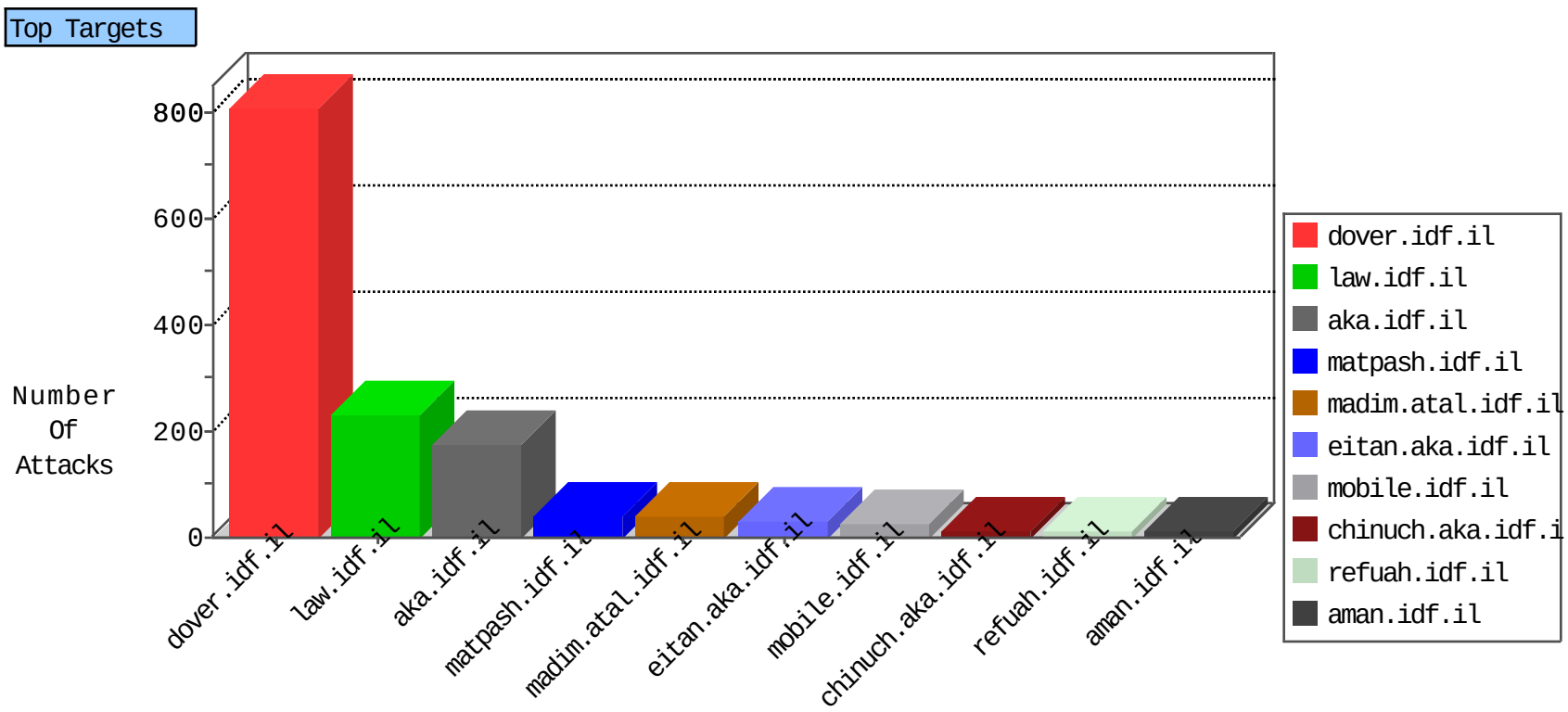
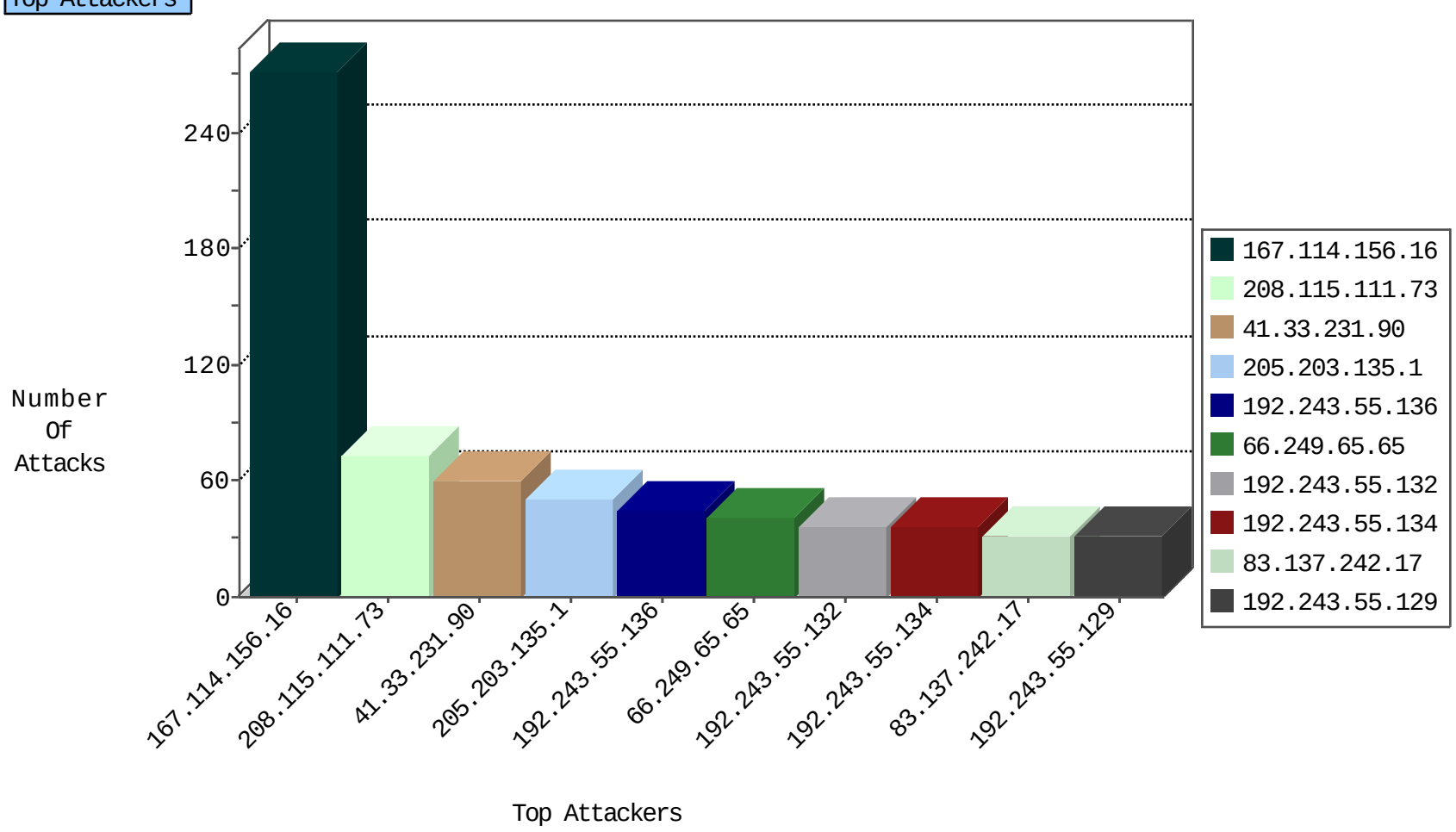
04-22-2016-12:04:09 to 04-22-2016-13:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-22-2016-12:04:09 to 04-22-2016-13:04:09

