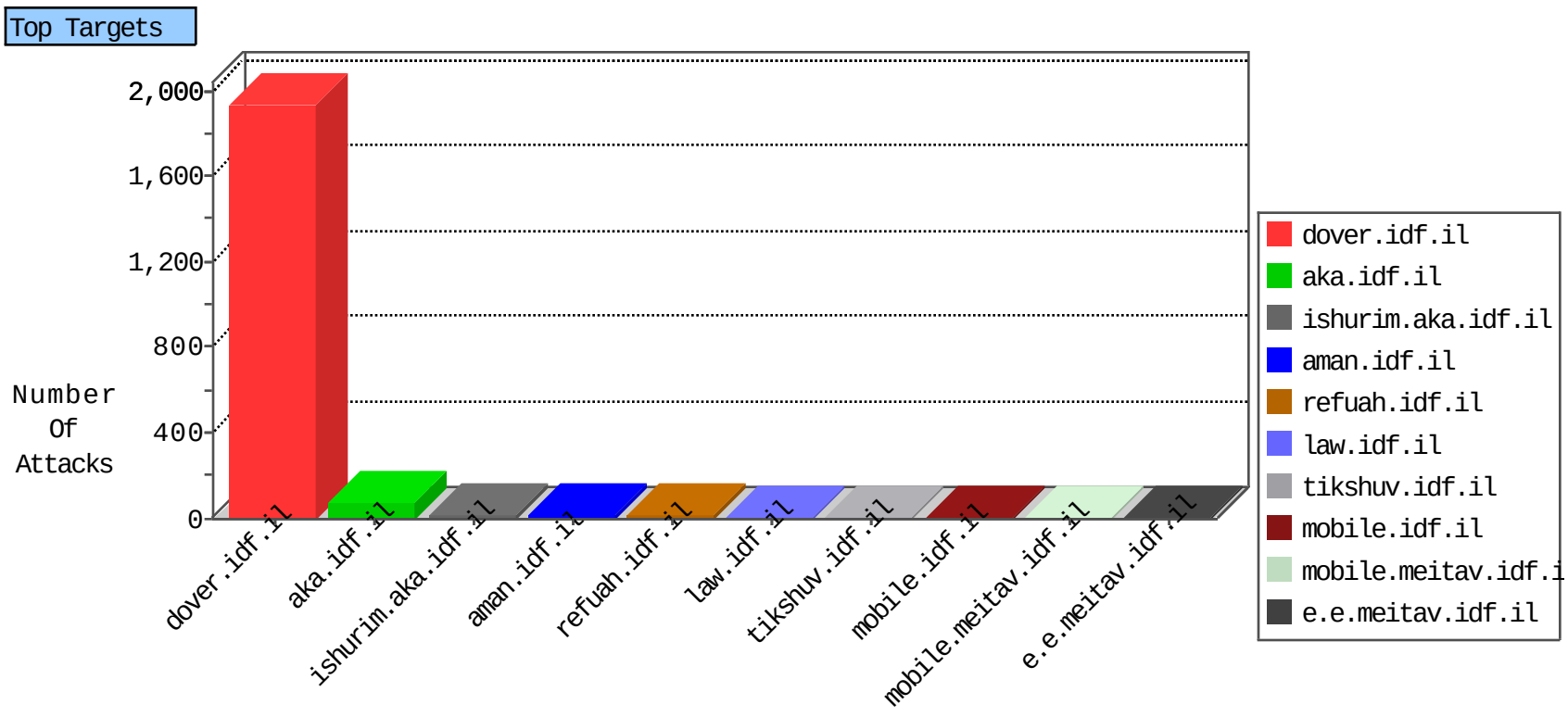
05-07-2015-17:03:06 to 05-07-2015-18:03:06

