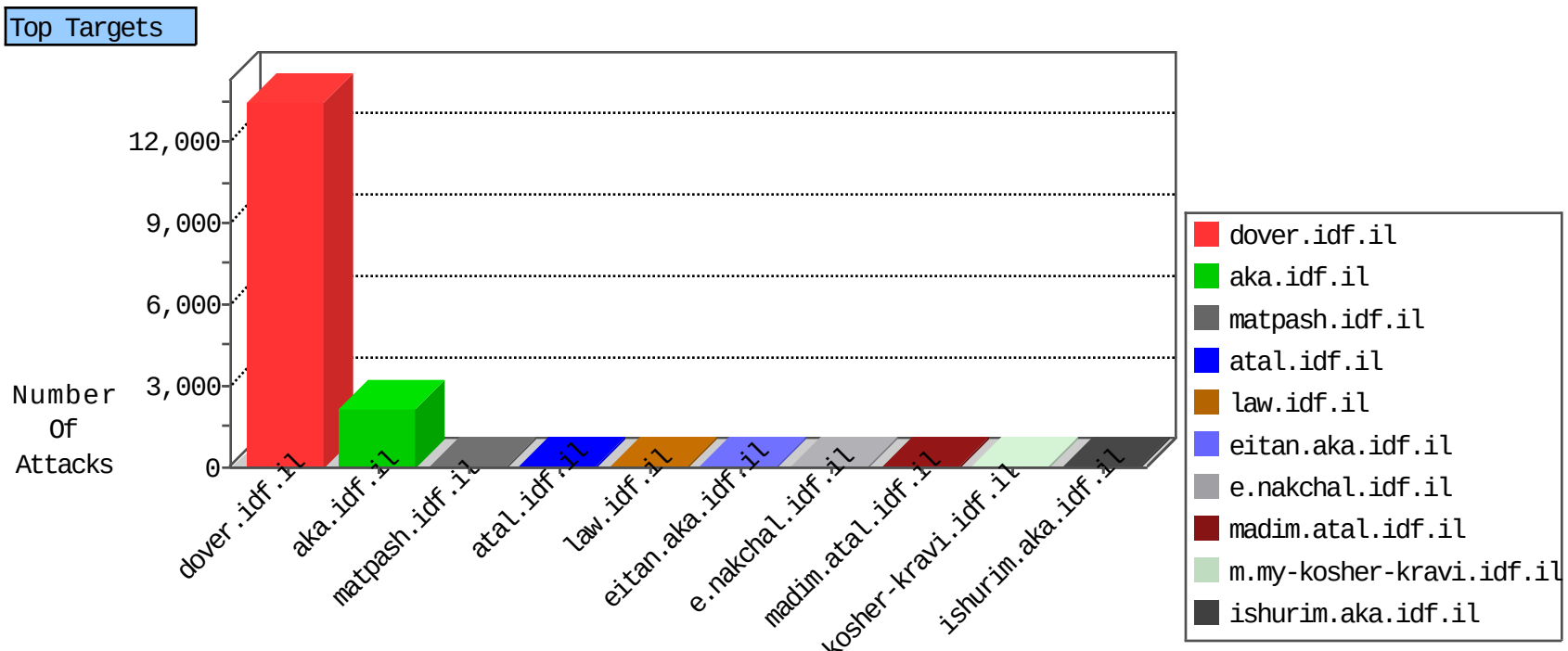
04-23-2016-08:04:08 to 04-23-2016-09:04:08

