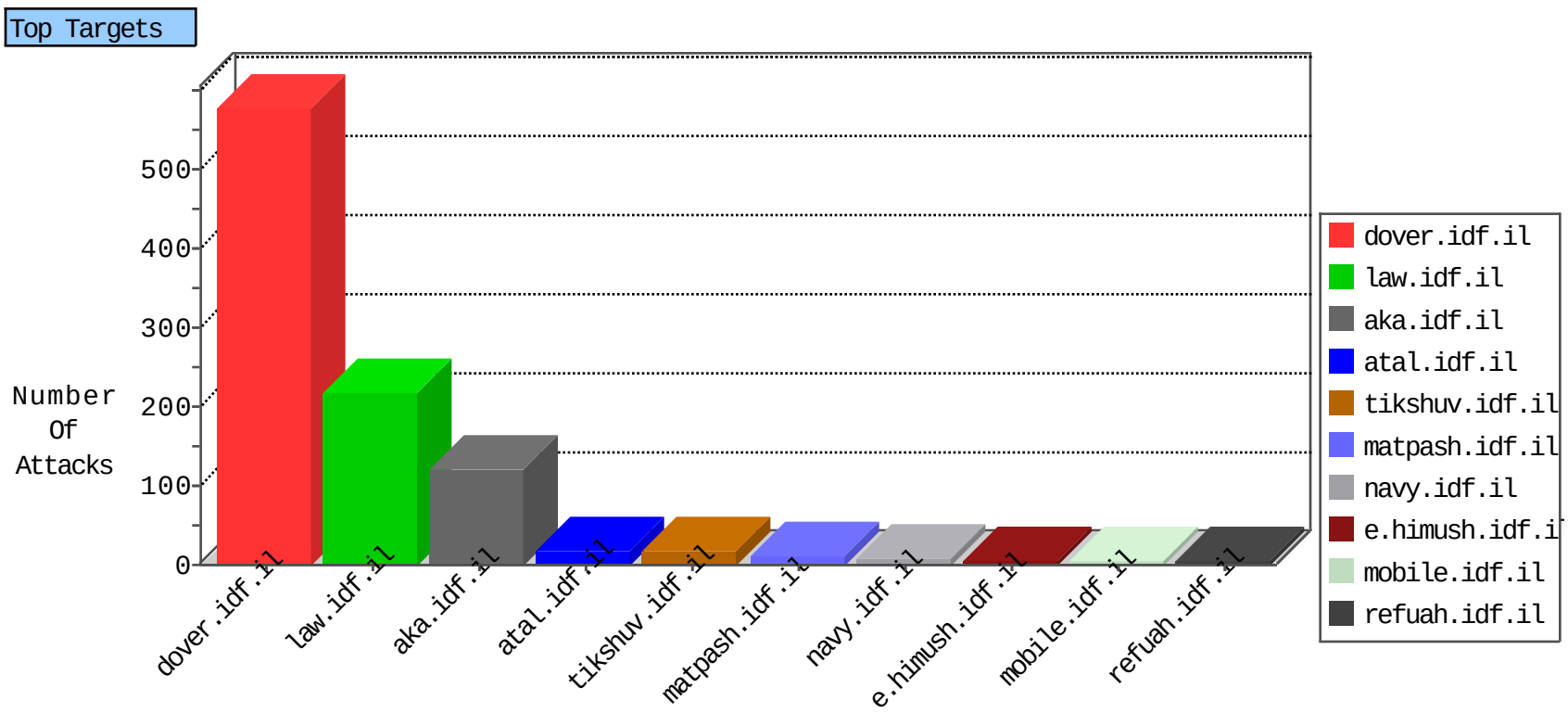
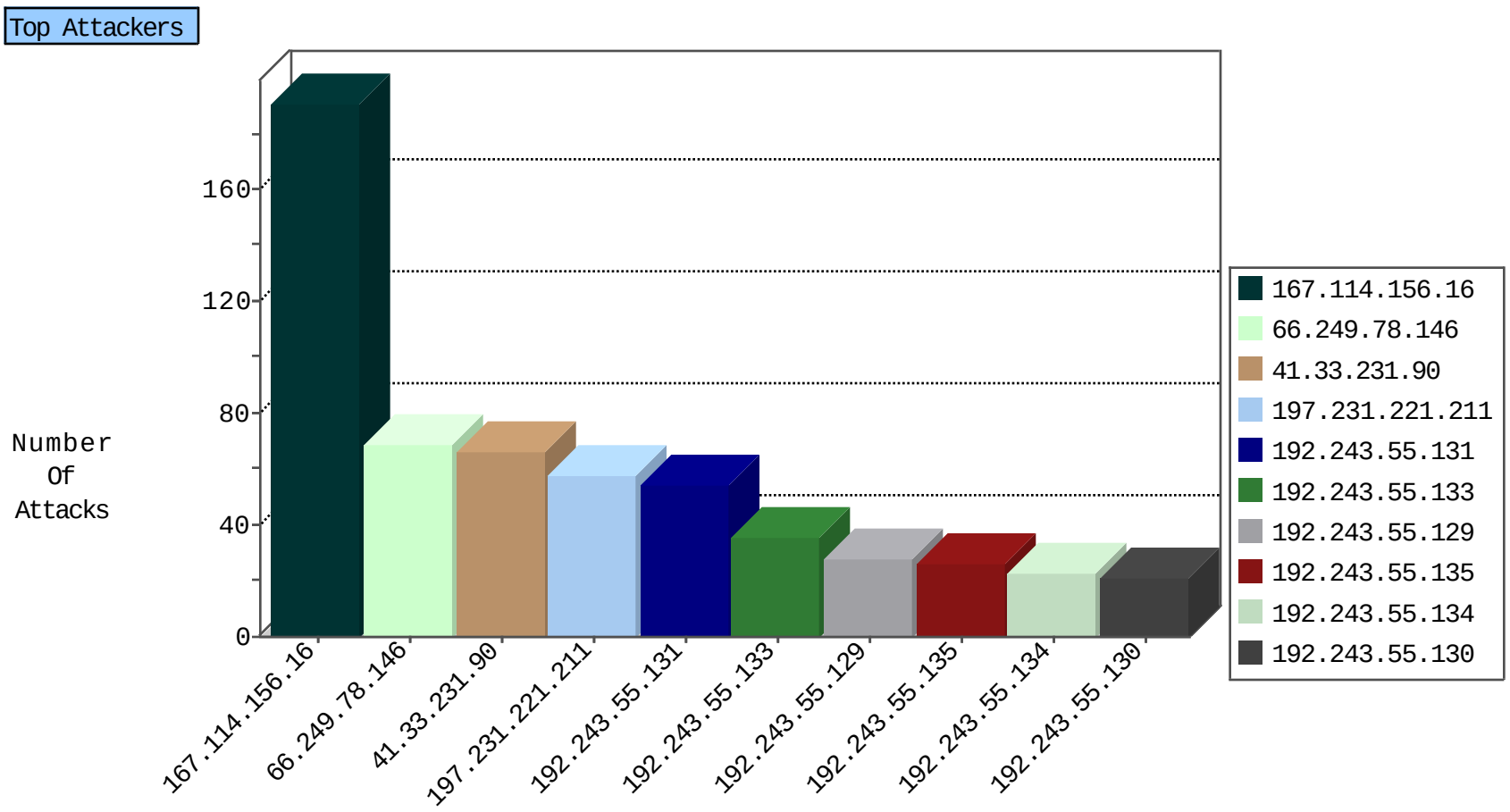
04-23-2016-09:04:06 to 04-23-2016-10:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-23-2016-09:04:06 to 04-23-2016-10:04:06

