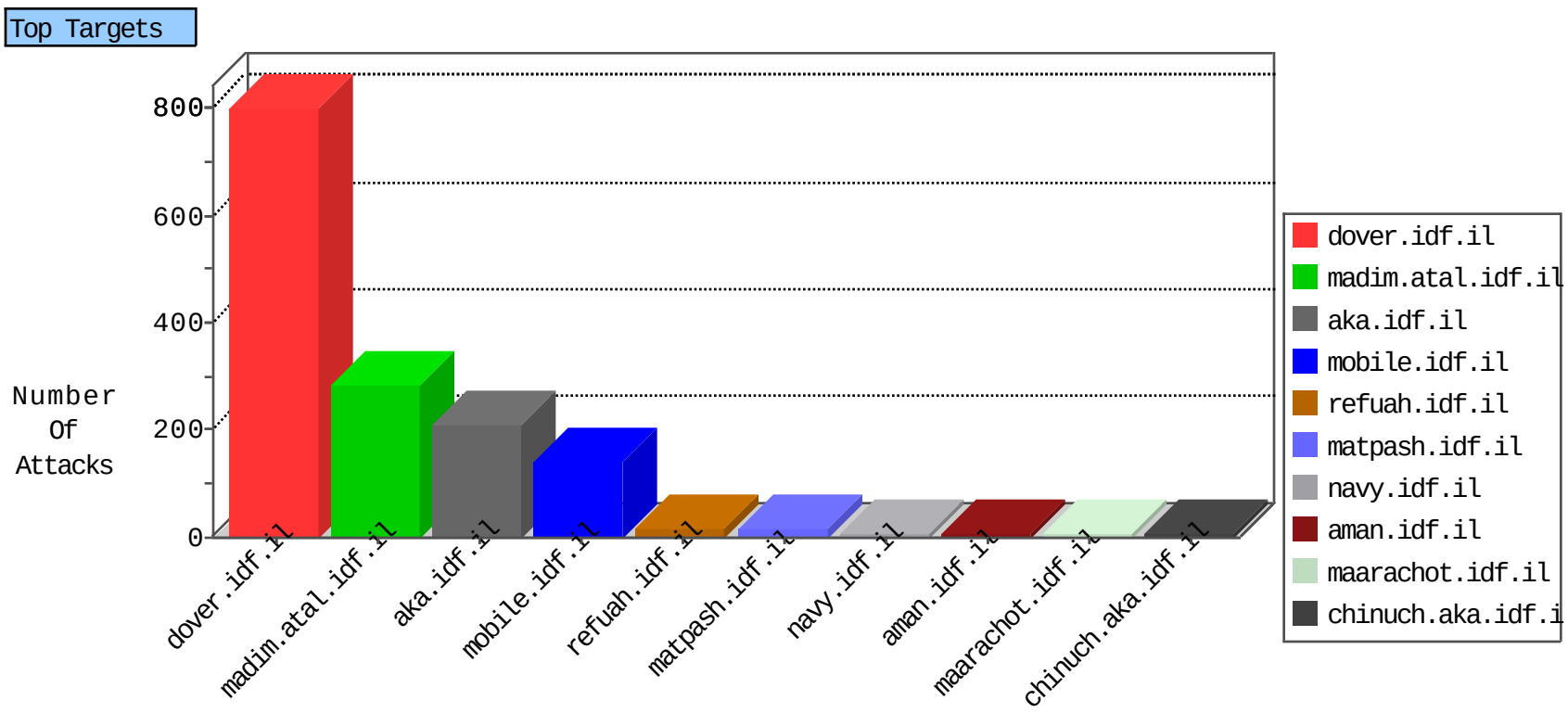
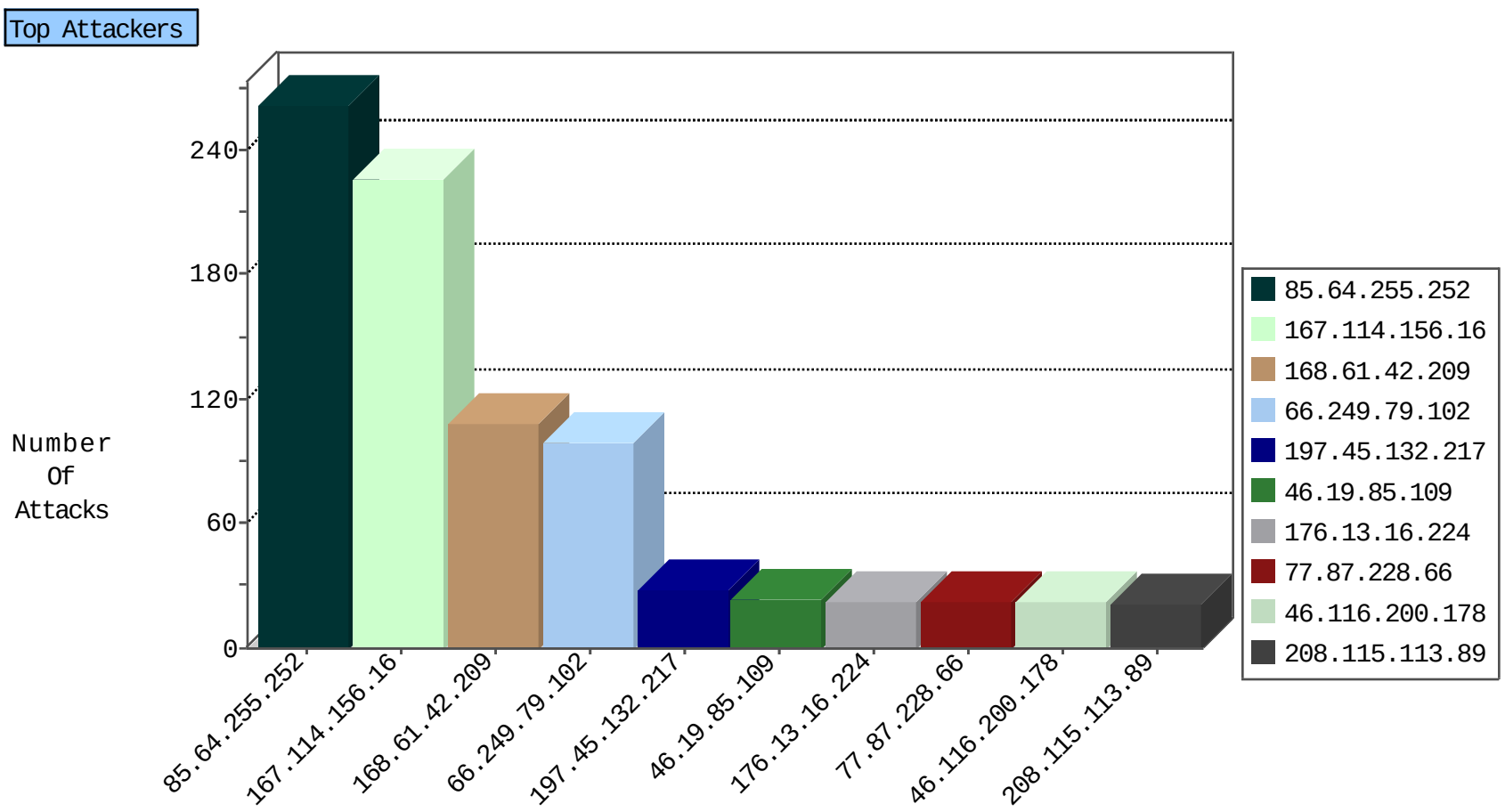
04-29-2016-17:04:00 to 04-29-2016-18:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-29-2016-17:04:00 to 04-29-2016-18:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.161	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30122
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	8409
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1837
84.108.244.204	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	105
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
69.248.129.181	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
71.227.229.178	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-29-2016-17:04:00 to 04-29-2016-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-17:04:00 to 04-29-2016-18:04:00

