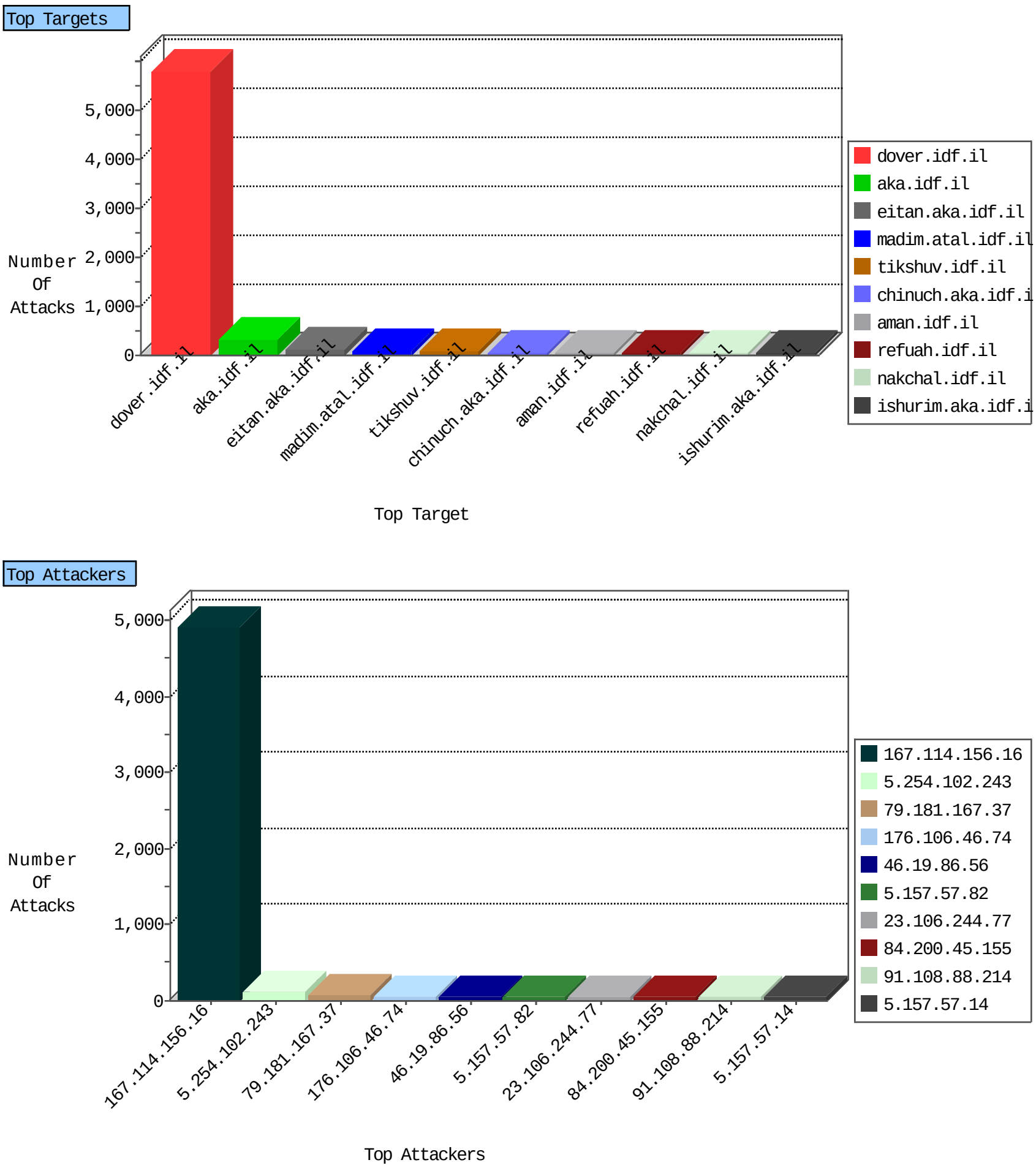
04-21-2016-09:04:04 to 04-21-2016-10:04:04

IDF Under Attack Daily Report



04-21-2016-09:04:04 to 04-21-2016-10:04:04

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	1299
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	470
46.117.124.89	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
213.151.57.157	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.178.193.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
62.90.163.180	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.55.147.142	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.56.245	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
89.46.102.242	Romania	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
112.78.7.198	Vietnam	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	1
89.46.102.242	Romania	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

04-21-2016-09:04:04 to 04-21-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-09:04:04 to 04-21-2016-10:04:04

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	2
79.176.8.209	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
93.180.66.29	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.228.248.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
67.211.217.131	147.237.77.205	United States	prisha.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.157.57.82	147.237.77.216	Sweden	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
92.82.229.102	147.237.8.28	Romania	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.80.59.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
67.211.217.131	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
64.46.23.242	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1

04-21-2016-09:04:04 to 04-21-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4313
79.181.167.37	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	60
5.254.102.243	Romania	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	57
5.254.102.243	Romania	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	57
91.108.88.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
5.157.57.14	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
5.157.57.45	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
23.106.244.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
84.200.45.10	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
5.157.57.82	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
84.200.45.155	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
23.81.247.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
62.219.137.242	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
144.76.80.151	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.46.39.223	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
1.136.96.239	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
185.89.217.233	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
2.53.128.31	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.89.217.225	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
207.46.13.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	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
80.246.139.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.225.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.89.217.228	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
85.75.79.141	Greece	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
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.143.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.89.217.229	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
5.29.165.139	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.70.55.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.185.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.189.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
124.154.227.229	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.122.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.80.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.232	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6

04-21-2016-09:04:04 to 04-21-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
79.181.181.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
46.19.85.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
62.90.35.105	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	8
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	5
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
192.115.97.253	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	4
207.46.13.118	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
62.90.35.105	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	3
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
109.253.147.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
17.138.55.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templatecontrols/generic/	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.143.80.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/	Block	2
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	2
109.253.212.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
17.138.55.96	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.55.96	Block	2
89.249.221.248	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
192.115.97.253	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	2
132.64.81.172	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
95.110.231.235	Italy	147.237.77.74	law.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#1]]ð5™‹({6@Æh•,§*JÛ[[#14]]<roJ[[#18]]ìQÞžÃaÒ¢s[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
213.8.204.8	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
89.249.221.248	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/3/	Block	1
109.64.9.27	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
95.110.231.235	Italy	147.237.77.74	law.idf.il	Illegal HTTP Version	Block	1
207.46.13.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.129	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.129	Block	1
62.219.137.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
23.106.166.235	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
95.110.231.235	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
95.110.231.235	Italy	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
220.255.148.142	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/16827.jpg	Block	1
109.64.9.27	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.64.9.27	Block	1
95.110.231.235	Italy	147.237.77.74	law.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/120203	Block	1
40.77.167.21	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/news/news.asp	Block	1
95.110.231.235	Italy	147.237.77.74	law.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#1]]ð5™‹({6@Æh•,§*JÛ[[#14]]<roJ[[#18]]ìQÞžÃaÒ¢s[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À in URL ¸[[#20]]¸	Block	1
95.110.231.235	Italy	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
220.255.148.148	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.30.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/7/size220x0/16827.jpg	Block	1
95.110.231.235	Italy	147.237.77.74	law.idf.il	Malformed URL ¸[[#20]]¸	Block	1
2.55.8.164	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.64.207.254	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8847-he/refuah.aspx	Block	1
192.115.97.253	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 192.115.97.253	Block	1
46.18.17.136	Palestinian Territory, Occupied	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/71929-eg/maarachot.aspx	Block	1

04-21-2016-09:04:04 to 04-21-2016-10:04:04