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	7839
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3350
174.100.20.17	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
94.102.49.116	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

04-23-2016-09:04:06 to 04-23-2016-10:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-09:04:06 to 04-23-2016-10:04:06

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
95.45.254.123	147.237.77.216	Ireland	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
83.149.126.98	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	2
169.54.233.124	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
105.157.40.137	147.237.0.34	Morocco	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
169.54.233.124	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.124	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.216.119.94	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
169.54.233.124	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.124	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.211.11	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
196.203.149.99	147.237.77.19	Tunisia	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
169.54.233.124	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
196.203.149.99	147.237.77.19	Tunisia	law-forum.idf.il	ET SCAN NMAP -f -sS	1
169.54.233.124	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.81.248.101	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.124	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.1.155.46	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
169.54.233.124	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.219.238.10	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
92.27.108.122	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.216.119.94	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.72.217	United States	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.114.36.145	147.237.0.34	United States	tikshuv.idf.il	ET WEB_SERVER Poison Null Byte	1
80.82.78.38	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.45.137.76	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
196.203.149.99	147.237.77.19	Tunisia	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
169.54.233.124	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.54.169	147.237.77.61	France	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-23-2016-09:04:06 to 04-23-2016-10:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
68.180.231.43	United States	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	12
83.149.126.98	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.126.252.12	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	8
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.26.148.157	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.31.140	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
213.244.118.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.87.83.99	United States	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
92.247.181.29	Bulgaria	147.237.77.216	dover.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	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	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	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	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
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
40.77.167.40	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.137	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	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4

04-23-2016-09:04:06 to 04-23-2016-10:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.25.133	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
46.116.187.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	2
173.231.1.80	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
80.230.231.174	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.169	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'_Ç"p#012eˆE¿ØÊ[[#5]]Ñ×@Ê<wEi×#012Õ8—œ[[#12]]£D&,[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
41.86.105.12	South Africa	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
79.181.191.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version	Block	1
66.220.145.243	United States	147.237.72.166	aka.idf.il	Multiple Post Request - Missing Content Type: 'none'	Block	1
192.243.55.129	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/לכתבה המלאה	Block	1
80.230.231.175	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/changelog.txt	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
141.8.132.2	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-5398-en/patzar.aspx.	Block	1
80.230.231.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.220.145.243	United States	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Malformed HTTP Header Line 2	Block	1
197.221.14.66	South Africa	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
85.214.116.128	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'_Ç"p#012eˆE¿ØÊ[[#5]]Ñ×@Ê<wEi×#012Õ8—œ[[#12]]£D&,[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À in URL ¸[[#20]]¸	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Header Name [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]]	Block	1
46.120.135.33	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nav	Block	1
80.230.231.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.220.145.244	United States	147.237.72.166	aka.idf.il	Multiple Post Request - Missing Content Type: 'none'	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Malformed URL ¸[[#20]]¸	Block	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
95.45.254.123	Ireland	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
220.255.148.247	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.37	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'_Ç"p#012eˆE¿ØÊ[[#5]]Ñ×@Ê<wEi×#012Õ8—œ[[#12]]£D&,[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
51.255.202.66	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17748-en/dover.aspx.	Block	1
80.230.231.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.220.145.246	United States	147.237.72.166	aka.idf.il	Multiple Post Request - Missing Content Type: 'none'	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	NULL Character in Header Name at	Block	1
40.77.167.63	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	1
109.253.200.62	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
79.181.191.243	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
209.114.36.145	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
54.243.53.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-12386-en/dover.aspx	Block	1

04-23-2016-09:04:06 to 04-23-2016-10:04:06