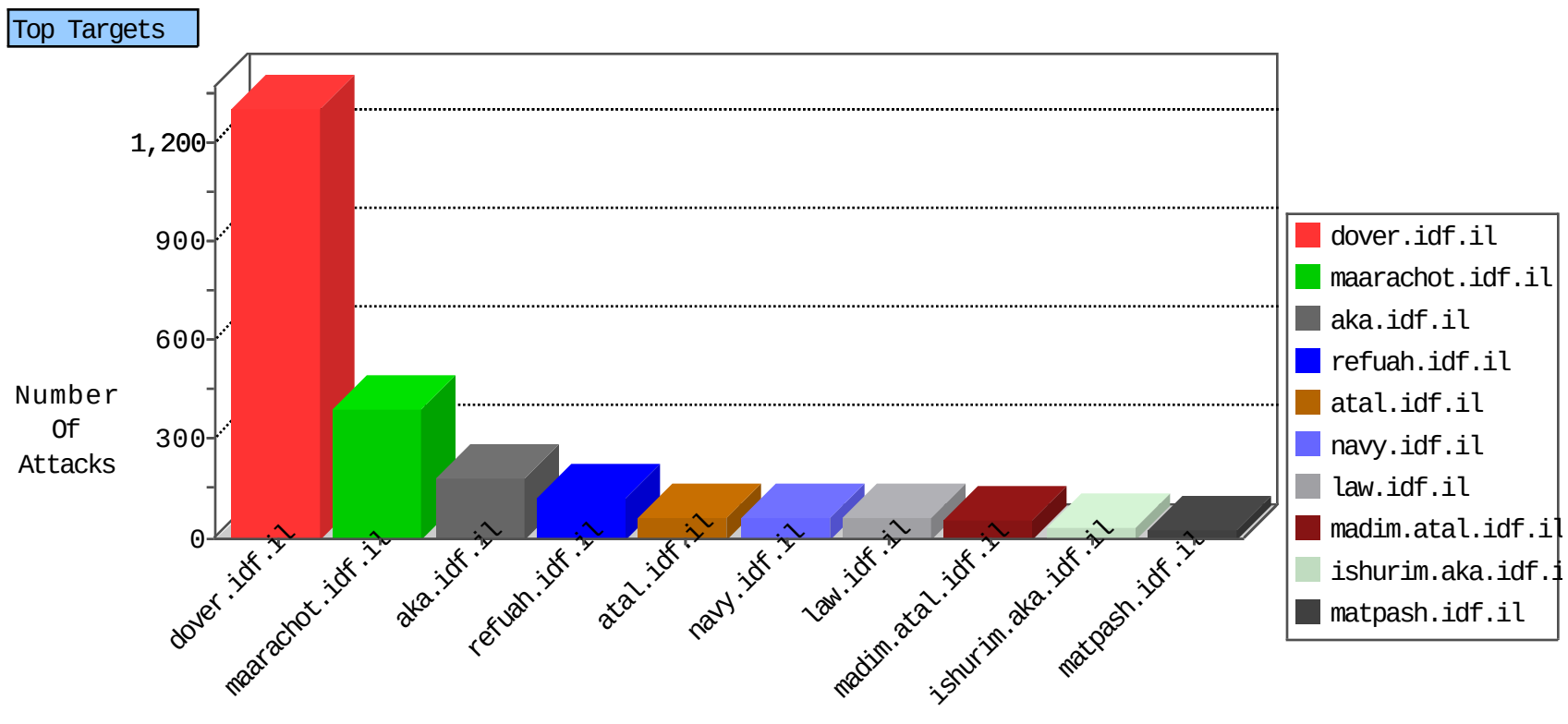
04-13-2015-07:03:04 to 04-13-2015-08:03:04

