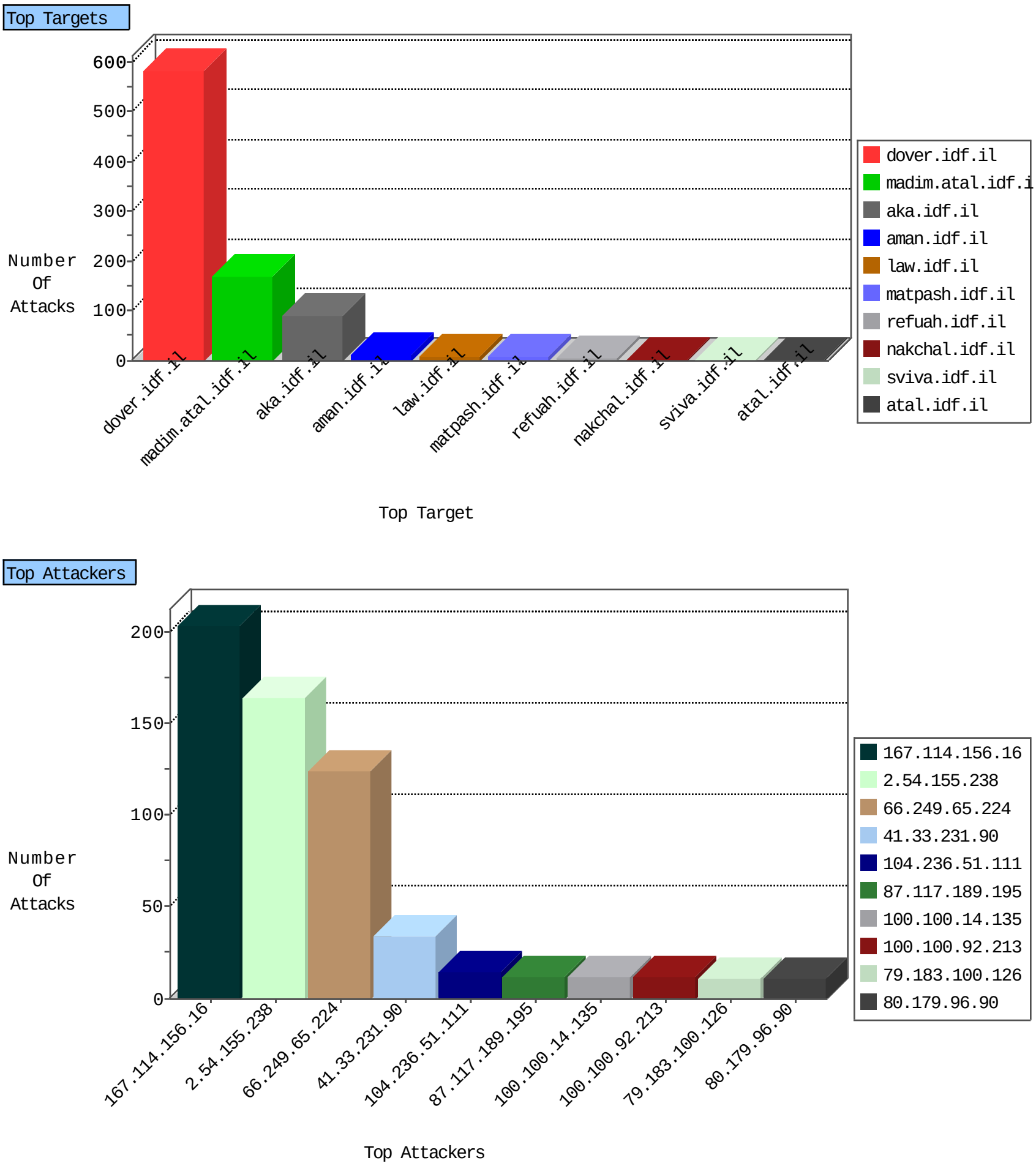
11-21-2015-08:04:09 to 11-21-2015-09:04:09

IDF Under Attack Daily Report



11-21-2015-08:04:09 to 11-21-2015-09:04:09

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	HTTP-POST-Segmented-DoS	dest-reset	16389
46.121.14.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
80.179.96.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
2.54.52.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
166.78.205.55	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

11-21-2015-08:04:09 to 11-21-2015-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-21-2015-08:04:09 to 11-21-2015-09:04:09

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
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 3072	1
74.117.209.136	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
210.50.197.154	147.237.77.178	Australia	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
188.214.128.12	147.237.76.38	Romania	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
27.213.224.213	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.50.197.154	147.237.77.178	Australia	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
188.214.128.12	147.237.76.148	Romania	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1

11-21-2015-08:04:09 to 11-21-2015-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	122
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
104.236.51.111		147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.14.135		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.92.213		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.183.100.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
220.255.98.33	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.179.96.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.122.152		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.46.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.127.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.119.103		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.122	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.132	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.111.110.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
64.246.165.150	United States	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
79.178.58.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.58.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.34.165.218	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
108.61.68.156	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.66.48.136	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
84.109.114.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.255.253.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.142.11	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.244	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.201.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
82.166.103.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
207.46.13.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.201.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.126.151.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

11-21-2015-08:04:09 to 11-21-2015-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.155.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.155.238	Block	105
2.54.155.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
87.117.189.195	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
87.117.189.195	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.117.189.195	Block	5
185.120.126.4		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.120.126.4	Block	3
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.177.50.183	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	2
185.120.126.4		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sahar	Block	2
2.52.133.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.230.224	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.12.141.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.182.198.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.243	Block	2
37.8.25.89	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
104.243.24.177		147.237.72.166	aka.idf.il	E-mail collector robots 14	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmi	Block	1
171.96.176.48	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/3195.pdf	Block	1
2.54.155.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born	Block	1
122.56.234.196	New Zealand	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	1
37.142.238.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
104.243.24.177		147.237.72.166	aka.idf.il	eMail Hoarding	Block	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
109.65.7.139	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3181.pdf	Block	1
87.117.189.195	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.136	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	1
107.150.55.53	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /	Block	1
2.54.26.173	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/4/394.pdf	Block	1
176.13.13.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.7.139	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.65.7.139	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3180.pdf	Block	1
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.122	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.240	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chamatz/kurs/default.asp	None	1
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.111.66	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.54.26.173	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 2.54.26.173	None	1

11-21-2015-08:04:09 to 11-21-2015-09:04:09