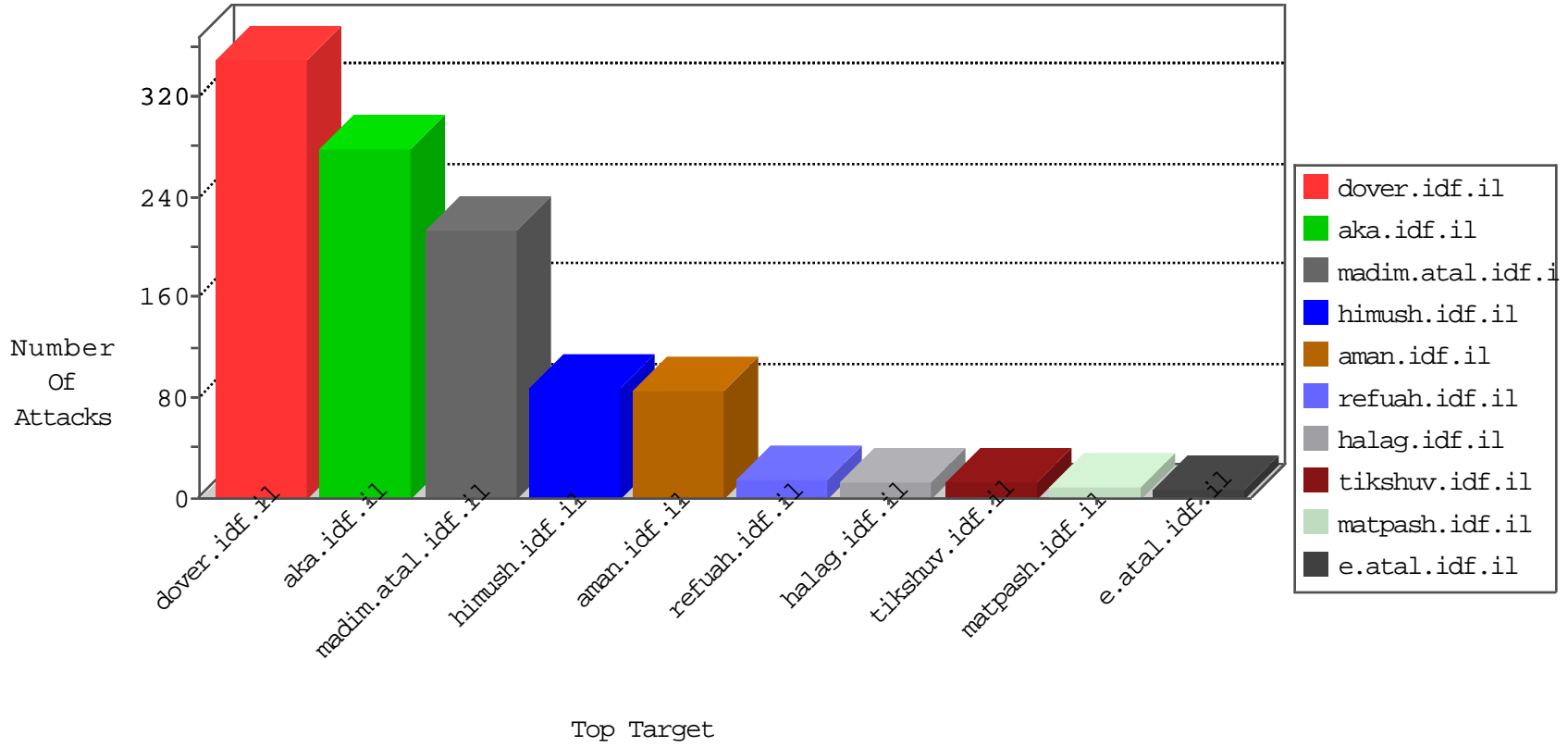
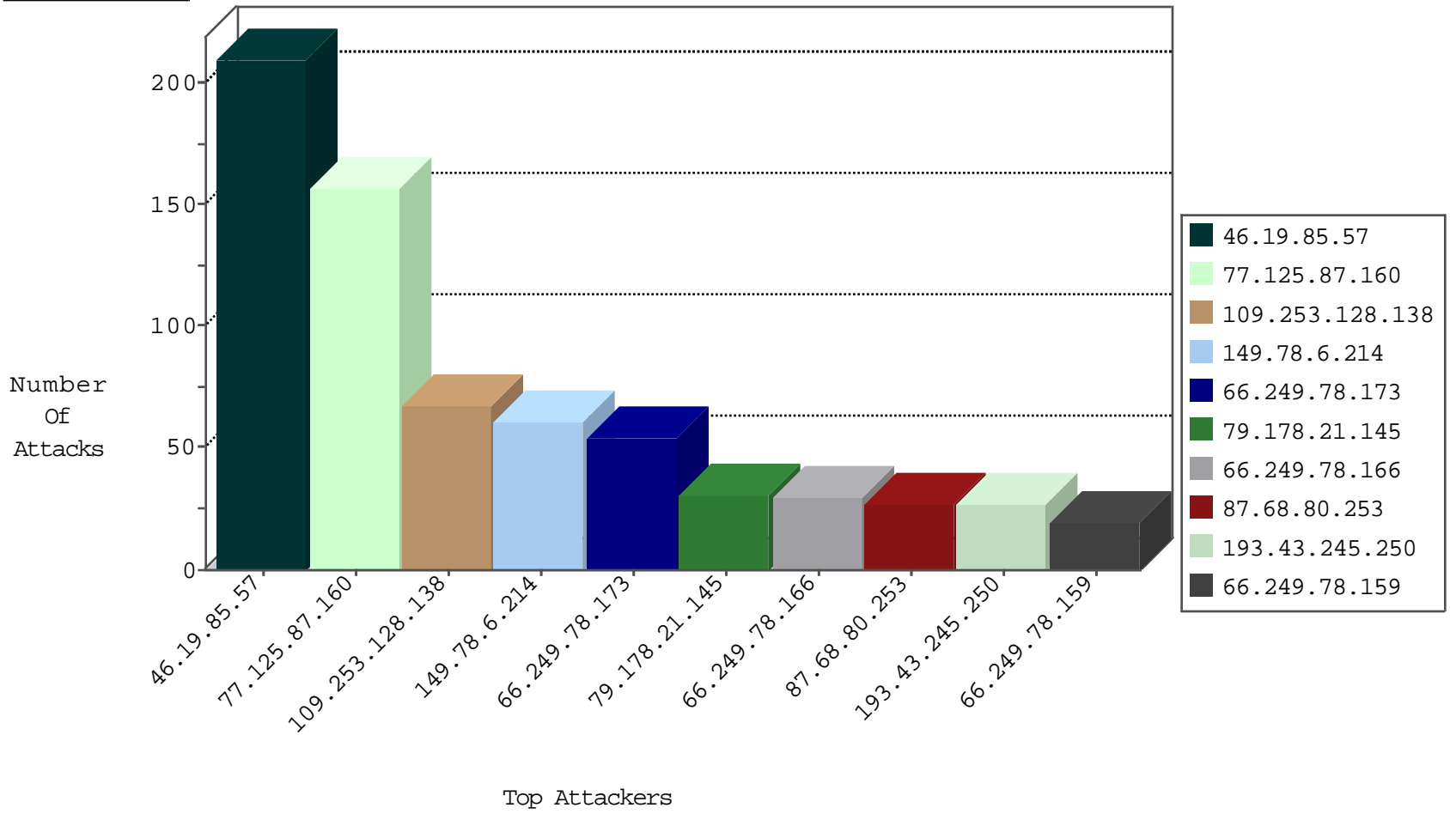


