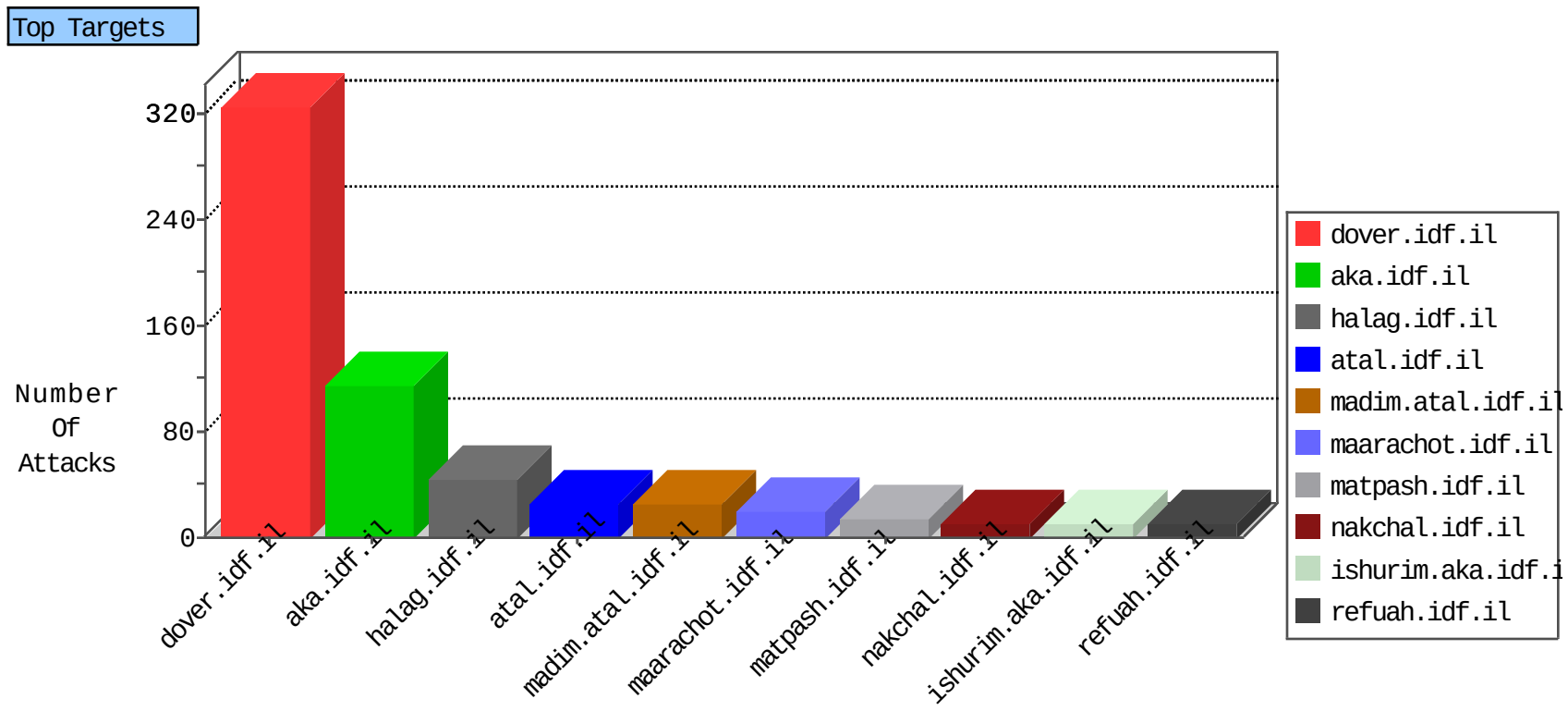
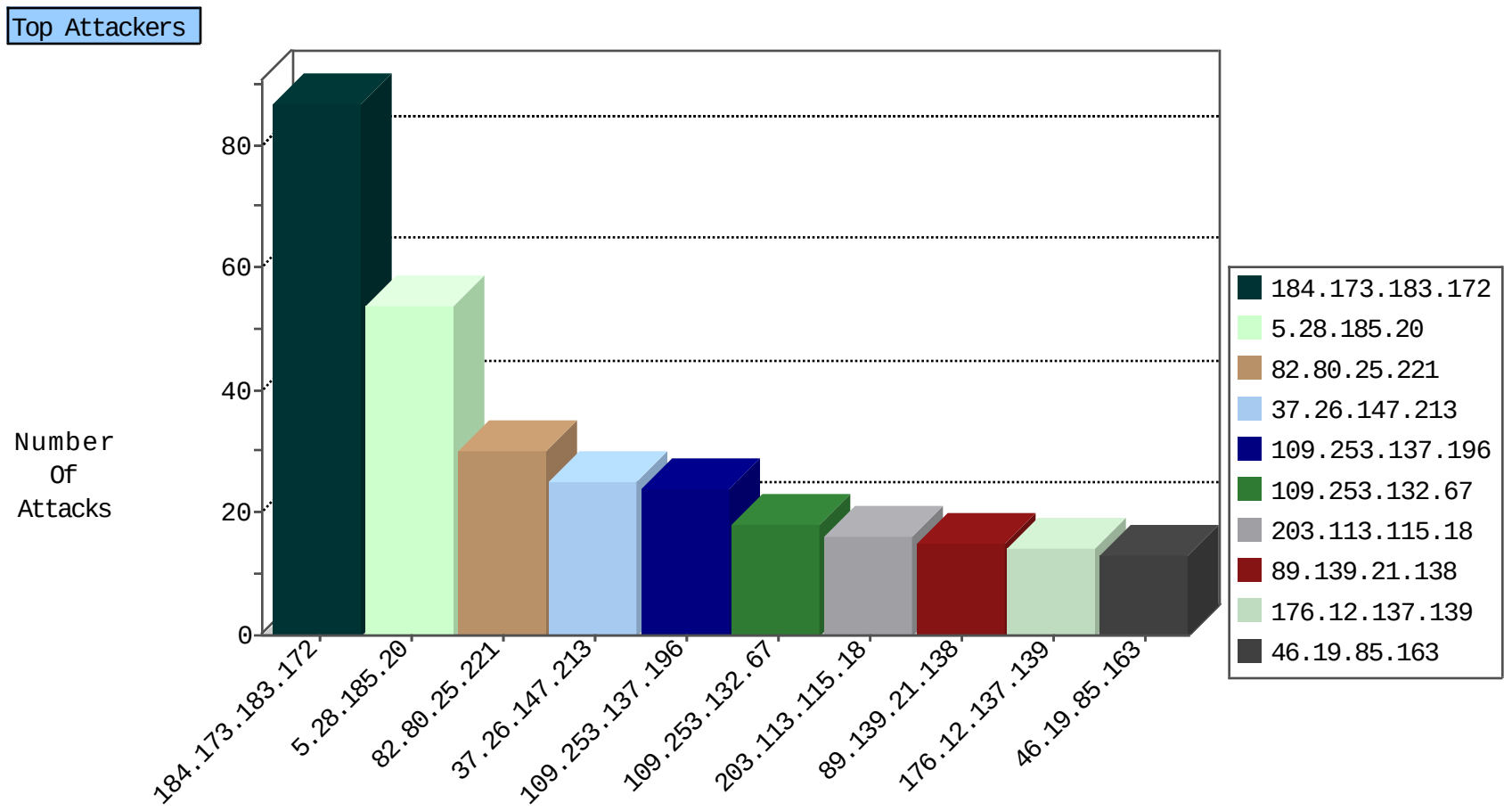
03-31-2015-19:03:03 to 03-31-2015-20:03:03

