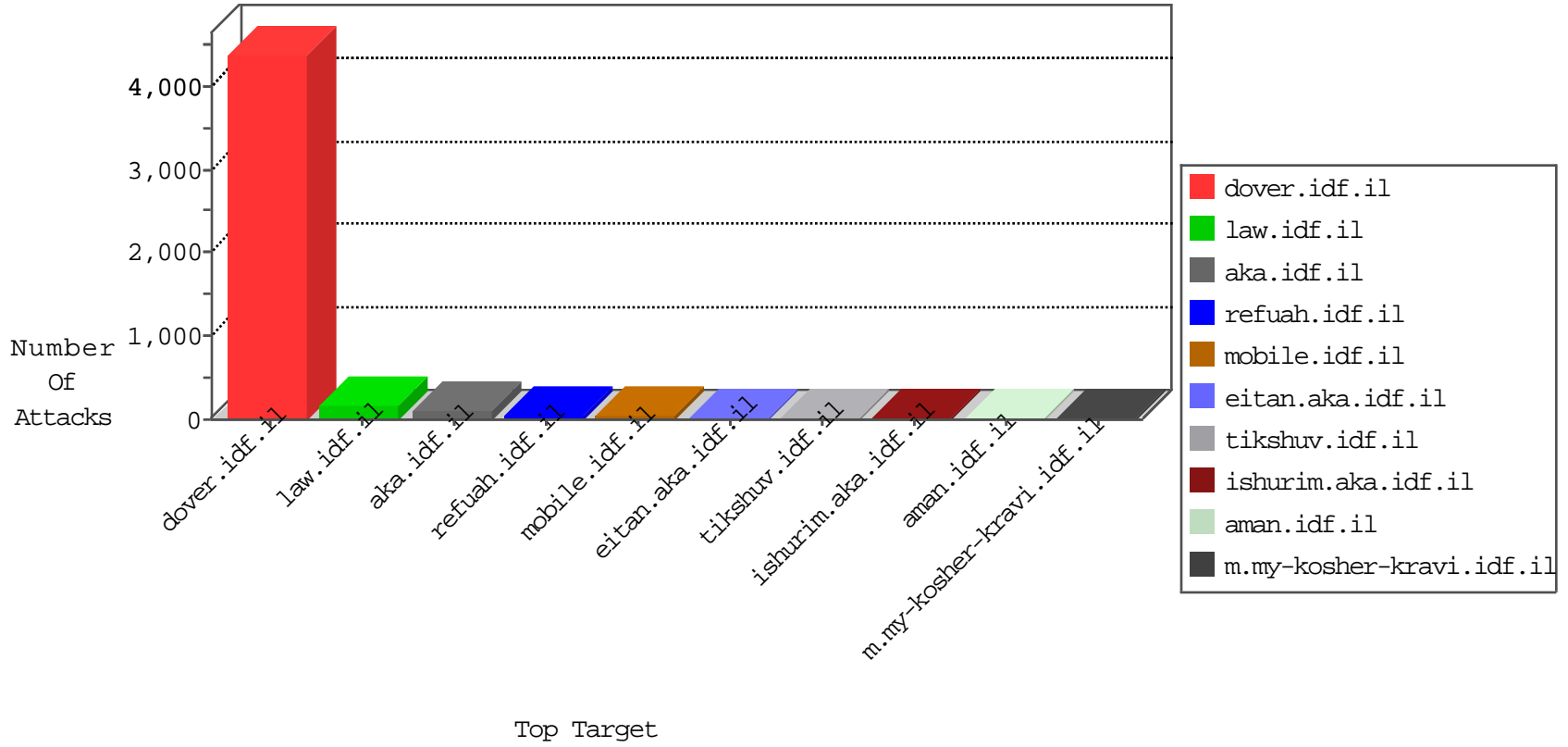


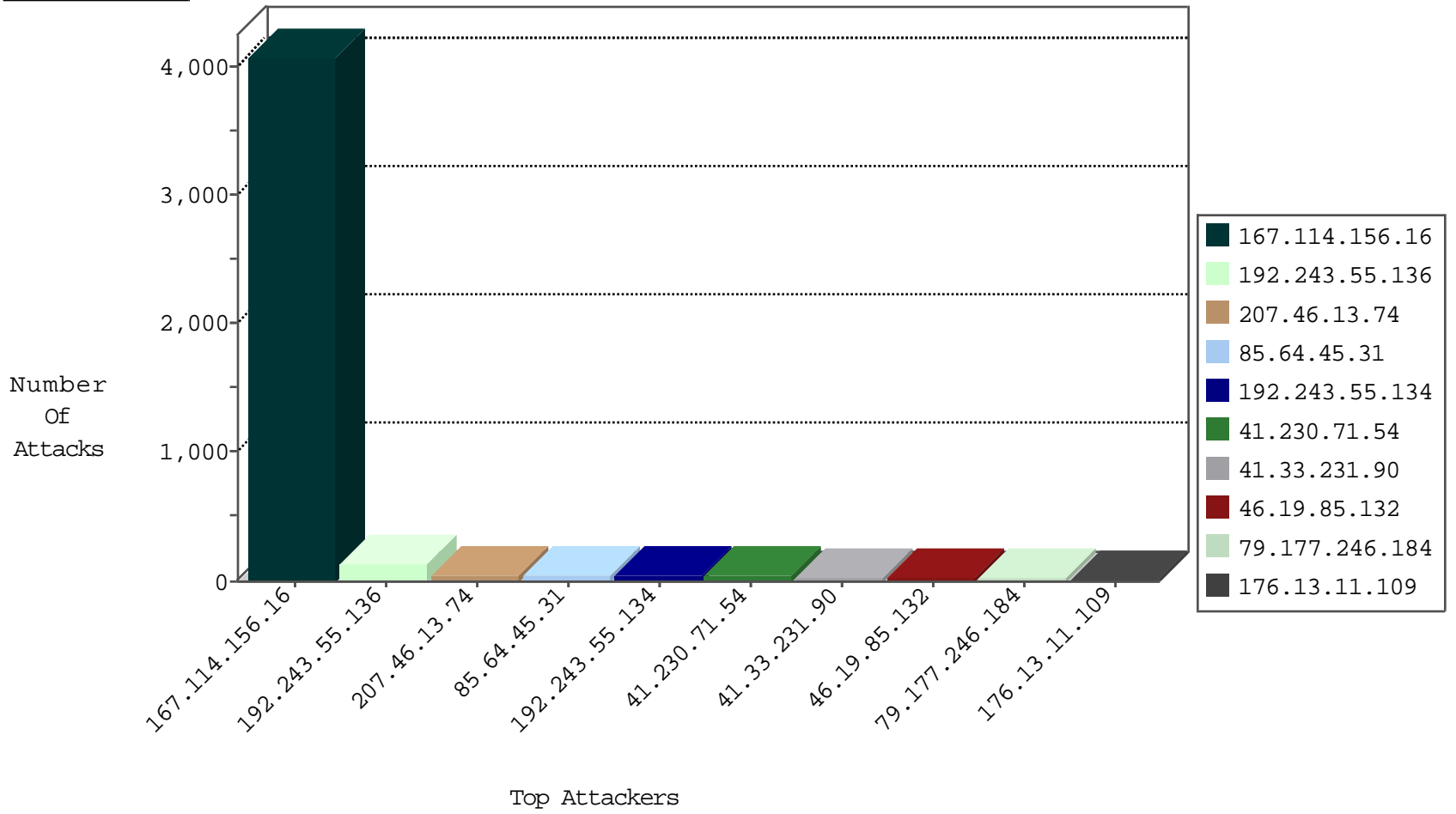
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	Block_Ip_Web_In	drop	4079
84.111.111.152	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30
66.249.93.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17
62.219.34.192	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
46.19.85.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
194.90.244.58	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
41.230.71.54	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
107.150.46.36	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-trafl	forward	2
79.177.246.184	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
85.65.16.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
121.81.217.214	Japan	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
180.102.110.42	China	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
158.130.6.191	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.253.133.61	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.179.174.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
158.130.6.191	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
85.93.89.243	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
31.210.186.41	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
111.225.161.47	China	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
85.93.89.243	Germany	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
61.135.189.98	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
2.55.189.205	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
185.106.92.47	Russian Federation	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
185.106.92.47	Russian Federation	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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
201.222.125.250	147.237.0.35	Bolivia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.103.252.56	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
80.82.78.38	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
31.5.44.33	147.237.0.200	Belgium	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
31.5.44.33	147.237.0.200	Belgium	m4u.idf.il	ET SCAN NMAP -f -sS	1
207.232.55.114	147.237.0.35	Israel	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.101.202.28	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET WEB_SERVER Poison Null Byte	1
185.106.92.47	147.237.0.19	Russian Federation	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
99.95.129.139	147.237.76.177	United States	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.230.71.54	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP admin.php access	1
31.5.44.33	147.237.0.200	Belgium	m4u.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.74	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	45
85.64.45.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
79.177.246.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.230.71.54	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	17
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.85.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.11.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
37.142.64.10	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.148.145	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.138.19.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.147.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.37.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.130.42.65	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.65.106.134	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.136.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.49	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
