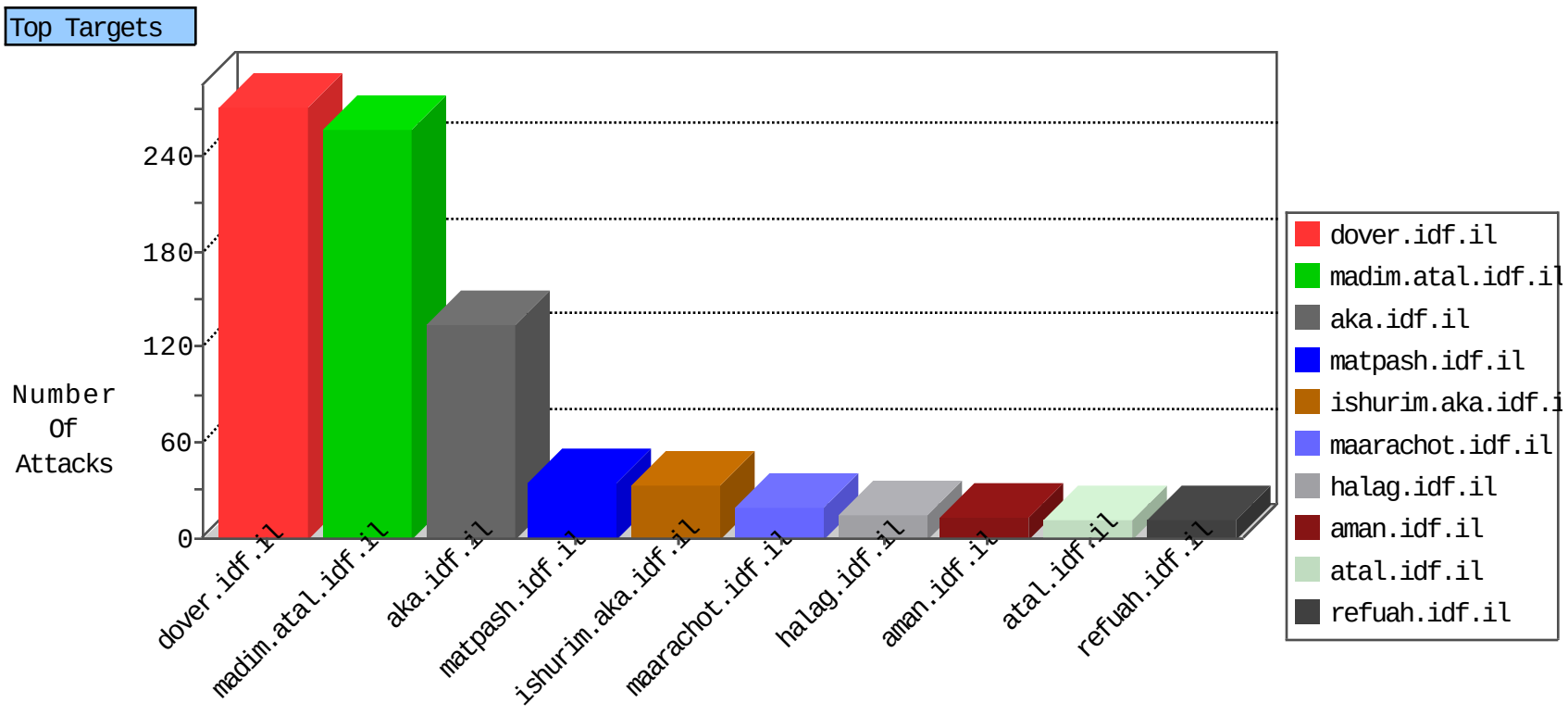
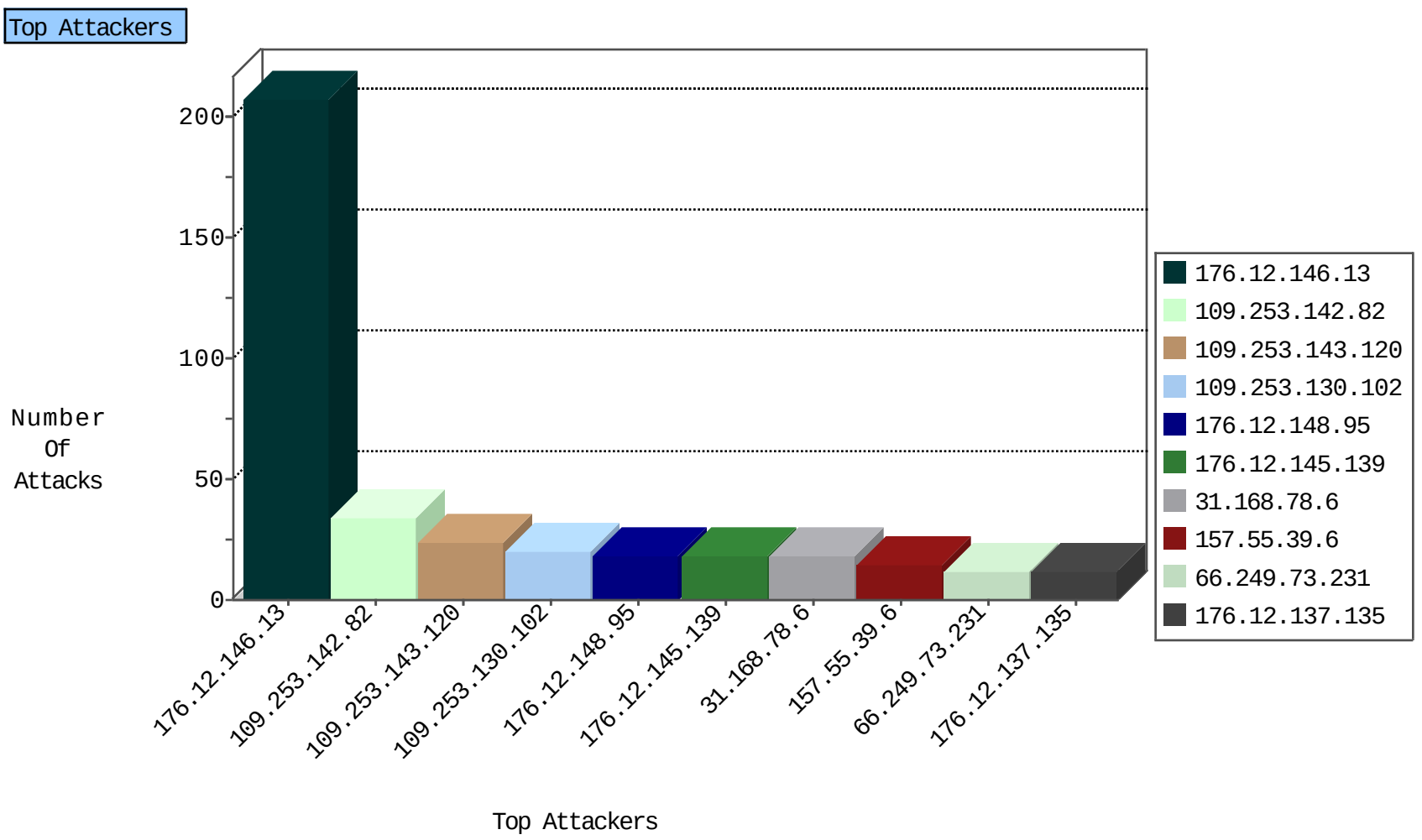
03-29-2015-14:03:06 to 03-29-2015-15:03:06