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	3
66.249.93.243	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	2
85.173.78.61	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
85.173.78.61	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.67.159.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.216.119.94	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
85.173.78.61	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
85.173.78.61	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
85.173.78.61	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.111	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.204.211	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.72.156	United States	aman.idf.il	ET DROP Dshield Block Listed Source	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
111.198.20.146	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
104.219.238.10	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
85.173.78.61	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1

04-29-2016-17:04:00 to 04-29-2016-18:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.61.42.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	99
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
77.87.228.66	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.116.200.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.16.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.146.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.150.193.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.29.93.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.28.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.178.140.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
147.75.208.225	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
69.62.29.111	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.135.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.75.208.224	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
147.75.208.229	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.43.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.29.191	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.24.207.58	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
24.205.183.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
147.75.208.235	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
199.7.131.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.24.207.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.242.40	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
147.75.208.228	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.121.80.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
147.75.208.233	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
89.46.182.240	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.75.208.234	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-29-2016-17:04:00 to 04-29-2016-18:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.255.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	262
2.53.163.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.16.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.182.63.159	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.63.159	Block	4
46.116.200.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
185.3.147.119	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
2.53.28.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.146.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.178.140.110	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.24	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/faq/mobile	Block	3
2.53.147.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.8.204.64	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 213.8.204.64	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
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
131.253.25.153	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.182.128.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/spx	Block	2
65.184.151.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
80.95.38.200	Russian Federation	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ReturnUrl in madim.atal.idf.il/login.aspx	Block	1
66.249.79.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
37.26.148.172	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.96.244	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.70.96.244	Block	1
79.177.145.137	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.64.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
141.212.122.161	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
5.29.57.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
80.246.136.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/newsflash/www.ynet.co.il	Block	1
2.53.43.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.8.204.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/	Block	1
147.75.208.230	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
13.76.128.61	Singapore	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
84.109.206.113	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.118.78.91	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/66846.ppt'	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/instagram.com/idfonline	Block	1
149.78.29.191	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
13.76.128.61	Singapore	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1398-en/dover.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
141.8.132.95	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.124	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
13.76.128.61	Singapore	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
2.53.27.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
87.69.245.45	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8948-he/refuah.aspx	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18863-en/dover.aspx.	Block	1
141.8.183.17	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.161.52	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1

04-29-2016-17:04:00 to 04-29-2016-18:04:00