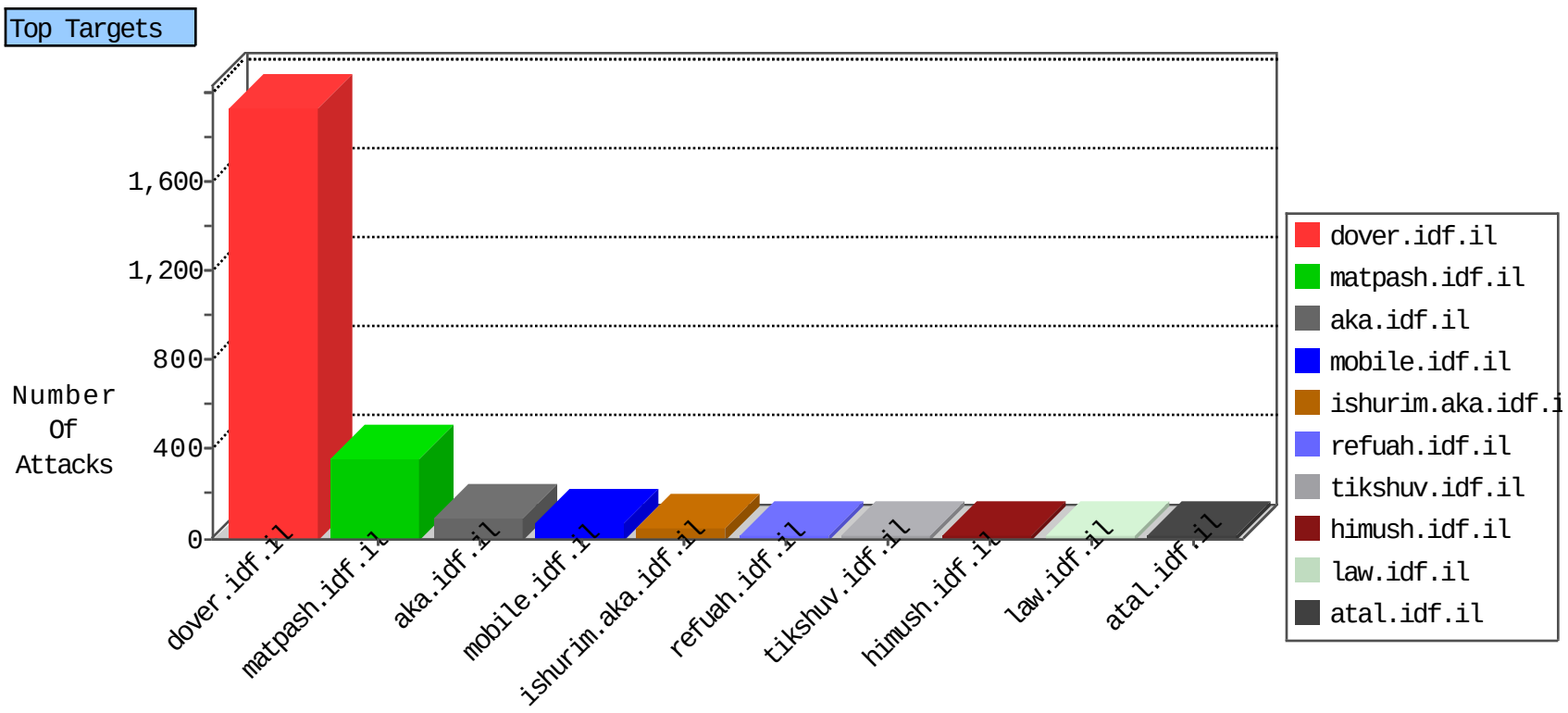
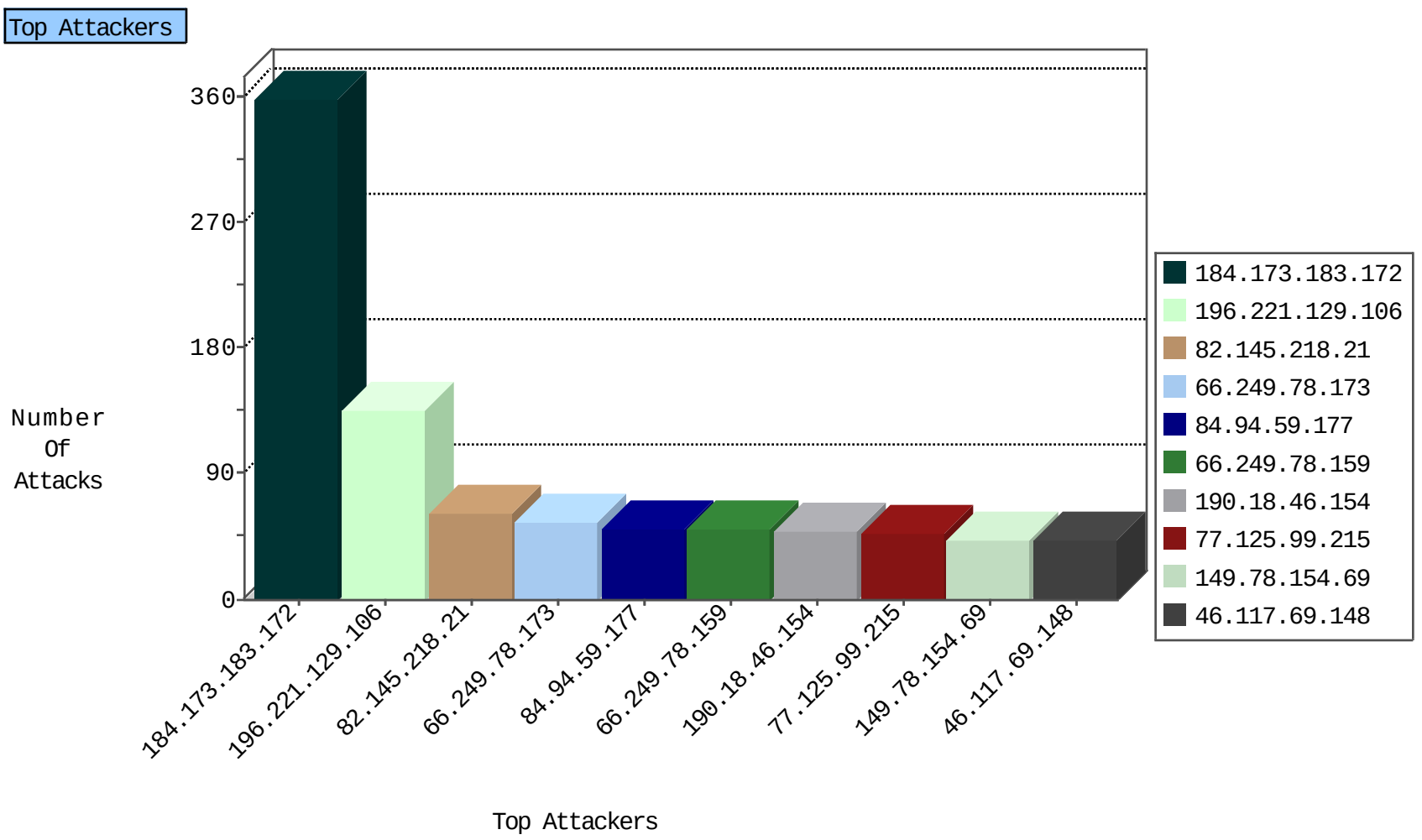
05-07-2015-21:03:01 to 05-07-2015-22:03:01

