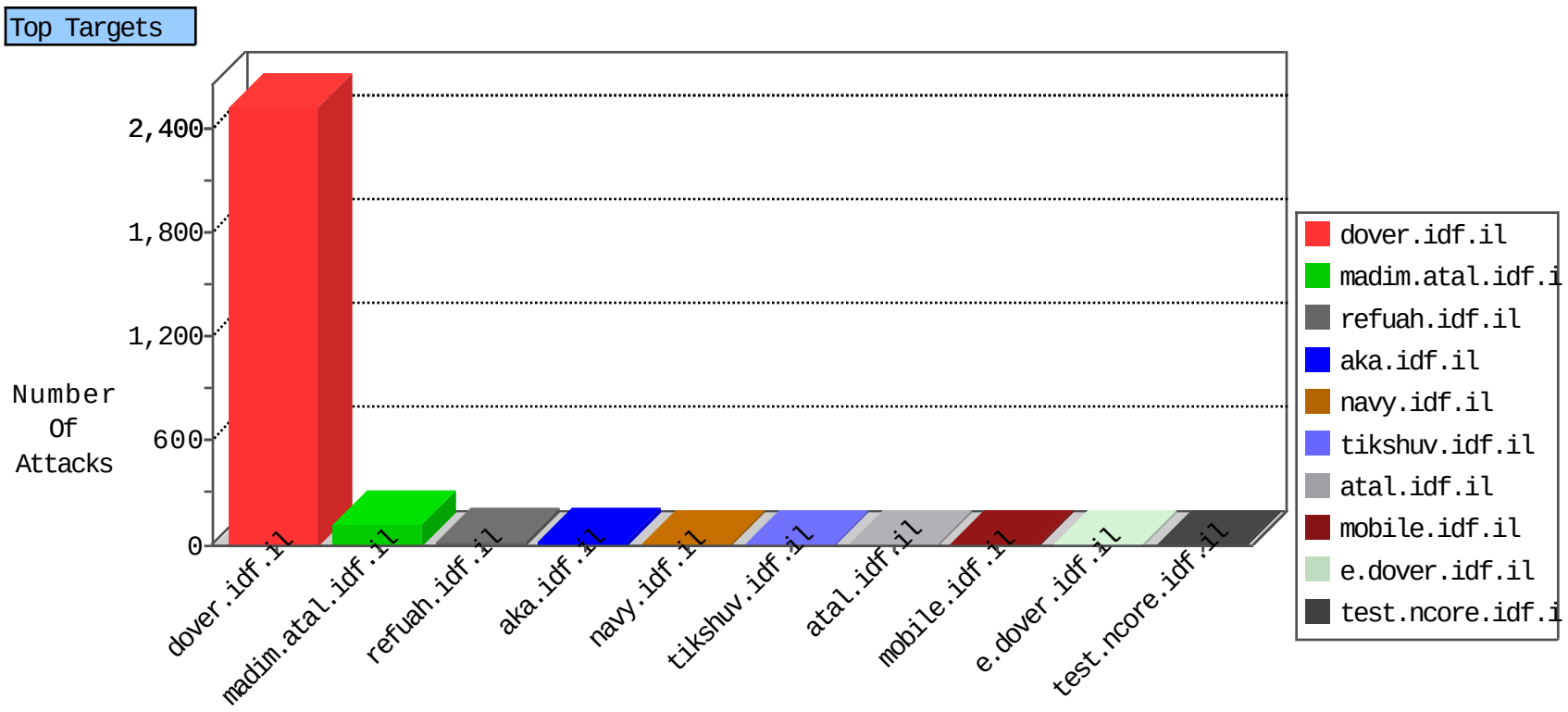
03-15-2016-06:04:05 to 03-15-2016-07:04:05