IDF Under Attack
03-29-2015-14:03:06

Top Targets



Top Attackers



03-29-2015-14:03:06 to 03-29-2015-15:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
5.29.192.196	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
174.92.179.64	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
178.195.221.116	Switzerland	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
188.26.131.116	Romania	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
157.55.39.42	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
178.196.215.136	Switzerland	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	4
91.32.26.222	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
82.205.118.133	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	3
141.0.10.226	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
80.3.244.70	United Kingdom	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
188.100.227.27	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
84.147.132.60	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
54.72.0.55	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.78.89	United States	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
82.145.209.102	Europe	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	2
66.249.78.160	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
173.252.73.114	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
66.249.93.213	United States	147.237.72.156	aman.idf.il	unblock-sp-traf1	forward	1
207.46.13.89	United States	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	1
185.27.118.48	Egypt	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
199.30.24.91	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
157.55.39.179	United States	147.237.0.34	tikshuv.idf.il	unblock-sp-traf1	forward	1
82.205.118.133	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
212.33.111.185	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
157.55.39.215	United States	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	1
66.249.78.204	United States	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
37.187.157.73	France	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1

03-29-2015-14:03:06 to 03-29-2015-15:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
147.236.238.10	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.93	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.177.125.254	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1

03-29-2015-14:03:06 to 03-29-2015-15:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
79.176.64.55	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
208.39.68.33	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
61.240.144.64	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
118.69.174.89	Vietnam	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.210.127.3	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.25.159	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
87.68.59.79	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.177.158.149	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.44.227	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
208.39.68.33	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.66	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
201.163.31.150	Mexico	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.230.81.98	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	Turkey	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
85.64.177.241	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.178.152	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.2.201	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

03-29-2015-14:03:06 to 03-29-2015-15:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.143.120	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.130.102	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
31.168.78.6	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.148.95	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.145.139	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.73.231	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.139.58	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
85.130.219.42	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
37.142.255.87	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
82.80.168.23	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
94.159.187.35	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	7
192.117.155.7	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.148.38	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.144.218	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
192.118.27.253	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	6
109.253.138.0	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
80.246.133.166	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
80.246.133.166	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
132.74.58.19	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	5
46.19.86.18	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.86.57	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
212.199.251.227	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
46.19.85.244	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.54.188.62	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
2.54.151.230	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
2.54.188.62	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
2.54.151.230	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
85.64.136.193	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
2.54.151.230	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
46.19.85.166	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
2.54.188.62	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.5.35	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.151	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
85.64.136.193	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
192.117.155.7	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
46.19.85.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.156	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
199.30.25.236	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
5.29.135.142	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.73.239	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
5.102.254.78	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
37.46.39.135	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	1
80.246.137.188	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.121.211.31	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
132.74.95.21	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.181	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.146.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	208
109.253.142.82	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.142.82	Block	34
176.12.137.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
87.68.23.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
5.29.32.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
212.25.102.57	Israel	147.237.0.16	my-kosher-kravi.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 212.25.102.57	None	4
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	3
213.8.71.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.139.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.8.122.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
197.15.39.130	Tunisia	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
8.29.198.40	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 8.29.198.40	Block	2
109.226.41.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
195.160.240.11	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/shonot/meida/noinformation.stm	Block	2
213.57.148.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.120.167.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
8.29.198.41	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 8.29.198.41	Block	2
8.29.198.39	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 8.29.198.39	Block	2
176.12.144.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
109.160.238.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.142.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
94.159.170.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.100.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.114.5.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
8.29.198.36	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1	Block	1
176.12.136.15	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	Unauthorized URL Access to www.idf.il/hebrew/organization/patzar/atar1/mls1/kesher.stm	Block	1
5.22.129.166	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
46.19.85.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
109.186.112.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
87.68.47.189	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
185.24.79.212	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/links.aspx	Block	1
79.180.171.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
8.29.198.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1043-he/idfg.a	Block	1
132.74.58.19	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
109.253.136.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.90.99.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.255.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl50.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
94.159.222.49	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtMisparTeuda in www.aka.idf.il/main/sachar/	None	1
8.29.198.37	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 8.29.198.37	Block	1
84.108.79.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
213.8.122.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter prefixText in www.aka.idf.il/homas/site/resources/services/wsmaterials.asmx/getmaterialpossiblenamesbynamestart	None	1
109.253.143.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.116.149.254	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	1

03-29-2015-14:03:06 to 03-29-2015-15:03:06