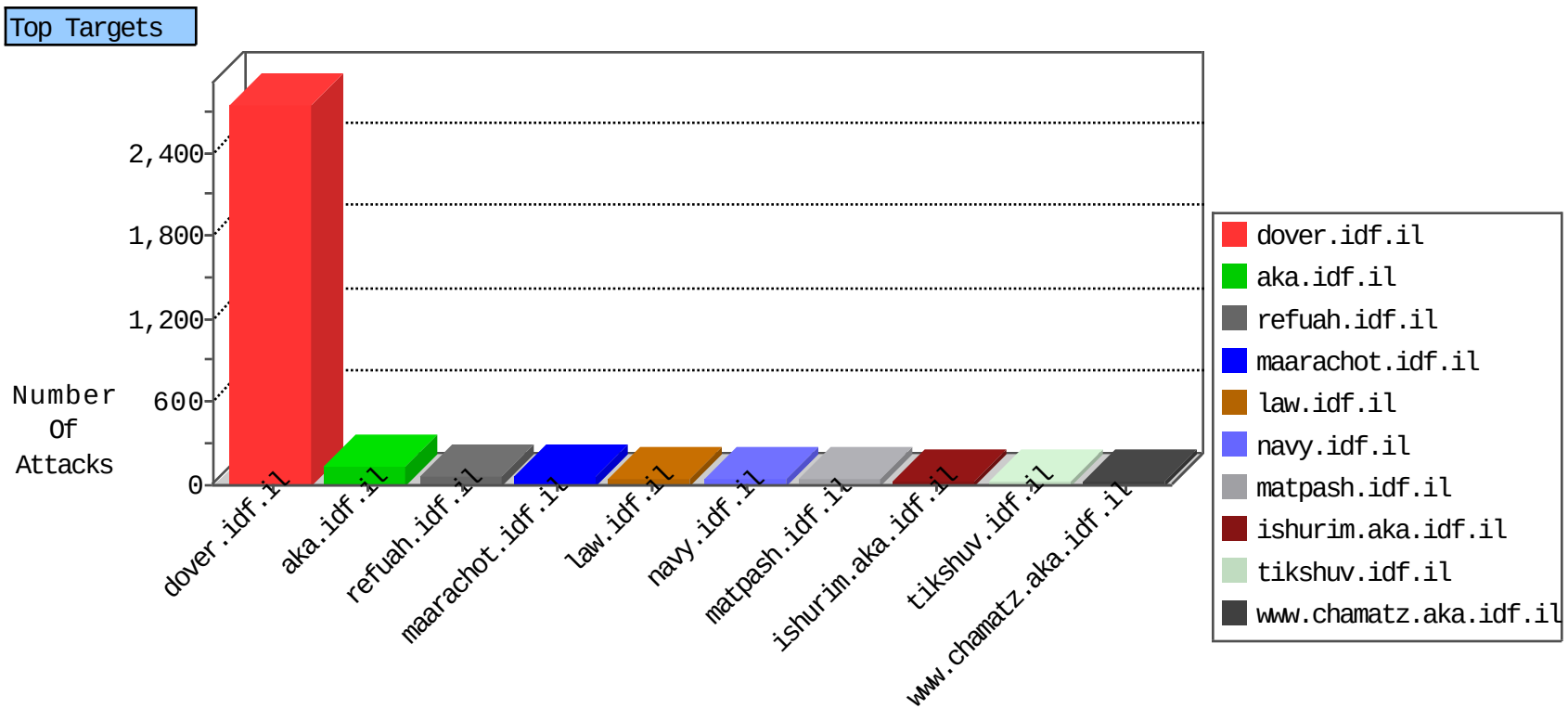
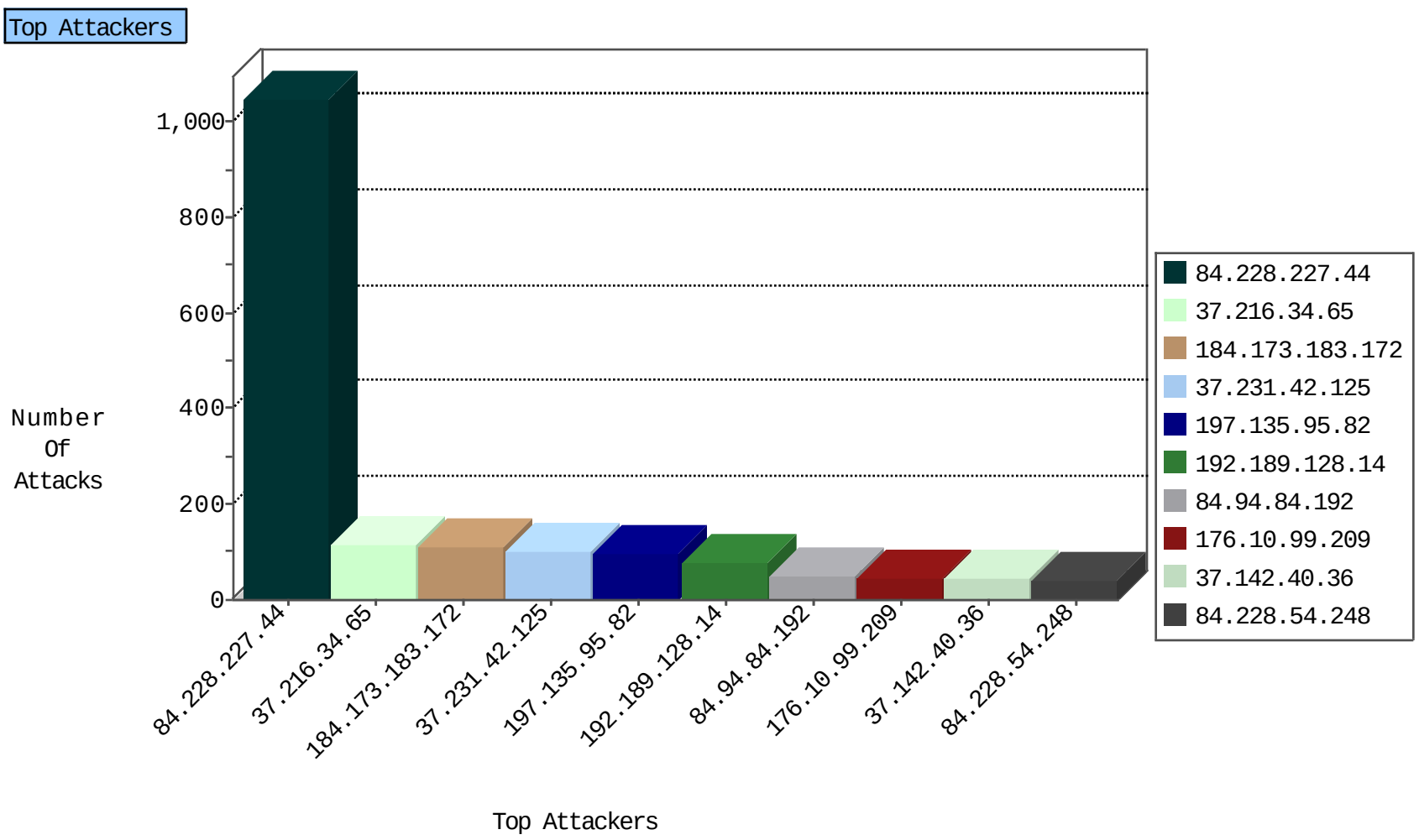
04-10-2015-09:03:07 to 04-10-2015-10:03:07

