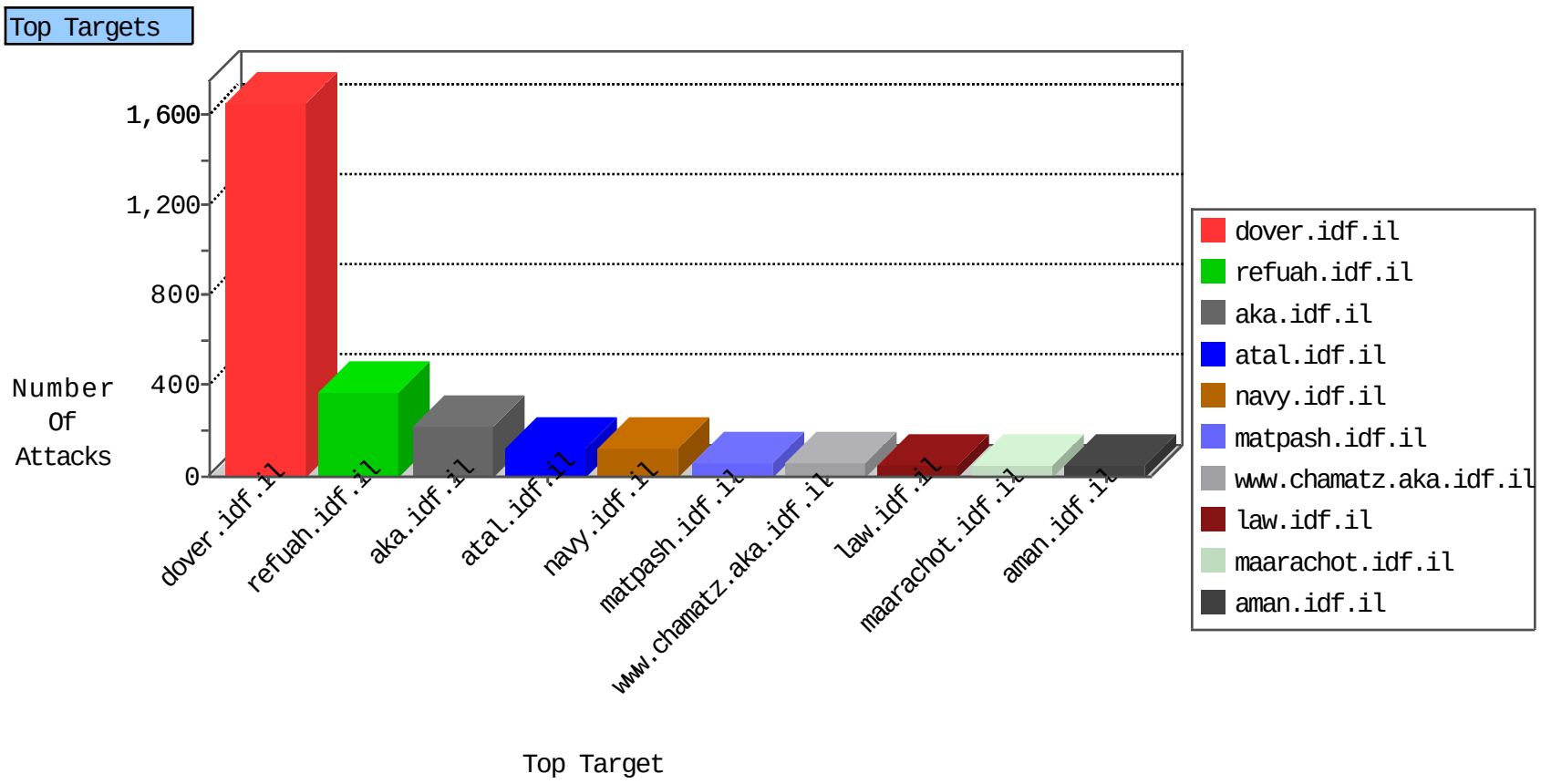
04-08-2015-13:03:01 to 04-08-2015-14:03:01

