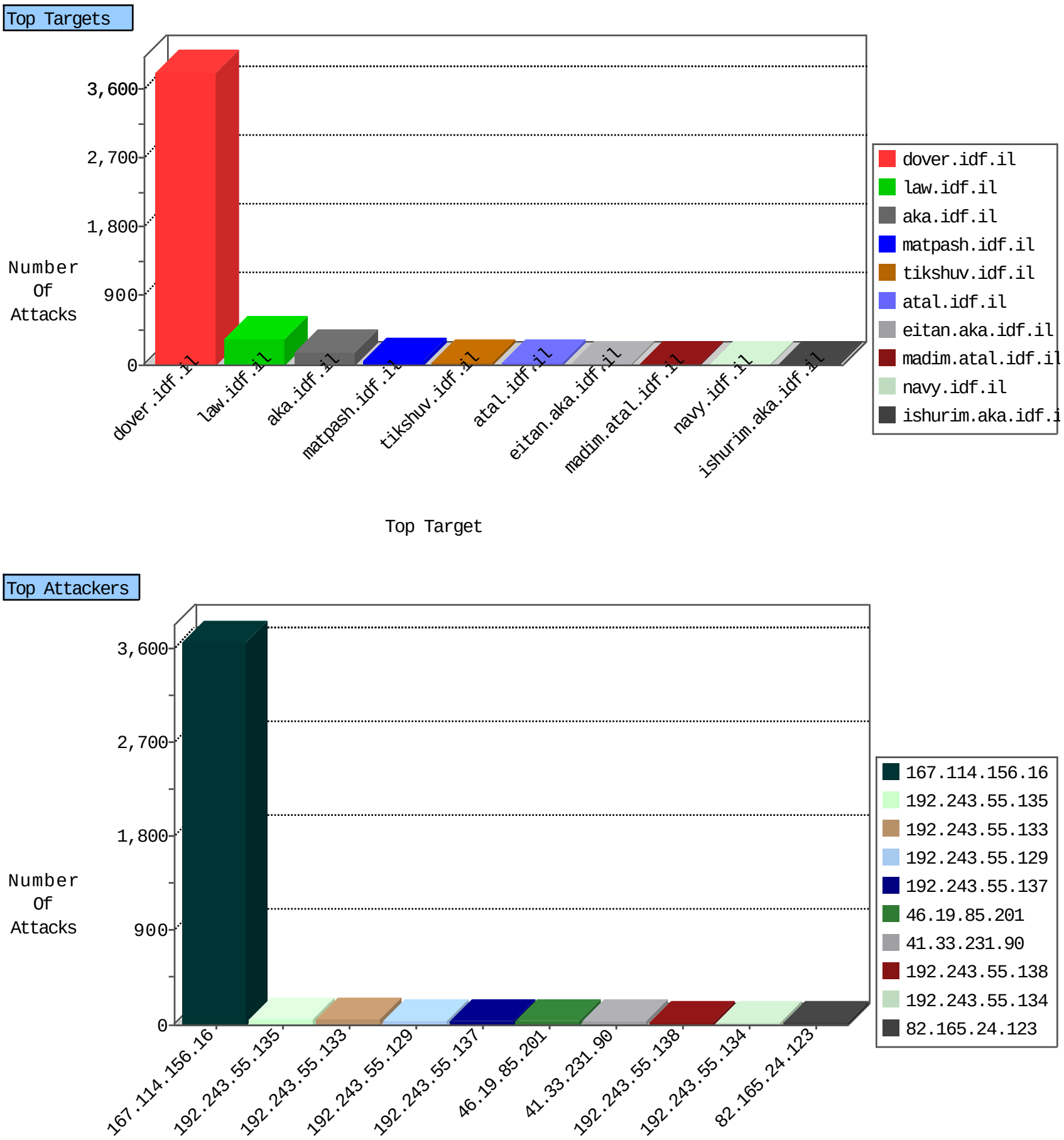
04-23-2016-13:04:00 to 04-23-2016-14:04:00

IDF Under Attack Daily Report



04-23-2016-13:04:00 to 04-23-2016-14:04:00

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	7218
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2088
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	532
104.148.71.133	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	6
101.100.136.81	New Zealand	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
104.148.71.133	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
61.145.16.15	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
104.148.71.133	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
104.238.135.152	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
188.138.17.205	France	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

04-23-2016-13:04:00 to 04-23-2016-14:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.165.24.123	Germany	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
82.165.24.123	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
70.68.224.173	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-23-2016-13:04:00 to 04-23-2016-14:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.165.24.123	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	14
70.68.224.173	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	4
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
62.98.65.170	147.237.77.216	Italy	dover.idf.il	Xenu Link Sleuth User Agent	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sA (2)	2
189.218.207.94	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.84.22	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
1.234.27.16	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
187.161.32.76	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.96	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.76.177	United States	ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
174.37.194.144	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
58.218.204.211	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
195.154.54.169	147.237.76.201	France	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
13.92.84.22	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.38	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
187.161.32.76	147.237.72.156	Mexico	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.234.27.16	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Potential SSH Scan	1
98.126.212.154	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
1.234.27.16	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
187.40.29.25	147.237.72.166	Brazil	aka.idf.il	Tehila - Perl LWP with fake user agent	1
93.174.93.96	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
180.106.36.37	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
174.37.194.144	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
58.218.204.211	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -f -sS	1
208.80.155.214	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
58.218.204.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
195.154.54.169	147.237.0.35	France	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1

04-23-2016-13:04:00 to 04-23-2016-14:04:00

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	2318
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.203.213	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
84.110.38.218	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
37.26.146.134	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.201	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	8
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
188.120.154.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.52.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.189.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.134	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence		alert	6
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.82.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.134	Israel	147.237.77.176	matpash.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	5
41.46.63.84	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.129	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	drop	First packet isn't SYN	drop	5
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.46.63.84	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.227.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.97	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.228.253.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
84.228.253.216	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.253.216	Block	2
84.228.253.216	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
191.101.2.30	United States	147.237.72.166	aka.idf.il	Multiple Illegal Parameter Encoding from 191.101.2.30	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
104.148.71.133	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.proxy-listen.de/azenv.php	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
181.215.104.65	United States	147.237.77.216	dover.idf.il	Multiple Illegal Parameter Encoding from 181.215.104.65	None	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-en/patzar.aspx.	Block	1
191.101.2.30	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
66.249.65.2	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
104.148.71.133	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.mesregies.com/azz.php	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/resources/styles/showbigstyle.css	Block	1
181.215.104.65	United States	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/templates/navmenu/navmenu.css.aspx	Block	1
62.98.65.170	Italy	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.98.65.170	Block	1
141.212.122.161	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8913-he/refuah.aspx	Block	1
192.243.55.131	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdezmzquzg9j&infocenteritem=true	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
104.148.71.133	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.proxy-listen.de/azenv.php	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	1
187.40.29.25	Brazil	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
62.98.65.170	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Abnormally Long Request method	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;popId in www.aka.idf.il/lomdim/news/	None	1
207.46.13.23	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.147.238	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
177.231.218.59	Mexico	147.237.76.30	himush.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
109.67.29.56	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
187.40.29.25	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/chamatz/miktzoa/default.asp	None	1
177.231.218.59	Mexico	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
37.46.41.132	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1

04-23-2016-13:04:00 to 04-23-2016-14:04:00