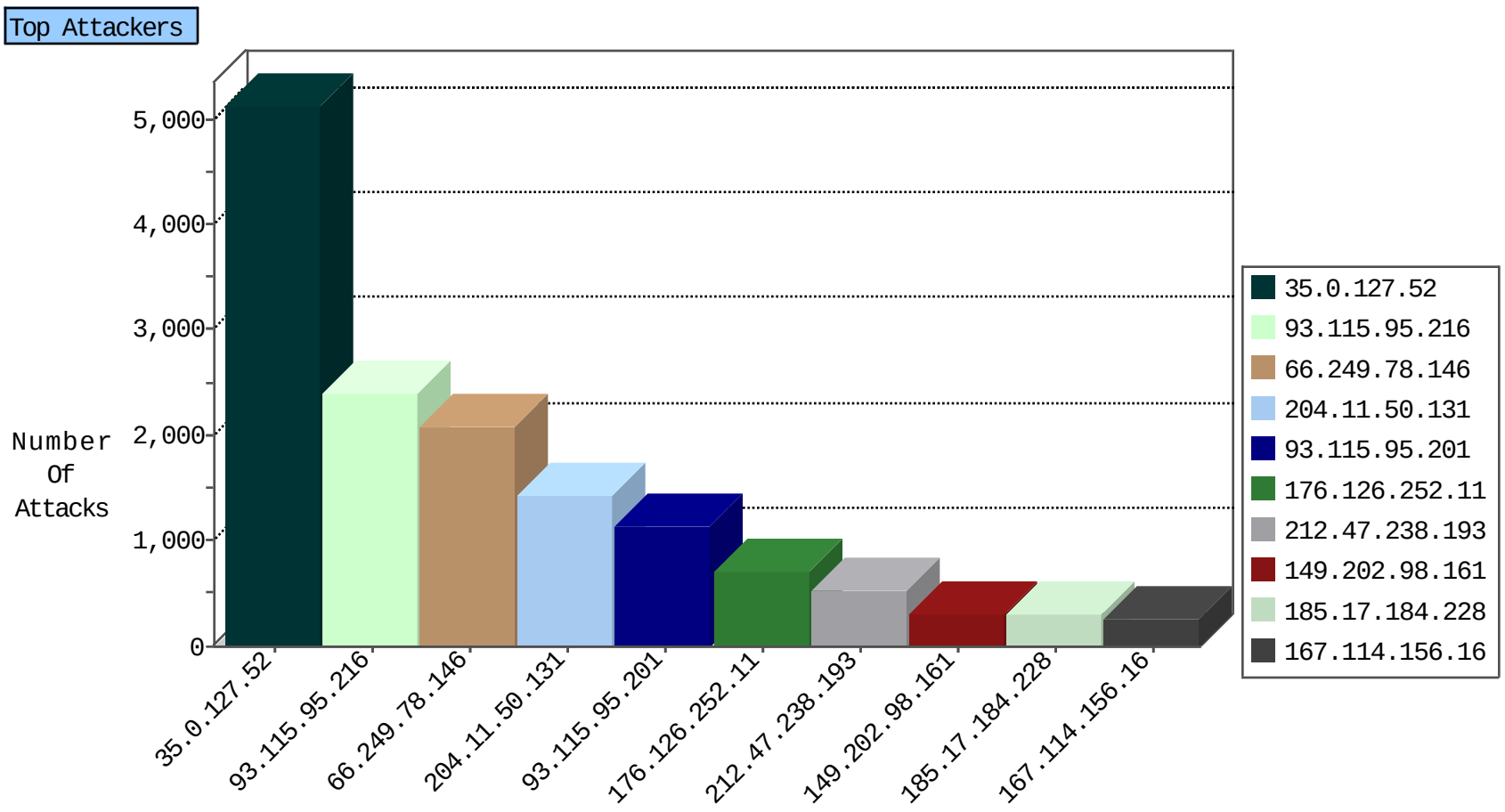
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-23-2016-08:04:08 to 04-23-2016-09:04:08

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	11797
35.0.127.52	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6324
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	1372
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1116
212.47.238.193	France	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	807
149.202.98.161	France	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	807
176.126.252.11	Romania	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	704
62.149.25.15	Ukraine	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	168
204.11.50.131	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	95
37.220.35.202	Netherlands	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	52
185.100.84.82	Romania	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	24
192.241.232.57	United States	147.237.77.216	dover.idf.il	DOS-WEB-HULK-improved	forward	6
204.11.50.131	Canada	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
194.8.253.145	Czech Republic	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	2
89.46.102.242	Romania	147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
204.11.50.131	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.46.102.242	Romania	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

04-23-2016-08:04:08 to 04-23-2016-09:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.96.128.60	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-23-2016-08:04:08 to 04-23-2016-09:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1962
66.96.128.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
176.126.252.11	147.237.77.216	Romania	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
95.45.254.123	147.237.72.167	Ireland	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
35.0.127.52	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
152.115.74.164	147.237.77.121	Denmark	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.244.75	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
101.108.232.49	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
169.54.244.75	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
179.43.144.37	147.237.0.34	Switzerland	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
169.54.244.75	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
174.37.194.144	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
152.115.74.164	147.237.8.46	Denmark	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.244.75	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.77.74	United States	law.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.244.75	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
211.149.156.87	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.244.75	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
186.213.204.184	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
169.54.244.75	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

04-23-2016-08:04:08 to 04-23-2016-09:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
35.0.127.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4956
204.11.50.131	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1408
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1369
93.115.95.201	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1136
212.47.238.193	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	391
185.17.184.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	305
149.202.98.161	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	227
176.126.252.11	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	159
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	123
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
94.155.49.47	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
5.199.142.195	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
62.149.25.15	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.220.35.202	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
195.22.126.119	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
24.12.191.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.58.79.110	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
5.39.76.158	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
77.42.252.199	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
140.147.249.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
141.0.15.46	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
195.154.56.44	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.203.191	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.71.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
35.0.127.52	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.81.233	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.202.98.161	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	6
176.126.252.12	Romania	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
172.218.164.55	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
140.147.249.7	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
194.8.253.145	Czech Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

04-23-2016-08:04:08 to 04-23-2016-09:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	642
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	295
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	153
35.0.127.52	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	112
176.126.252.12	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	82
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	80
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	79
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	76
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	43
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	41
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	36
35.0.127.52	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	22
176.126.252.12	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	17
35.0.127.52	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	14
149.202.98.161	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	11
35.0.127.52	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	9
176.126.252.12	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	9
176.126.252.12	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	9
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	8
176.126.252.12	Romania	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	8
62.210.37.82	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	8
37.220.35.202	Netherlands	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	6
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	4
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	4
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
149.202.98.161	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	3
149.202.98.161	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	3
62.210.37.82	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	2
62.210.37.82	France	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	2
66.249.82.91	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.82.91	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
140.147.249.7	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
185.93.183.215	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
159.226.95.66	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
37.220.35.202	Netherlands	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Query String	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
62.4.22.224	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
64.62.219.156	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 64.62.219.156 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.82.88	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
62.4.22.224	France	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
95.45.254.123	Ireland	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
76.31.170.233	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1
109.64.100.72	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	1
157.55.39.156	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
37.220.35.202	Netherlands	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Parameter Name	Block	1

04-23-2016-08:04:08 to 04-23-2016-09:04:08