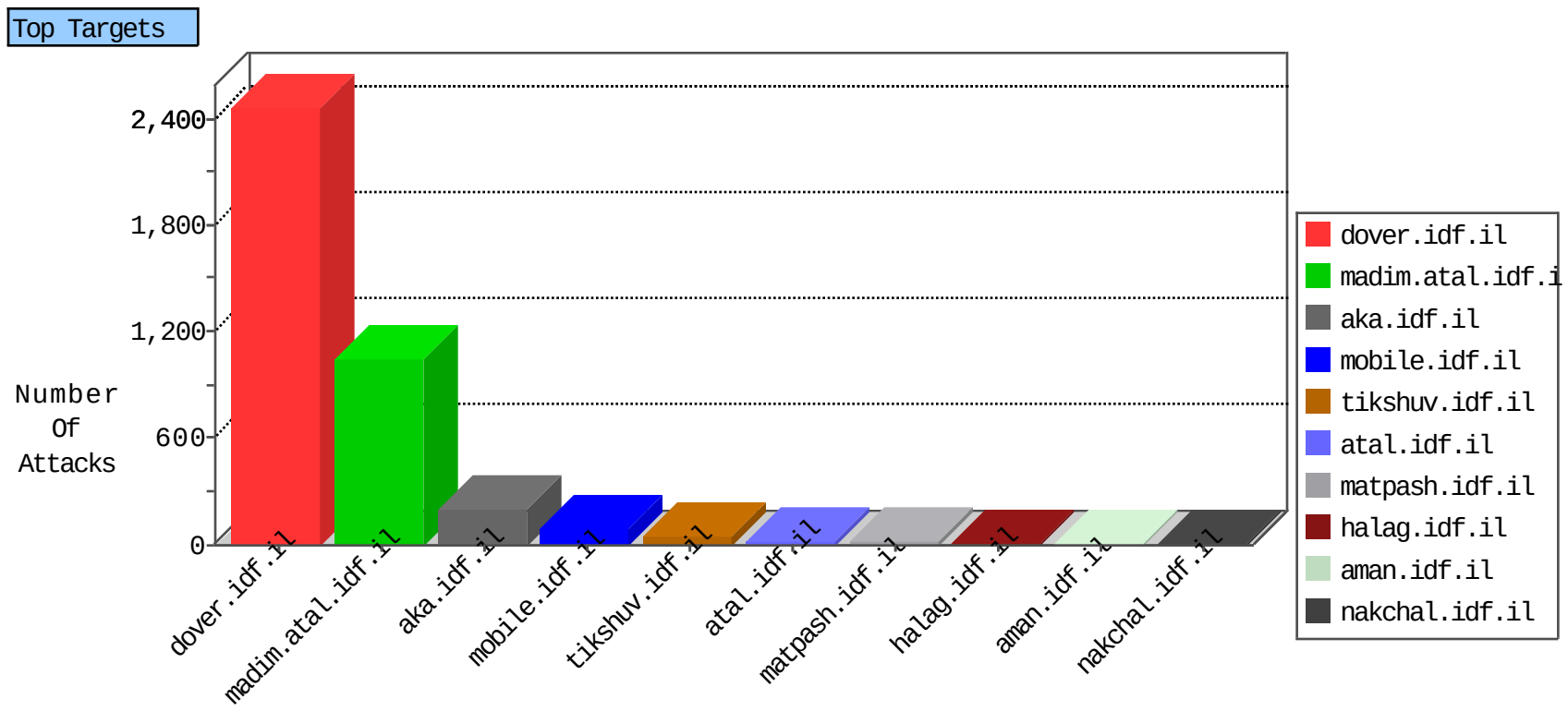
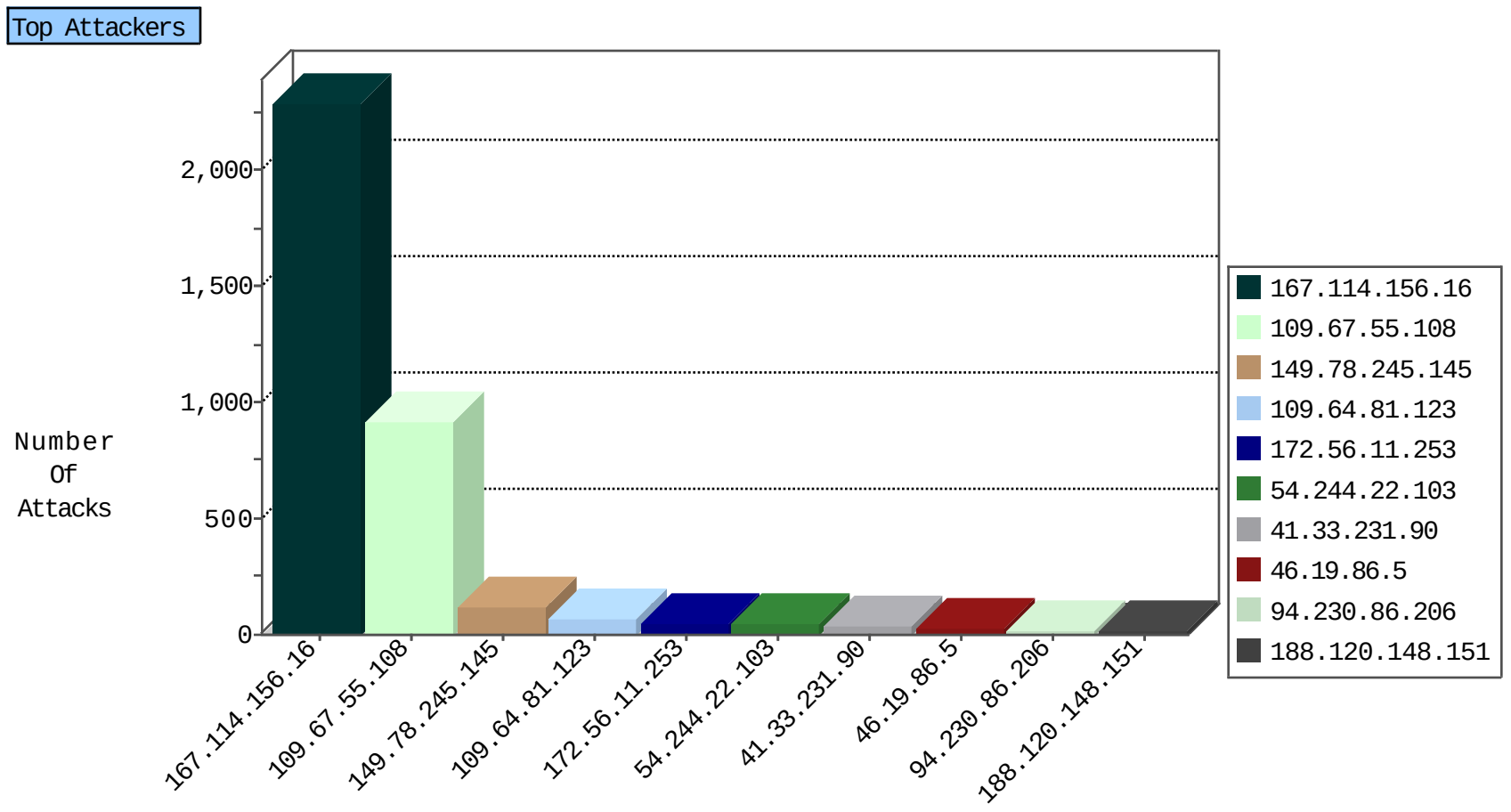
01-26-2016-00:04:08 to 01-26-2016-01:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-26-2016-00:04:08 to 01-26-2016-01:04:08