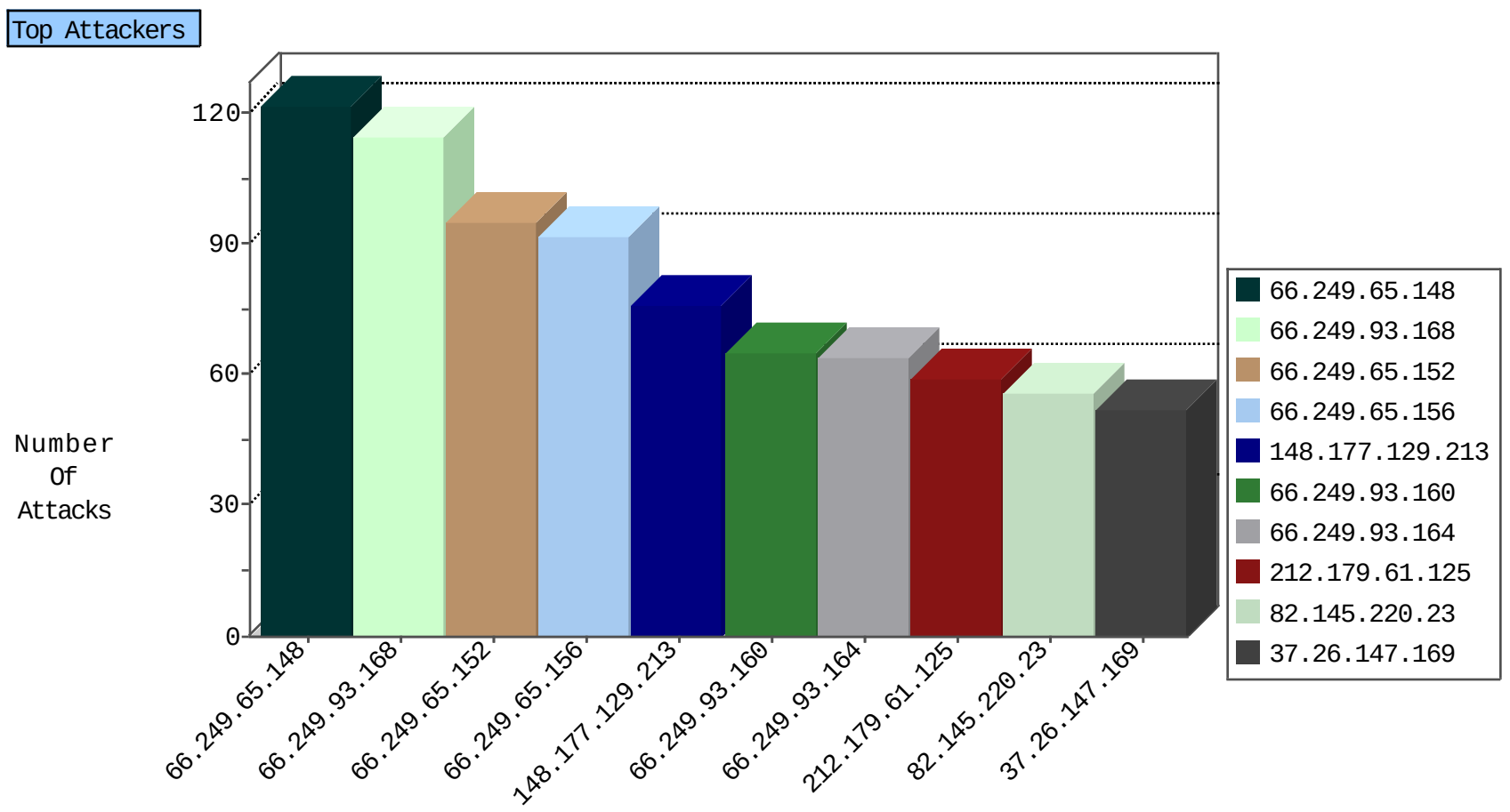
IDF Under Attack
04-13-2015-07:03:04

Top Targets



Top Target

Top Attackers



Top Attackers

04-13-2015-07:03:04 to 04-13-2015-08:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
82.145.220.23	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6982
195.88.130.91	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1115
207.46.13.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1048
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	401
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	260
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	122
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	95
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	92
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	91
37.26.147.148	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	65
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	47
66.249.93.190	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	34
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	32
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	29
66.249.93.168	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.90.86	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	20
66.249.65.191	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	20
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.93.164	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	17
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	17
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.93.194	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	13
66.249.73.201	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.73.132	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.73.140	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
79.180.117.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	7
66.249.90.82	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.73.244	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	7
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.93.172	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.93.186	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	6

04-13-2015-07:03:04 to 04-13-2015-08:03:04

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	23
2.70.180.93	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.182	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.43.94	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1

04-13-2015-07:03:04 to 04-13-2015-08:03:04

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	6
195.88.130.91	Sweden	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.88.130.91	Sweden	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS Wordpress timthumb look-alike domain list RFI	4
195.88.130.91	Sweden	147.237.77.216	dover.idf.il	SERVER-WEBAPP Wordpress timthumb.php theme remote file include attack attempt	4
221.235.188.210	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
183.60.106.175	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
144.76.93.118	Germany	147.237.72.156	aman.idf.il	WEB-CGI redirect access	1
107.178.214.66	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
221.235.188.210	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.210	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.106.175	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
107.178.214.66	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
107.178.214.66	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.210	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
80.55.55.59	Poland	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1

04-13-2015-07:03:04 to 04-13-2015-08:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
148.177.129.213	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	75
212.179.61.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
37.26.147.169	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
176.12.137.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
82.145.220.23	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
79.180.117.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
178.8.76.180	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
5.41.168.60	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
207.241.229.99	United States	147.237.77.216	dover.idf.i	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	27
