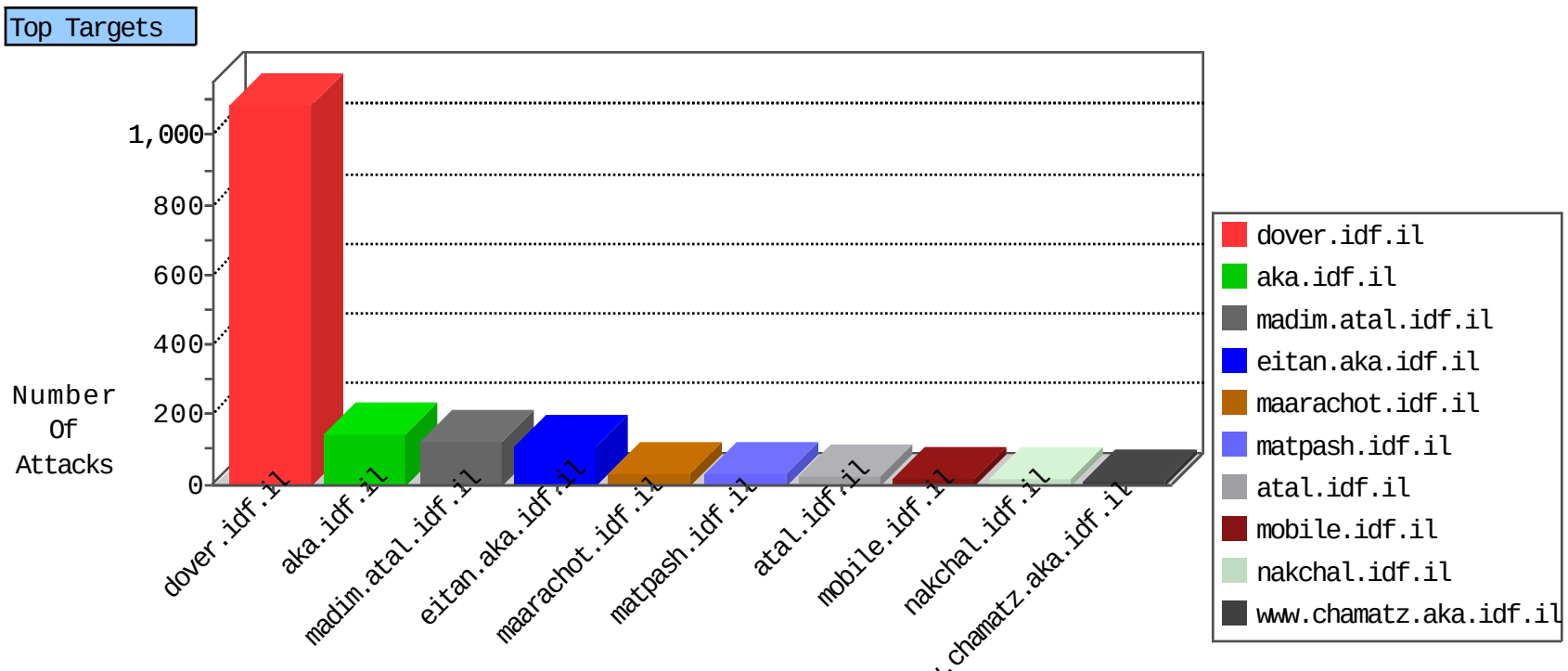
04-30-2016-17:04:01 to 04-30-2016-18:04:01

