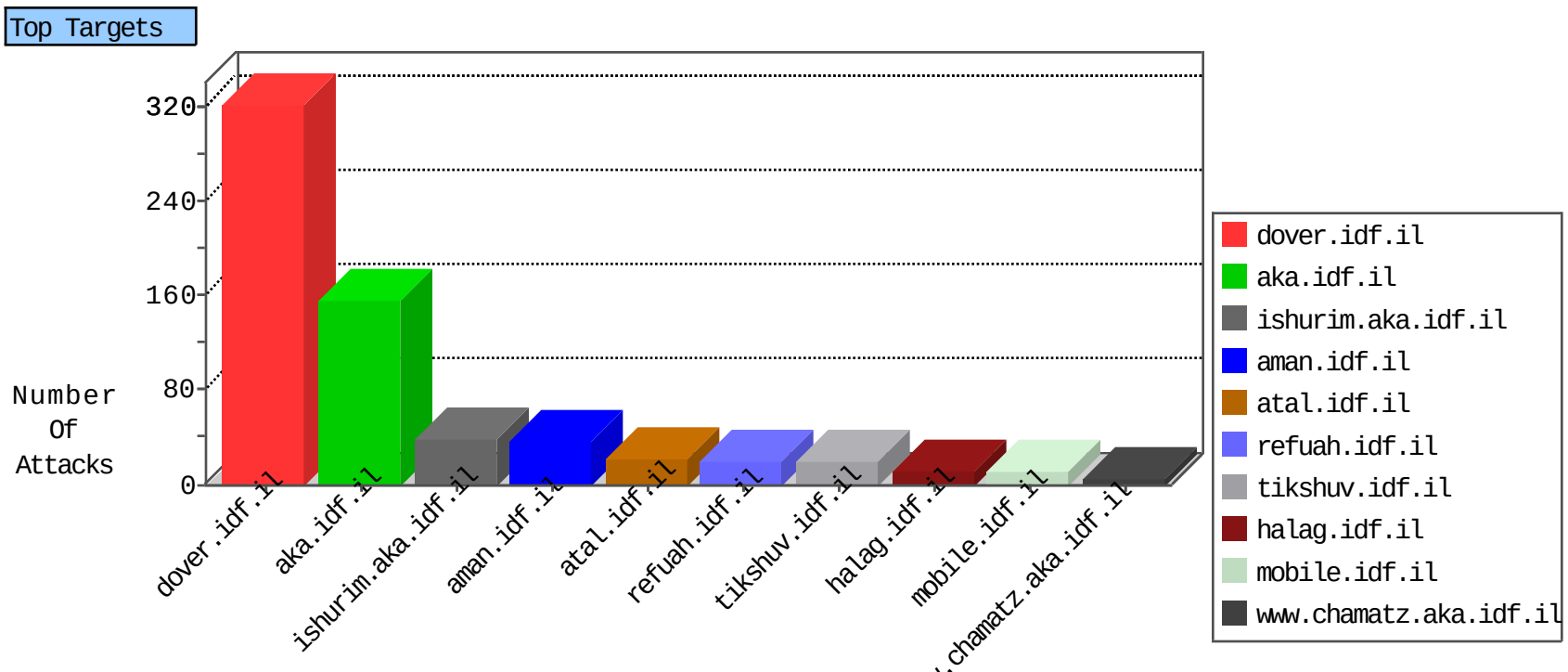
03-30-2015-17:03:01 to 03-30-2015-18:03:01

