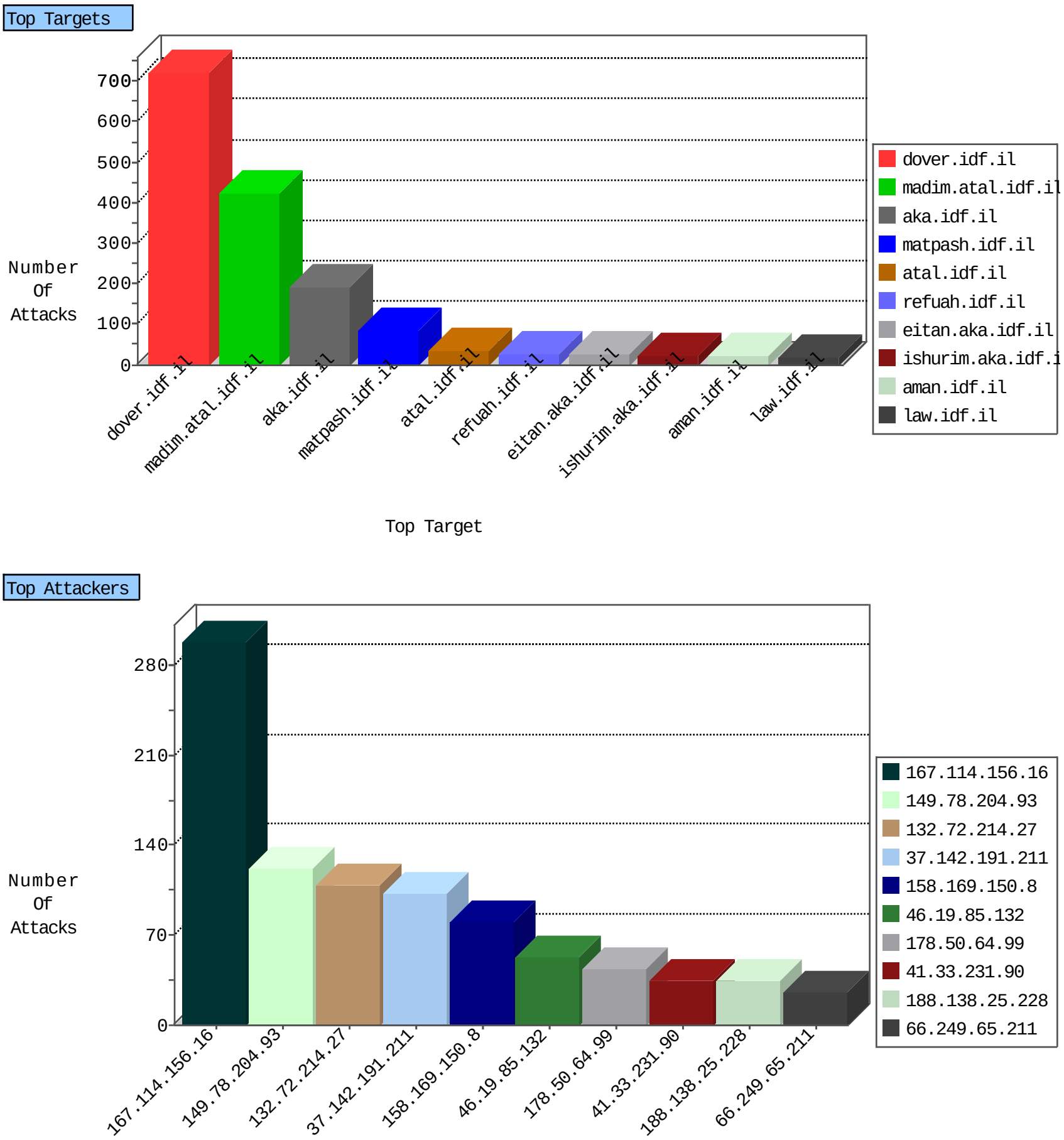
04-21-2016-15:04:05 to 04-21-2016-16:04:05

IDF Under Attack
Daily Report



04-21-2016-15:04:05 to 04-21-2016-16:04:05

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	13267
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3337
122.178.110.253	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	780
66.249.64.233	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	632
84.109.24.109	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	104
79.179.64.204	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
113.240.250.157	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.62.188.15	Netherlands	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
89.46.102.242	Romania	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

04-21-2016-15:04:05 to 04-21-2016-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-15:04:05 to 04-21-2016-16:04:05

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	2
185.130.5.99	147.237.76.176	Lithuania	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
151.24.159.54	147.237.72.166	Italy	aka.idf.il	portscan: TCP Distributed Portscan	1
119.93.229.105	147.237.76.44	Philippines	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.158.255.194	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.131.208.140	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.74	United States	law.idf.il	ET DROP Dshield Block Listed Source	1
66.249.66.9	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
188.138.25.228	147.237.8.46	France	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.117.192.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.99	147.237.77.226	Lithuania	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
13.92.84.22	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.99	147.237.8.24	Lithuania	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
132.72.10.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.191.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.131.208.140	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
213.57.248.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.90.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.94.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.152.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-21-2016-15:04:05 to 04-21-2016-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
158.169.150.8	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	73
178.50.64.99	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
66.249.65.211	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
77.127.92.25	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.111.2.126	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.3.6	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.75.79.141	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.21.65	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	9
85.130.129.245	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
158.169.150.8	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
92.253.21.187	Jordan	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	7
17.138.55.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.4.223	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
176.13.3.6	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.138.249.4	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.130.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.53.161.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.130.129.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.209	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.39	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.138.25.228	France	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
163.247.46.239	Chile	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
163.247.46.239	Chile	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	5
85.130.129.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.67.185.83	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.39	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.65.82.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.116.50.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.177.169.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
188.138.25.228	France	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
89.138.249.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.0.114.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.6.125.178	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.198.151.43	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.204.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
132.72.214.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
37.142.191.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.53.167.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.53.140.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
217.132.41.33	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.41.33	Block	4
37.46.39.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
17.138.55.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templatecontrols/newsflash/www.ynet.co.il	Block	2
5.22.135.169	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 5.22.135.169	Block	2
109.253.156.151	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
66.249.65.211	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.211	Block	2
95.86.119.182	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
95.86.119.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	2
5.22.135.169	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	2
131.253.25.247	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
66.249.78.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
207.46.13.134	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/â€ž	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Malformed URL Úþ1•]]81#[[ügk‡c˙]כ[[42#]]“	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Abnormally Long Request	Block	1
109.65.82.129	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
180.97.106.162	China	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/struts/utils.js	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Header Name	Block	1
147.91.1.43		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.247.139	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
207.46.13.170	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method éû˜.;T˜p›Bïþ[[#22]][[#4]]gÑÚýwª1ïbè*•!RY¹ in URL Úþ1‡c˙]kgù[[#18]]•[[כ#24“]]	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
180.97.106.162	China	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method éû˜.;T˜p›Bïþ[[#22]][[#4]]gÑÚýwª1ïbè*•!RY¹	Block	1
46.19.85.169	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.97.106.36	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/struts/utils.js	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
5.22.135.169	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/homepage/mobile	Block	1
109.253.218.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
193.126.232.142	Portugal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL Úþ1•]]81#[[ügk‡c˙]כ[[42#]]“	Block	1
2.53.4.223	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.215	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/minhalnews/pages/default.aspx	Block	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/struts/utils.js	Block	1
46.19.86.22	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal HTTP Version [[#4]]óåÒ§•.EUÝ@~[[#12]]Ñ	Block	1