192.116.108.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
118.71.251.114	Vietnam	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
109.253.143.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
109.253.142.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
85.250.135.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
109.253.132.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
46.19.85.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
115.158.155.192	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
129.94.8.125	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
212.28.230.202	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
195.88.130.91	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
192.118.10.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
212.179.224.96	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
207.46.13.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
2.54.7.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
176.12.139.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
2.54.34.20	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	8
109.253.156.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
2.54.34.20	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	8
80.246.133.89	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
2.52.32.189	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
2.54.34.20	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	8
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.168.65.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
2.52.33.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
37.26.147.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.241.229.99	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.i	SAM rule	drop	drop	5
2.54.130.188	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
2.54.130.188	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
81.218.208.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4

04-13-2015-07:03:04 to 04-13-2015-08:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.78.97.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
92.222.45.62	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
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
114.33.42.185	Taiwan	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
31.168.164.114	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	2
79.182.131.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
92.222.45.62	France	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
54.172.196.207	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
192.116.166.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
112.111.172.185	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/3/3593.pdf/trackback/	Block	1
79.183.27.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$txtSearch in www.aka.idf.il/main/sachar/	None	1
207.46.13.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1226-2.stm	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.30.240.46	United States	147.237.76.30	himush.idf.il	Illegal HTTP Version	Block	1
195.88.130.91	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
114.33.42.185	Taiwan	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
80.179.188.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
171.96.181.224	Thailand	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
95.86.88.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
195.88.130.91	Sweden	147.237.77.216	dover.idf.il	EXPDB-17602:WordPress-TimThumb-Plugin-RCE	Block	1
84.110.214.151	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/terms.aspx	None	1
171.96.181.224	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
104.193.9.233		147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/592-6584-en/patzar.aspx/trackback/	Block	1
79.179.16.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
195.88.130.91	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-10574-en/dover.aspx&amp	Block	1
85.250.161.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.19.85.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
188.138.17.205	France	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
109.160.254.40	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1

04-13-2015-07:03:04 to 04-13-2015-08:03:04