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	11314
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2909
82.102.252.192	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1603
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	544
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	5
204.42.253.2	United States	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
104.148.71.133	United States	147.237.8.46	e.chinuch.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
61.182.170.38	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
79.181.221.158	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-22-2016-12:04:09 to 04-22-2016-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-22-2016-12:04:09 to 04-22-2016-13:04:09

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
66.249.65.65	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
213.133.131.194	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sA (2)	2
196.203.149.99	147.237.76.39	Tunisia	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
190.124.35.115	147.237.77.74	Nicaragua	law.idf.il	ET SCAN NMAP -sS window 3072	1
190.124.35.115	147.237.77.74	Nicaragua	law.idf.il	ET SCAN NMAP -f -sS	1
146.0.79.211	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
112.198.15.36	147.237.0.17	Philippines	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
76.181.249.213	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
206.210.120.253	147.237.76.147	Canada	chinuch.aka.idf.il	ET WEB_SERVER Poison Null Byte	1
37.142.68.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.203.149.99	147.237.76.39	Tunisia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.246.145	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
190.124.35.115	147.237.77.74	Nicaragua	law.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
115.29.138.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
76.181.249.213	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
61.182.170.38	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
196.203.149.99	147.237.76.39	Tunisia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
23.253.111.228	147.237.77.233	United States	atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

04-22-2016-12:04:09 to 04-22-2016-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
83.137.242.17	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
46.121.74.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
85.64.202.190	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	15
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.0.55	Ireland	147.237.77.216	dover.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	12
79.177.220.93	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.185.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.32.126.61	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
213.6.46.38	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.40.238	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
31.19.16.253	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.43.33	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
157.55.39.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.28.230	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 79.183.28.230	Block	22
176.13.15.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
79.179.211.213	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Days in mobile.idf.il/milluim	Block	7
5.22.135.187	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.22.135.187	Block	5
79.179.211.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	3
176.13.18.13	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/faq/mobile	Block	2
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
108.4.143.45	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
79.179.162.208	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	NULL Character in Header Name at [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
80.178.157.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$hiddenUpdateQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
207.46.13.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
131.253.25.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
79.179.173.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]Õì¯³I<åQ‹!þà'Qò1^h«Þ‡?¬7{•…\[[#19]]…Ó»[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
5.22.135.187	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
192.243.55.137	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-5176-he/patzar.aspxborn-vagabond-where-have-you-been-all-myl-of-these-hitdreamsarticle&r=2&tmpl=blog	Block	1
82.166.244.86	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.121.107.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
207.46.13.186	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/default.asp	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Illegal HTTP Version	Block	1
144.76.27.118	Germany	147.237.0.19	madim.atal.idf.il	Double URL Encoding - parameter: in madim.atal.idf.il/login.aspx?returnurl=%2fdefault.aspx	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
23.253.111.228	United States	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Abnormally Long Request method	Block	1
85.250.254.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
207.241.229.225	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.in.aspx	Block	1
2.53.43.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Malformed HTTP Header Line 1	Block	1
151.80.31.153	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8920-he/refuah.aspx	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]Õì¯³I<åQ‹!þà'Qò1^h«Þ‡?¬7{•…\[[#19]]…Ó»[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À in URL ¸[[#20]]¸	Block	1
45.32.239.214	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/jpg/image.jpg	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in Header Name [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]	Block	1
105.107.197.67	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
220.181.108.139	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Malformed URL ¸[[#20]]¸	Block	1
2.55.159.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
207.46.13.56	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus/general.aspx	Block	1
206.210.120.253	Canada	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]Õì¯³I<åQ‹!þà'Qò1^h«Þ‡?¬7{•…\[[#19]]…Ó»[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1