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	DOS-Tool-SwitchbladG	dest-reset	3036
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
115.230.124.164	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Tcp	drop	2
82.145.33.11	United Kingdom	147.237.76.201	e.atal.idf.il	Block_Ip_Web_In	drop	1
185.56.28.67	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
31.146.178.86	Georgia	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
82.145.33.11	United Kingdom	147.237.76.176	test.ncore.idf.il	Block_Ip_Web_In	drop	1

01-26-2016-00:04:08 to 01-26-2016-01:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.132.195.59	Hungary	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
188.165.15.176	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
208.98.56.66	United States	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

01-26-2016-00:04:08 to 01-26-2016-01:04:08

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
94.76.22.211	147.237.0.35	Bahrain	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.22.211	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
137.117.168.203	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
5.230.134.13	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
137.117.168.203	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.230.134.13	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
134.219.148.12	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
222.174.5.63	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.76.23.173	147.237.0.34	Bahrain	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.23.173	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.77.61	Latvia	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.22.211	147.237.76.38	Bahrain	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
94.76.22.211	147.237.0.34	Bahrain	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
137.117.168.203	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.148.90	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
137.117.168.203	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
5.230.134.13	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
137.117.168.203	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.17.13	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
115.182.17.13	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
222.174.5.63	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.76.23.173	147.237.0.16	Bahrain	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.70.114	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
94.76.23.152	147.237.0.34	Bahrain	tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

01-26-2016-00:04:08 to 01-26-2016-01:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.81.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	34
172.56.11.253	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
176.13.18.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.200.191.38	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
94.230.86.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
188.120.148.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
173.227.183.65	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
149.78.245.145	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
172.58.16.236	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
172.56.11.253	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.60.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.102.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.188.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.20.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.240.192	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.240.192	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
172.56.11.253	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.206	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
100.127.222.66		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
89.139.10.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
89.139.33.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
172.56.11.253	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
31.210.188.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.120.126.35		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.145.95.42	United Kingdom	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.18.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.175.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.107	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
93.172.62.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.151.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.56.11.253	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
31.210.187.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.205.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

01-26-2016-00:04:08 to 01-26-2016-01:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	479
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	241
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	193
149.78.245.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.169	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	6
176.13.18.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.18.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.138.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.154.155.4	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 31.154.155.4	Block	2
109.67.126.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.65.13.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.12.251.37	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17802-he/dover.aspx	Block	1
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
109.163.234.4	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.23.237	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
95.133.163.86	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	1
66.220.156.118	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.72.196.72	Kenya	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
89.139.33.165	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 9 in URL	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
176.13.20.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
41.72.196.72	Kenya	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
2.54.5.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.159.166.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
149.78.245.145	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.168.14.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.182.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.17.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.86.206	Israel	147.237.76.31	nakchal.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 94.230.86.206	Block	1
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	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
46.120.79.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.179	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
31.168.87.204	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
185.107.26.32		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1

01-26-2016-00:04:08 to 01-26-2016-01:04:08