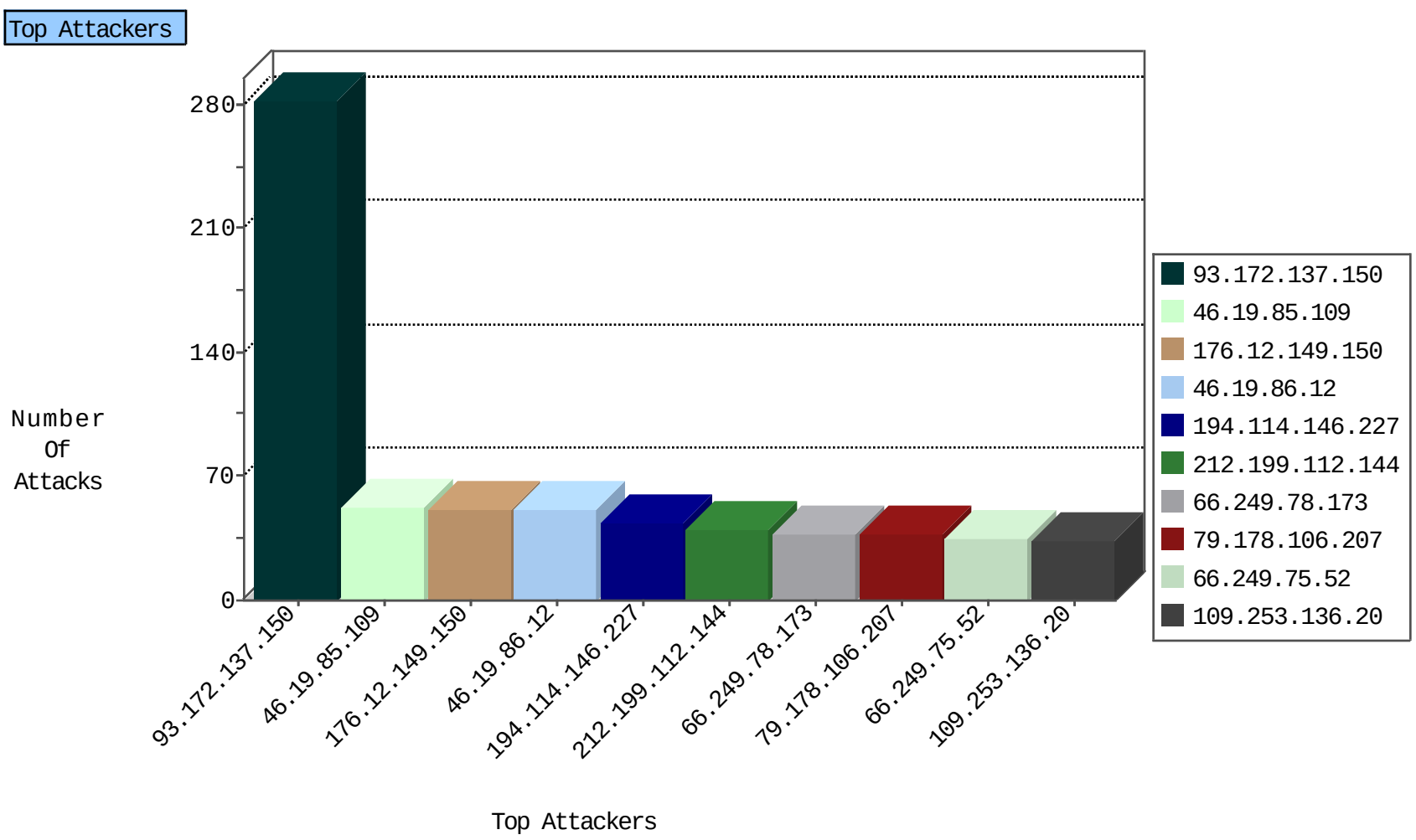
IDF Under Attack
04-08-2015-13:03:01

Top Targets



Top Target

Top Attackers



Top Attackers

04-08-2015-13:03:01 to 04-08-2015-14:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
81.218.159.247	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2179
109.253.159.255	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1100
192.116.130.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	688
2.52.49.9	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	411
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	364
46.117.96.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	37
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	35
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	34
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	26
130.104.29.209	Belgium	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.67.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	21
66.249.64.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	21
66.249.75.44	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	21
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.75.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	20
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	19
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.78.166	United States	147.237.77.216	dover.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	15
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	14
66.249.93.154	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	13
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.69.58	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.78.148	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	8
109.253.132.234	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6