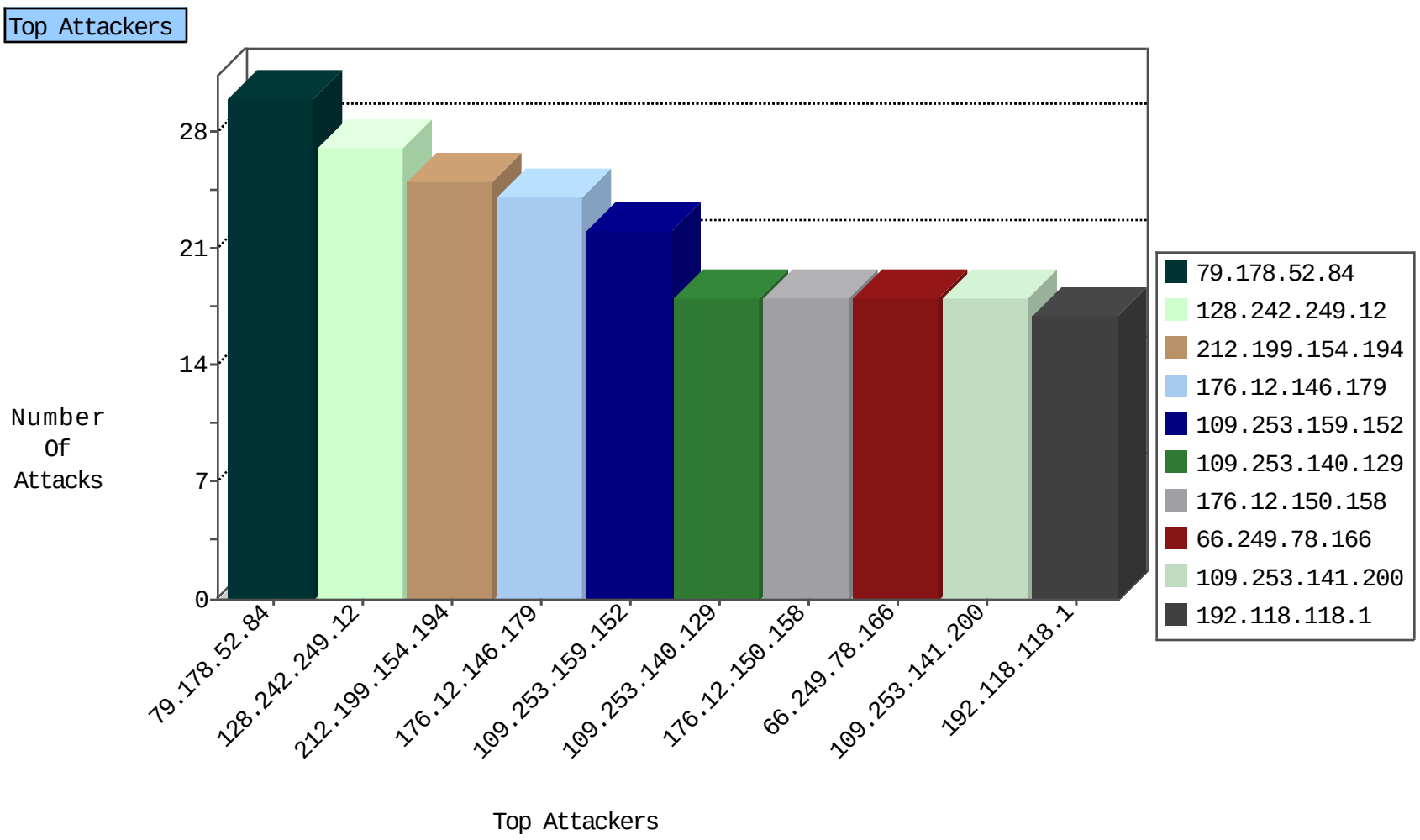
IDF Under Attack
03-30-2015-17:03:01

Top Targets



Top Target

Top Attackers



Top Attackers

03-30-2015-17:03:01 to 03-30-2015-18:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.178.52.84	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	302
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	252
37.142.175.10	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
59.84.70.174	Japan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	2
23.95.248.132	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
23.95.248.132	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
23.95.248.132	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

03-30-2015-17:03:01 to 03-30-2015-18:03:01

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	27
2.52.13.233	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	2
195.160.240.11	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
162.247.72.201		147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
77.109.141.138	Switzerland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.64.189.99	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
79.178.189.202	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1

03-30-2015-17:03:01 to 03-30-2015-18:03:01

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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
46.19.85.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.124.237	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.2.230	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
37.142.144.237	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
2.54.151.224	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
93.173.236.165	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.180.31	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.118.28	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.241.231	Singapore	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.228.207.76	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.142.131.245	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
2.52.15.11	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.197.103.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.9	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

03-30-2015-17:03:01 to 03-30-2015-18:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.12.146.179	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.159.152	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.141.200	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.150.158	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.140.129	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
192.118.118.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
109.253.141.106	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.131.225	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.135.183	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.140.147	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
37.26.147.159	Israel	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.1	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.140.251	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.133.94	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.142.200	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.143.179	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.176.11.60	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
46.116.175.2	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
176.12.149.181	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
85.130.226.9	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
185.32.177.156	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
94.230.86.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
176.12.151.136	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
149.78.164.108	United States	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.33	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
37.26.148.228	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
37.26.148.228	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
84.110.53.170	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
79.176.11.60	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	3
37.26.148.228	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
174.238.1.107	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	2
84.110.53.170	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
85.130.206.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.146	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
149.88.87.110	United States	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.36	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.86.212	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
174.238.1.107	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
174.238.1.107	United States	147.237.77.216	dover.idf.il		Bad TCP sequence	monitor	2
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	15
212.235.108.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	6
199.203.100.145	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 199.203.100.145	Block	6
212.143.99.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	3
80.246.138.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
217.194.198.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
85.64.255.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.235.108.132	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
84.108.236.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.108.236.171	Block	3
199.203.100.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	2
79.176.215.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.142.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.236.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/6_s3_	Block	2
67.186.32.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
208.54.70.144	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
109.65.134.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.117.204.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
219.110.237.218	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	2
85.250.9.203	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
176.12.142.175	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.4	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.253.140.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.147.184	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9827-he/refuah.aspx	Block	1
149.200.184.229	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qr/	Block	1
46.117.47.217	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
109.67.192.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 1427727862600 in www.aka.idf.il/main/giyus/general.aspx	None	1
85.250.9.203	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
80.179.122.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
176.12.143.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.158.182	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.78.18	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
95.86.119.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.147.231	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
213.8.52.148	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
84.109.44.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
164.138.114.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.117.181.239	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.131.170	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.158.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
176.12.145.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.158.228	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
37.142.75.164	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.194.198.114	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.194.198.114	Block	1
192.114.5.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
84.228.118.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
176.12.136.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

03-30-2015-17:03:01 to 03-30-2015-18:03:01