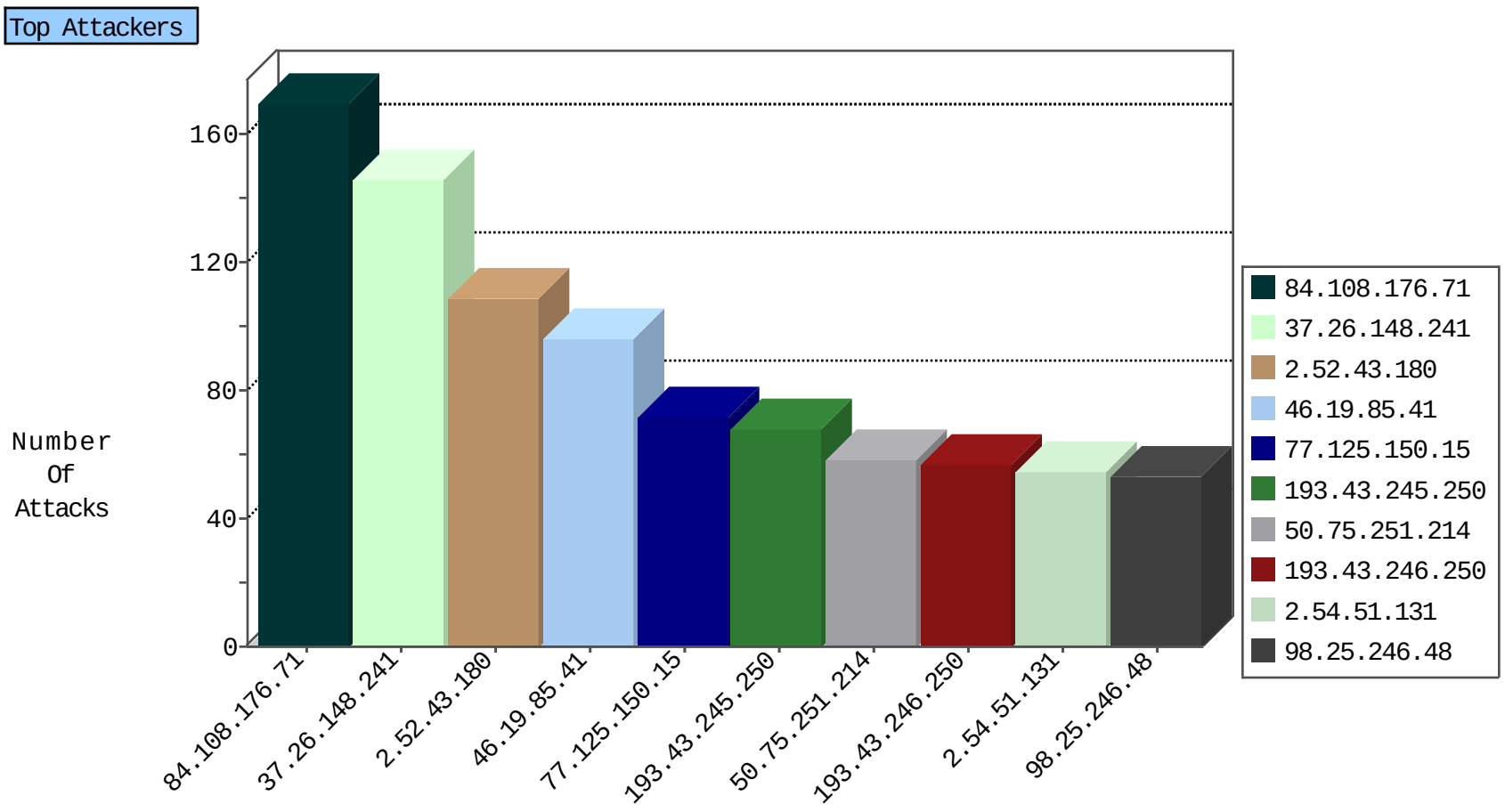
IDF Under Attack
05-07-2015-17:03:06

Top Targets



Top Target

Top Attackers



Top Attackers

05-07-2015-17:03:06 to 05-07-2015-18:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	632
5.29.162.232	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
31.168.64.169	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
5.28.144.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
212.179.28.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
164.138.113.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
109.66.19.29	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
62.219.99.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.80.128.9	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
31.168.241.249	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
10.0.0.7		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.27.132	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
62.219.245.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.117.244.229	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.115.248.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-07-2015-17:03:06 to 05-07-2015-18:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	30
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	11
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	2
2.54.162.125	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	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
62.210.254.239	France	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
5.196.1.129	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.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
69.159.112.159	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.214.11.209	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
37.142.73.52	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.50	e.tikshuv.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
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1