85.130.219.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.210.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.86.112	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.102.9.119	United States	147.237.77.234	halag.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
85.130.219.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.136.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
191.185.41.1	Brazil	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.178.48.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.210.186.41	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
79.178.215.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.178.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.74	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	3
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.178.242.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.135.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.230.71.54	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.71.54	Block	7
80.246.136.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
41.230.71.54	Tunisia	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
46.19.85.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
41.230.71.54	Tunisia	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.230.71.54	Block	2
185.32.179.190	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	2
149.78.72.39	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
130.185.155.10	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed HTTP Header Line 2	Block	1
41.230.71.54	Tunisia	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
176.13.0.81	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
89.138.19.165	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]][[#3]][[#3]][[#8]]2w[[#6]] Ó•%w\$y×Yp̄hm~hntÇ+_ 'W° < *	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Header Name	Block	1
130.185.155.10	Sweden	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL [[#20]]	Block	1
107.150.46.36	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
202.191.63.69	Australia	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]][[#3]][[#3]][[#8]]2w[[#6]] Ó•%w\$y×Yp̄hm~hntÇ+_ 'W° < *	Block	1
73.170.84.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in Header Name at [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]] [[#0]]	Block	1
197.40.0.173	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.203.189	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.66.176	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
202.191.63.69	Australia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in URL [[#20]]	Block	1
5.29.1.242	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
157.55.39.118	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.178.48.242	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]][[#3]][[#3]][[#8]]2w[[#6]] Ó•%w\$y×Yp̄hm~hntÇ+_ 'W° < *	Block	1
197.40.63.23	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.147.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal HTTP Version	Block	1
5.39.222.159	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
41.230.71.54	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
198.101.202.28	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1