04-08-2015-13:03:01 to 04-08-2015-14:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
73.214.31.4	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
80.82.70.198	Netherlands	147.237.77.61	e.cogat.idf.il	DVRep_P-N_40-59	Permit	1
2.70.248.35	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
112.198.64.62	Philippines	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.77.178	e.matpash.idf.il	DVRep_P-N_40-59	Permit	1
5.254.97.68	Romania	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
80.82.70.198	Netherlands	147.237.8.50	e.tikshuv.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.77.227	e.hamaz.idf.il	DVRep_P-N_40-59	Permit	1
46.19.85.0	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.76.177	ncore.idf.il	DVRep_P-N_40-59	Permit	1
84.108.68.25	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.169	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.82.70.198	Netherlands	147.237.76.197	e.himush.idf.il	DVRep_P-N_40-59	Permit	1

04-08-2015-13:03:01 to 04-08-2015-14:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
221.235.188.212	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.72.156	aman.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
5.254.97.68	Romania	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	1

04-08-2015-13:03:01 to 04-08-2015-14:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
93.172.137.150	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	278
176.12.149.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
46.19.85.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
46.19.86.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
194.114.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
79.178.106.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
109.253.149.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
24.31.228.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
77.127.127.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
212.76.99.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
2.54.43.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
5.29.125.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
37.26.147.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.19.86.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.253.130.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.159.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
2.54.14.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.150.174.130	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	12
77.127.235.45	Israel	147.237.72.166	aka.idf.il	Invalid checksum. Packet dropped.	Streaming Engine: TCP Invalid Checksum	drop	11
87.74.17.32	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
2.54.152.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
84.228.208.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
81.218.159.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
87.68.214.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.179.103.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
31.168.226.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
192.116.188.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
5.22.135.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
93.172.40.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
77.126.32.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
130.104.29.209	Belgium	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
176.12.147.253	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
80.178.24.76	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
87.69.210.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.228.199.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.178.160.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
117.196.223.161	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.179.17.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.176.61.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
2.52.165.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.86.68.29	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	4
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
79.182.62.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.16.72.139	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	2
94.159.219.155	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.159.219.155	Block	2
212.76.105.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.208.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 202.112.50.77	Block	1
5.254.97.68	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8871-he/refuah.aspx	Block	1
94.159.219.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/insignia/insignia.stm	Block	1
79.180.103.186	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.150.174.130	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 212.150.174.130	Block	1
195.154.199.79	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 195.154.199.79	Block	1
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
2.52.161.167	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
164.138.116.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	1
84.228.247.229	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.247.229	Block	1
77.127.217.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
188.165.15.239	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
212.179.42.241	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7489-he/tikshuv.aspx#.vsrl5mre-nm	Block	1
195.154.199.79	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18020-en/dover.aspx++++++++++++++++++++++++++++++++++++result:+error:+"/+-+/+-+document.location.href+=+'/404_ie6_en.htm'	Block	1
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.51.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
164.138.116.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.x in aka.idf.il/main/sachar/	None	1
84.228.247.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/gallery/6_s3_	Block	1
77.127.227.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
207.46.13.18	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
194.54.168.76	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 194.54.168.76 (Unknown SSL Session)	None	1
31.13.112.119	Ireland	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/1132-8767-he	Block	1
109.186.147.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
80.246.130.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Malformed URL	Block	1
46.19.85.168	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.27.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
93.172.137.150	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
79.177.16.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/fund/×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Â§×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½	Block	1
194.54.168.76	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
84.228.118.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Malformed URL from 202.112.50.77	Block	1
46.19.86.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.254.97.68	Romania	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
174.129.237.157	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.180.54.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	1
194.90.167.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-08-2015-13:03:01 to 04-08-2015-14:03:01