05-07-2015-17:03:06 to 05-07-2015-18:03:06

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	3
208.80.155.214	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
46.116.219.196	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
203.194.234.109	Hong Kong	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.59.84	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
201.239.118.143	Chile	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
61.160.224.130	China	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.130	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.19.107.114	Poland	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
176.12.146.6	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.245	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
93.173.169.124	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.245	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
89.139.161.124	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.245	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
82.232.173.139	France	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
203.194.234.109	Hong Kong	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
79.182.32.75	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
203.113.9.143	Thailand	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
79.180.204.233	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
201.239.118.143	Chile	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
61.160.224.130	China	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.138.9.51	Germany	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.245	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.241	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.245	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.189.245	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
93.172.11.168	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.189.245	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
85.65.34.199	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
81.200.91.2	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1

05-07-2015-17:03:06 to 05-07-2015-18:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.108.176.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	169
37.26.148.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	145
2.52.43.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109
46.19.85.41	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	96
77.125.150.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
50.75.251.214	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
193.43.246.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
193.43.245.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
2.54.51.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
98.25.246.48	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
94.159.150.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
2.54.22.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
194.90.83.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
94.159.167.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
208.87.234.180	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
85.65.34.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
80.83.99.125	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
87.68.54.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
194.90.66.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
212.179.28.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
185.32.177.116	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
2.54.22.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
88.74.200.180	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
193.43.245.250	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
107.77.89.30	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
83.244.109.234	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
62.219.99.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
192.114.91.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
37.142.215.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
192.118.30.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
62.219.138.117	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
46.19.86.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
80.178.11.148	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
46.19.86.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
84.95.255.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
69.159.112.159	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
109.253.139.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.19.85.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
178.215.112.238	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
93.173.225.87	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
93.172.136.213	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
192.116.190.26	Israel	147.237.72.166	aka.idf.il	Invalid checksum. Packet dropped.	Streaming Engine: TCP Invalid Checksum	drop	6
164.138.113.14	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6

05-07-2015-17:03:06 to 05-07-2015-18:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
109.64.172.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
176.228.12.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
5.9.151.67	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.9.151.67	Block	3
212.116.173.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	Block	2
104.131.210.95		147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
192.241.245.86	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
81.144.138.34	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5174-he/patzar.aspx	Block	1
104.131.210.238		147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
95.86.121.67	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/133-22182he/dover.aspx	Block	1
173.236.25.10	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
62.81.85.102	Spain	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/).html(	Block	1
104.131.210.179		147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (403)	Block	1
84.108.176.71	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/atuda	Block	1
66.249.78.134	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	1
5.29.27.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
104.131.217.26		147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
104.131.193.87		147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
78.47.8.52	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
109.64.187.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
104.131.210.179		147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
209.200.244.57	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
85.64.159.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.148	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
157.55.39.227	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/sitemap/sitemap.aspx	Block	1
37.142.143.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl54.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
107.170.130.41	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
104.131.193.87		147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
79.177.151.219	Israel	147.237.72.166	aka.idf.il	Too Many 403: Response Code per All Sources	Block	1
176.228.148.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.132.255	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
104.131.210.185		147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to 147.237.76.39/	Block	1
85.250.43.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
162.243.17.210	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
62.81.85.102	Spain	147.237.76.31	nakchal.idf.il	Abnormally Long Request request version	Block	1
109.64.6.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.131.193.190		147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
185.32.177.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.172.241.42	Portugal	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
132.72.168.124	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
5.9.151.67	Germany	147.237.77.74	law.idf.il	Illegal Parameter Encoding SearchText in www.law.idf.il/163-6639-he/patzar.aspx	None	1

05-07-2015-17:03:06 to 05-07-2015-18:03:06