IDF Under Attack
03-31-2015-19:03:03

Top Targets



Top Attackers



03-31-2015-19:03:03 to 03-31-2015-20:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
213.57.198.66	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
79.178.116.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
79.181.127.252	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
89.248.172.57	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.57	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

03-31-2015-19:03:03 to 03-31-2015-20:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	87
91.212.205.187	France	147.237.77.176	matpash.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	9
109.65.182.122	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
89.139.21.138	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
203.113.115.18	Thailand	147.237.77.170	maarachot.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
89.139.21.138	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.163	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	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.253	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.132.2	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	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
193.50.135.144	France	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
84.228.29.11	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	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
2.54.23.51	Israel	147.237.76.39	mobile.meitav.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.46	e.chinuch.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
218.30.103.52	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
5.29.62.9	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-31-2015-19:03:03 to 03-31-2015-20:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	30
203.113.115.18	Thailand	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
79.180.31.144	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
202.160.175.231	India	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
115.231.218.147	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.228	Netherlands	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.188.212	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.228	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.188.212	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
46.116.212.180	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
202.160.175.231	India	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.162.228	Netherlands	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.162.228	Netherlands	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.188.212	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.228	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
80.120.225.170	Austria	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.188.212	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1

03-31-2015-19:03:03 to 03-31-2015-20:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.28.185.20	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
109.253.137.196	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.132.67	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.137.139	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
109.253.139.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.133.229	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.93.219	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.93.213	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.144.231	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.201	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
109.65.182.122	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
176.12.136.149	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.157	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
5.102.254.198	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
77.127.243.167	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.201	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
37.26.148.178	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
80.229.223.5	United Kingdom	147.237.77.176	matpash.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
89.139.21.138	Israel	147.237.77.234	halag.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
89.204.135.131	Germany	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3
80.229.223.5	United Kingdom	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
185.32.176.86	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
37.26.148.178	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
46.19.85.45	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
185.32.176.86	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
185.32.176.86	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
46.19.86.143	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
37.26.148.132	Israel	147.237.72.166	aka.idf.il	illegal header format detected: Malformed HTTP protocol name in response	Block HTTP Non Compliant	monitor	2
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
217.132.99.222	Israel	147.237.77.61	e.cogat.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
46.19.86.43	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
93.172.84.161	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	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
89.139.21.138	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
37.26.148.178	Israel	147.237.76.31	nakchal.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
109.253.159.189	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.211	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
109.160.136.191	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
37.142.197.218	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
85.65.230.218	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.121.192	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
213.57.98.95	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.32	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.213	Block	24
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
85.250.95.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	5
149.78.57.48	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	4
203.113.115.18	Thailand	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	4
37.26.148.132	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
85.65.153.54	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	3
2.54.147.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.54.147.201	Block	3
2.54.34.154	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
50.118.172.172	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	2
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
37.26.147.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	2
66.249.93.239	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
37.142.113.134	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl05 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
106.187.46.34	Japan	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 106.187.46.34	Block	1
2.54.62.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/sari.stm	Block	1
176.12.143.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
77.127.228.239	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/payslips.aspx/	Block	1
109.253.149.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
46.121.254.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
93.172.6.6	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
84.94.91.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/30b.stm	Block	1
149.78.232.116	United States	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtPassword in www.aka.idf.il/main/sachar/	None	1
46.19.85.45	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
106.187.46.34	Japan	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-admin/	Block	1
85.250.44.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtPassword in www.aka.idf.il/main/sachar/	None	1
2.54.143.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
212.179.61.126	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
176.12.147.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.180.148.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
120.15.33.201	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 120.15.33.201	Block	1
93.172.35.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
203.133.169.208	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.208	Block	1
84.108.214.123	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/69-he/sb_item_lev1	Block	1
175.42.91.133	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/7/4207.pdf/trackback/	Block	1
109.64.186.214	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
176.12.149.53	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.182.96.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
120.15.33.201	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx/trackback/	Block	1
66.249.64.56	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
93.173.187.43	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
84.111.29.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.34.154	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.34.154	Block	1
203.133.169.208	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1210-3.stm	Block	1
176.12.137.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1