IDF Under Attack
04-10-2015-09:03:07





04-10-2015-09:03:07 to 04-10-2015-10:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.76	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	366
149.78.238.241	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	297
220.181.108.121	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	229
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	34
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
152.62.109.60	Europe	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	15
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.69.128	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	10
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	8
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.64.63	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.65.178	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.64.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.65.155	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	4
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.64.155	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.91.99	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.69.8	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	4
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.64.59	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	4
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	3
66.249.91.107	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	3

04-10-2015-09:03:07 to 04-10-2015-10:03:07

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	108
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	12
110.77.229.113	Thailand	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.52.127.168	Saudi Arabia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.120	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
118.97.190.174	Indonesia	147.237.76.30	himush.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
68.96.180.171	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
149.78.131.62	United States	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
82.128.252.32	Finland	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
107.3.96.226	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-10-2015-09:03:07 to 04-10-2015-10:03:07

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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
62.219.224.45	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.150.247	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.77	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.77	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.60	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.56.231	Netherlands	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.230.73	United States	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.60	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
27.50.132.60	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
209.126.230.74	United States	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

04-10-2015-09:03:07 to 04-10-2015-10:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.228.227.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1050
37.216.34.65	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	116
37.231.42.125	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	102
197.135.95.82	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	95
192.189.128.14	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	78
84.94.84.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
37.142.40.36	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
84.228.54.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
176.10.99.209	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
109.253.158.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
109.253.141.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
190.107.176.148	Chile	147.237.77.216	dover.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	24
89.139.20.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
176.12.147.178	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.65.19.206	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	17
105.226.16.157	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
39.48.183.65	Pakistan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
212.150.174.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
220.225.247.121	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.253.145.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.130.192	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.145.228	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
185.24.205.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.137.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
80.246.133.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
109.253.139.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.181.209.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
178.152.253.7	Qatar	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
94.230.82.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
24.234.180.234	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
37.26.147.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
41.69.246.75	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6

04-10-2015-09:03:07 to 04-10-2015-10:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
190.107.176.148	Chile	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	4
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
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
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
37.26.146.131	Israel	147.237.76.86	navy.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 37.26.146.131	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Extremely Long HTTP Request	Block	1
109.65.19.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.251	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
180.76.4.170	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
84.109.37.120	Israel	147.237.72.166	aka.idf.il	NULL Character in Method	Block	1
37.152.88.35	Spain	147.237.77.216	dover.idf.il	Distributed Extremely Long HTTP Request	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
109.253.143.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.154.28.130	United States	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
85.65.102.89	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
37.152.88.35	Spain	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
188.138.17.205	France	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
79.183.106.48	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
207.46.13.103	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Distributed Extremely Long HTTP Request	Block	1
93.172.13.133	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.152.88.35	Spain	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
188.165.15.239	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/news/www.sviva.gov.il	Block	1
157.55.39.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.36.88	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
217.200.201.104	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/klf/	Block	1
94.159.204.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	Block	1
176.10.99.209	Switzerland	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
84.109.37.120	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	1

04-10-2015-09:03:07 to 04-10-2015-10:03:07