IDF Under Attack
05-07-2015-21:03:01

Top Targets



Top Attackers



05-07-2015-21:03:01 to 05-07-2015-22:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
77.125.99.215	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	537
109.253.132.231	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	287
84.228.50.12	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
82.81.192.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
77.127.214.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.177.101.188	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
2.52.142.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.253.132.231	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
180.27.203.65	Japan	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
192.3.207.66	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
37.142.5.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-07-2015-21:03:01 to 05-07-2015-22:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	358
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	2
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
64.90.250.253	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.77.61	e.cogat.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	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
101.251.236.91	China	147.237.76.30	himush.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.48	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.197	e.himush.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
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1

05-07-2015-21:03:01 to 05-07-2015-22:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
78.108.169.33	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
46.121.211.116	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
109.64.110.100	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.2.206	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
37.142.147.252	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.130.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.75.117	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.73.168	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	ET DROP Dshield Block Listed Source	1
46.19.86.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
178.19.107.114	Poland	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
24.203.59.13	Canada	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
162.243.219.157	United States	147.237.0.16	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.64	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.146.126	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
121.46.0.125	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
104.131.193.55		147.237.77.243	mobile.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

05-07-2015-21:03:01 to 05-07-2015-22:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
196.221.129.106	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	129
82.145.218.21	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
84.94.59.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
190.18.46.154	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
46.117.69.148	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
129.42.208.182	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
77.125.252.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
78.108.169.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
213.151.62.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
84.153.30.25	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
71.118.29.7	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
79.177.199.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.117.254.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
2.54.160.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
176.12.142.152	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
79.181.128.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
164.138.119.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
84.109.179.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
46.120.102.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
37.26.146.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
185.32.176.24	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
90.144.130.224	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
107.77.83.58	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
62.219.112.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
77.127.214.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.26.147.179	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
37.26.147.179	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	11
46.19.86.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
31.186.228.91	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.181.101.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.117.121.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
93.173.169.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
87.68.219.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
85.250.165.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
176.12.149.244	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
173.34.193.54	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.182.105.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
85.250.15.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
87.68.47.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.177.205.99	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.52.28.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
79.181.101.118	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
77.127.72.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
31.44.141.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
85.64.96.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.117.69.148	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication	Block	2
87.68.219.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	2
46.120.228.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.66.56.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
157.55.39.4	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
104.131.193.55		147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
5.29.222.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.185.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
162.243.219.157	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.117.27.244	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENER in www.aka.idf.il/main/sachar/payslips.aspx	None	1
104.131.211.96		147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on //	Block	1
188.165.15.87	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.243	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
104.131.193.55		147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on //	Block	1
79.182.29.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
162.243.219.157	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on //	Block	1
104.131.211.96		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on //	Block	1
79.176.151.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
202.46.50.128	China	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1540-he/refuah.aspx	Block	1
104.131.193.55		147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.168.212.91	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
80.246.133.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
162.243.219.157	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on //	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
109.64.149.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
87.68.231.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
2.54.165.255	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.176.151.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
212.129.13.178	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
157.55.39.151	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers/news	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
104.131.193.62		147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on //	Block	1
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
82.166.130.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
176.12.148.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	1
93.172.167.148	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
5.22.135.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1