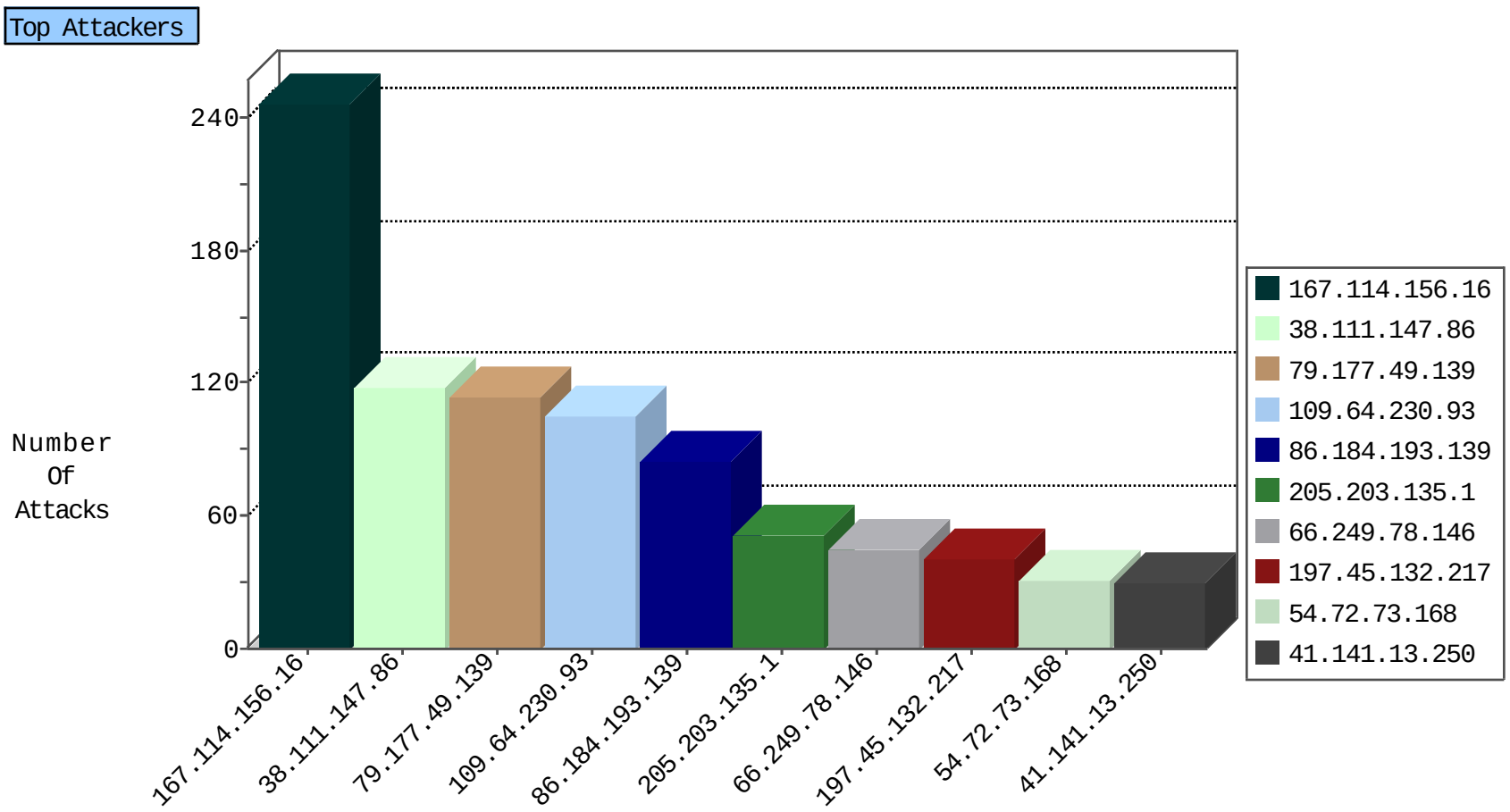
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-30-2016-17:04:01 to 04-30-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	39560
198.58.102.49	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4137
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2828
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2283
196.149.10.61	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1479
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1364
46.105.110.34	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	626
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	353
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	56
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	41
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
46.121.85.238	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.102.52.10	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
156.198.61.75	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-30-2016-17:04:01 to 04-30-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-30-2016-17:04:01 to 04-30-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
78.63.82.209	147.237.77.74	Lithuania	law.idf.il	Xenu Link Sleuth User Agent	1
76.181.249.213	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
212.98.189.183	147.237.77.170	Belarus	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
66.240.213.93	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
212.98.189.183	147.237.77.170	Belarus	maarachot.idf.il	ET SCAN NMAP -f -sS	1
58.218.204.211	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
203.86.29.220	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.12.175	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
184.80.10.136	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
106.184.2.29	147.237.77.170	Japan	maarachot.idf.il	ET SCAN Potential SSH Scan	1
76.181.249.213	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
212.98.189.183	147.237.77.170	Belarus	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
58.218.204.211	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
203.86.29.220	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.12.175	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
198.20.69.74	147.237.77.74	United States	law.idf.il	ET DROP Dshield Block Listed Source	1
45.32.12.175	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
184.80.10.136	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

04-30-2016-17:04:01 to 04-30-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.230.93	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
86.184.193.139	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	41
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.141.13.250	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
217.132.115.243	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
196.149.10.61	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
83.134.73.228	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.117.255.135	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.112.196.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.117.255.135	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
196.149.255.194	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.102.254.134	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
175.106.22.23	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.137.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.7.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.121	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.232.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.64.137.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.177.232.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.108.32.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.106	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4

04-30-2016-17:04:01 to 04-30-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.49.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
5.29.54.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.48.219	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
109.253.131.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.32.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	NULL Character in Method	Block	1
84.111.184.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
46.19.85.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
149.78.7.173	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.16.209.177	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /skin/error.php	Block	1
176.228.67.35	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
85.64.137.198	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
51.255.65.32	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
157.55.39.251	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	1
77.237.146.28	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
64.16.209.177	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /skin/error.php	Block	1
176.228.137.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.54.230	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
87.70.87.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
52.12.99.95	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1133-he/dover.aspx parameter PageNum	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
64.16.209.177	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /skin/error.php	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16648-en/dover.asp	Block	1
37.142.64.96	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
105.157.165.234	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
54.212.115.207	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1133-he/dover.aspx parameter PageNum	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
64.16.209.177	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /skin/error.php	Block	1
46.19.85.11	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1559-he/atal.aspx	Block	1
62.90.164.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1

04-30-2016-17:04:01 to 04-30-2016-18:04:01