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	7
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.65.169	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.92.57	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6

04-05-2015-12:03:04 to 04-05-2015-13:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
46.19.85.204	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.199.108.206	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
84.228.30.36	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
2.52.176.255	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
93.172.29.127	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
109.65.105.102	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-05-2015-12:03:04 to 04-05-2015-13:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
84.94.125.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.189.179	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
101.226.179.84	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
140.119.80.110	Taiwan	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 2048	1
140.119.80.110	Taiwan	147.237.77.216	dover.idf.il	ET SCAN NMAP -f -sS	1
104.207.149.204		147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
89.248.162.228	Netherlands	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.121.45	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.130	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
183.136.216.7	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
140.119.80.110	Taiwan	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1

04-05-2015-12:03:04 to 04-05-2015-13:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	26
109.253.128.111	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
84.228.30.36	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	23
197.134.49.156	Egypt	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	11
5.102.254.154	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
80.179.114.27	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
31.168.227.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
176.12.142.110	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.86.215	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
93.172.29.127	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
77.127.188.193	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
80.179.114.27	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	7
37.247.36.78	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	6
80.246.133.127	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.137.222	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
212.199.251.227	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	6
84.108.136.164	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
109.253.149.57	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
84.108.136.164	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
80.246.133.92	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
212.179.46.22	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
212.199.251.227	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
80.246.133.92	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
2.54.172.170	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
2.54.172.170	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.54.172.170	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
5.102.254.184	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
80.178.138.115	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
85.64.212.69	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	3
216.99.158.78	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	3
2.54.145.156	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
82.102.141.254	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
193.43.246.250	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
109.253.135.158	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
81.218.33.77	Israel	147.237.72.167	ishurim.aka.idf.i	SAM rule	drop	drop	2
80.179.114.27	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.54.145.156	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
46.19.86.159	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.86.57	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
217.69.133.222	Russian Federation	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
82.102.141.254	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
188.120.148.212	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.116.152.154	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
80.246.141.48	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.145.156	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
82.102.141.254	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.116.152.154	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
58.52.134.13	China	147.237.0.33	idf.il		drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.65.154.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	15
80.178.157.40	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.178.157.40	Block	5
188.247.93.236	Jordan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//894-ar	Block	3
80.178.157.40	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1750	Block	3
93.172.172.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.120.158.23	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.158.23	Block	3
5.102.254.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
77.127.130.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.21.148	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
23.254.129.17	United States	147.237.0.34	tikshuv.idf.i	Suspicious Response Code	Block	2
79.177.57.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.67.157.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
216.99.158.78	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 216.99.158.78	Block	2
80.178.168.48	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
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	2
188.165.15.238	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9169-he/refuah.aspx	Block	1
109.253.139.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.7.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
89.138.10.247	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
84.94.175.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Malformed URL from 202.112.50.77	Block	1
79.177.50.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.118.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.158.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/neworpi/lobby.aspx	Block	1
216.99.158.78	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
85.250.45.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
77.127.130.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.159.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.138.10.247	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/default.aspx	None	1
46.19.85.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.228.30.36	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
2.54.63.118	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 202.112.50.77	Block	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-	Block	1
46.120.229.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
23.254.129.17	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
85.250.61.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
77.127.188.193	Israel	147.237.72.156	aman.idf.il	Multiple Too Many Cookies in a Request from 77.127.188.193	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
93.172.29.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.86.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
85.64.42.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.28.168.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTTARGET in www.aka.idf.il/main/sachar/	None	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1
176.12.145.244	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
79.178.53.118	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
109.67.188.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1