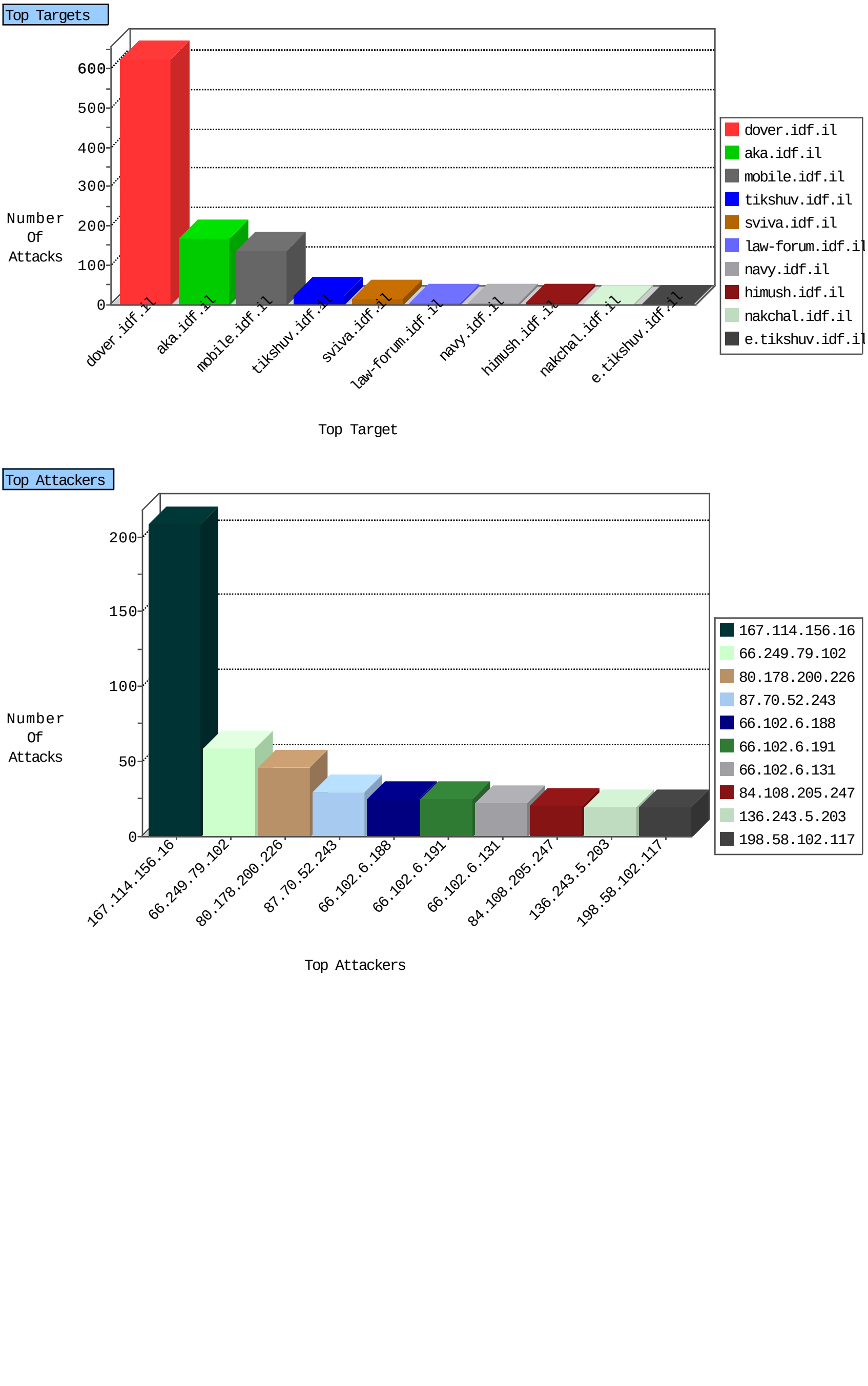
04-29-2016-23:04:05 to 04-30-2016-00:04:05

IDF Under Attack Daily Report



04-29-2016-23:04:05 to 04-30-2016-00:04:05

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	9026
192.249.66.247	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2876
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	983
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
222.186.55.215	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
46.116.254.167	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1

04-29-2016-23:04:05 to 04-30-2016-00:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-23:04:05 to 04-30-2016-00:04:05

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
109.65.25.239	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	3
109.65.25.239	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
66.249.79.102	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
89.248.167.131	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
82.114.83.166	147.237.77.227	Albania	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.225	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
82.114.83.166	147.237.0.15	Albania	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
104.219.238.10	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
84.108.190.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.67.1.225	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
82.114.83.166	147.237.0.34	Albania	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
200.77.10.241	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.245.192.184	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
174.37.194.144	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1
109.65.25.239	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	1
106.184.3.122	147.237.77.235	Japan	sviva.idf.il	ET WEB_SERVER Poison Null Byte	1

04-29-2016-23:04:05 to 04-30-2016-00:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
80.178.200.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.102.6.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.102.6.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.102.6.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
94.13.162.90	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
84.108.205.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
37.237.136.32	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
93.172.4.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
217.237.89.26	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.3.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.44	United States	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
188.161.113.230	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.99.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.137.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.225.131.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.181.4.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.51.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.55.158.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.147.162	Israel	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
80.179.184.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
146.185.35.148	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.39.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.138.103.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.121.245.13	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.180.123.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.101.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.161.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

04-29-2016-23:04:05 to 04-30-2016-00:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.200.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
84.108.205.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
93.172.4.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.179.184.165	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.234	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Malformed URL ¸[[#20]]¸	Block	1
95.25.72.62	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#24]]Î\‹¤Åd#Êüýv•ô…, ©0ôÆGmòh{ÑhÌÕpbª[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À in URL ¸[[#20]]¸	Block	1
5.22.130.81	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#24]]Î\‹¤Åd#Êüýv•ô…, ©0ôÆGmòh{ÑhÌÕpbª[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
85.64.232.75	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 106.184.3.122	Block	1
103.55.24.163	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 103.55.24.163	Block	1
46.120.204.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
109.65.25.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
87.69.245.45	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Multiple NULL Character in Method from 106.184.3.122	Block	1
103.55.24.163	Hong Kong	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
80.246.137.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
109.65.25.239	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Illegal HTTP Version	Block	1
90.230.143.235	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
66.249.79.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/69042.pdf	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	NULL Character in Header Name at [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Abnormally Long Request method	Block	1
84.108.95.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
66.249.66.54	Israel	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Malformed HTTP Header Line 1	Block	1
79.180.121.13	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#24]]Î\‹¤Åd#Êüýv•ô…, ©0ôÆGmòh{ÑhÌÕpbª[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
2.55.158.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
106.184.3.122	Japan	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1

04-29-2016-23:04:05 to 04-30-2016-00:04:05