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	549
79.182.19.251	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
37.142.175.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
204.42.253.130	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.130	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
82.102.141.255	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	157
46.19.85.214	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
24.1.201.160	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.178.21.145	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.181.57.72	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.127.243.167	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.239	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
31.168.136.9	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.180.170.183	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	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.179	e.mazi.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
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
46.19.85.203	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.180.250.195	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	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
109.66.59.113	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	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	ychalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
147.188.240.104	United Kingdom	147.237.77.216	dover.idf.il	Cl000004: HTTP: options method (Microsoft)	Block	1

Top Attackers In ID

Attacker Address	Attacker Country	Target Address	Site	Name	Count
109.253.128.138	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	11
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
43.255.191.162	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.128.48.130	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.205.126	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
213.8.76.189	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.130	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.115.248.2	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.172	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.147.119	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
43.255.191.162	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
109.253.144.1	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
43.255.191.162	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
109.65.121.212	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.162	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
81.218.32.210	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.226	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
62.128.40.226	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.76.34	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.171.86	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.130	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
115.231.218.147	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
109.253.146.99	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
109.253.128.138	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	29
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
109.253.128.138	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	alert	27
87.68.80.253	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.131.148	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.149.177	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
79.178.21.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
212.179.75.118	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
79.178.21.145	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	9
80.178.195.89	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
178.135.118.70	Lebanon	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
176.12.136.24	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
149.78.237.43	United States	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
176.12.145.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.147.119	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.150.163	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.132.39	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
188.120.148.176	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
79.178.21.145	Israel	147.237.77.234	halag.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
109.253.146.99	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
37.247.36.69	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	5
82.80.34.127	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
176.12.137.189	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
79.178.21.145	Israel	147.237.77.234	halag.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	4
176.12.141.116	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
188.120.148.176	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.86.233	Israel	147.237.0.19	madim.atal.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
192.115.90.42	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
212.150.195.192	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
66.249.78.197	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	3
212.179.75.118	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
109.253.144.1	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
147.235.185.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.0.88	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
212.150.195.192	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
62.219.119.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.34.76	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
209.95.36.61	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/0	Block	7
2.54.166.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.250.5.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
46.19.85.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.78.150.59	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
94.230.86.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.175.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.80.34.127	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.80.168.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
180.76.6.136	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
109.253.159.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.188.80	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
79.183.56.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/wante.stm	Block	1
159.224.160.225	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/3/3223.pdf+++++++result:~x?x*x?x?x"x>xžx;Ä¼+xoxžx xœÄ»+x" x>Äž+xžxcxŸx x?x'xšx~	Block	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/armored2.stm	Block	1
109.67.205.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
83.244.6.141	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluintemplates/inner.asp	Block	1
188.165.15.121	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1405-he/atal.aspx	Block	1
141.212.122.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
87.69.206.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.141.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/print_bottom.asp	Block	1
46.19.85.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.253.136.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.110.8.87	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	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
192.115.90.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
62.219.118.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.151.39.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
176.12.147.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_bottom.asp	Block	1
109.253.141.152	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.41.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.163.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/fagselecion.aspx	None	1
192.187.126.162	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
149.78.237.43	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.64.115	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
109.64.66.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.150.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/print_bottom.asp	Block	1
46.19.85.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.142.0	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.212.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.160.240.11	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1