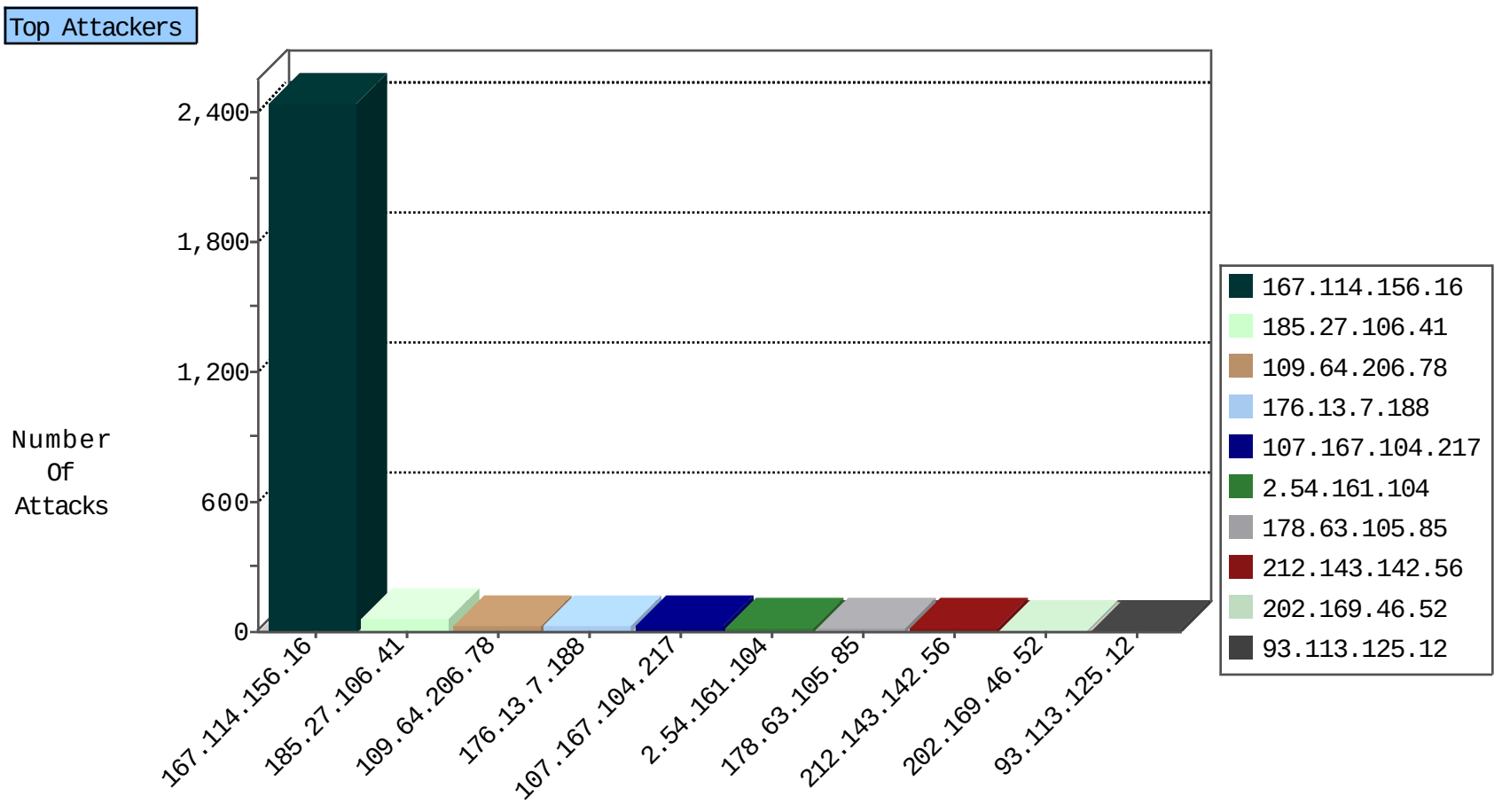
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-15-2016-06:04:05 to 03-15-2016-07:04:05

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	DOS-Tool-SwitchbladG	dest-reset	3779

03-15-2016-06:04:05 to 03-15-2016-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
195.154.185.20	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
46.116.11.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
213.251.184.38	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1

03-15-2016-06:04:05 to 03-15-2016-07:04:05

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	4
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
173.214.169.188	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
69.4.82.226	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.195	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
173.214.169.188	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
93.189.26.18	147.237.77.176	Austria	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
69.4.82.226	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
69.4.82.226	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1

03-15-2016-06:04:05 to 03-15-2016-07:04:05

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	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
109.64.206.78	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
107.167.104.217	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
77.126.166.96	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.39.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.160.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.113.125.12	Romania	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
74.217.28.153	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
109.253.206.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.193.101.41	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	2
93.113.125.12	Romania	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.5.201	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.179.9.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.193.24.125	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
93.113.125.12	Romania	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
176.13.5.201	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.122	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.147.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.162.222.24	Netherlands	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.83	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
178.63.105.85	Germany	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
137.116.71.170	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.204	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.222.24	Netherlands	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.104	United States	147.237.0.33	idf.il	drop		drop	1
85.65.208.119	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
213.251.184.38	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.102.242.0	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.194.129	Netherlands	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.248	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
176.13.20.79	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
38.229.1.15	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.109.209	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.27.106.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
176.13.7.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
2.54.161.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
2.54.3.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.86.94.7	Germany	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 80.86.94.7	Block	4
2.54.39.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.54.27.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.134.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
93.113.125.12	Romania	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
198.20.69.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
109.186.40.191	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
202.169.46.52	Indonesia	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 4	Block	1
41.40.229.104	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.50.182.55	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
149.88.118.75	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
95.0.143.197	Turkey	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-19706-he/dover.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/	Block	1
202.169.46.52	Indonesia	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
109.186.40.191	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
80.86.94.7	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.aspx	Block	1
202.169.46.52	Indonesia	147.237.77.216	dover.idf.il	Malformed URL html	Block	1
41.40.229.104	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
2.50.182.55	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
95.0.143.197	Turkey	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
202.169.46.52	Indonesia	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
109.186.40.191	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
91.227.164.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
202.169.46.52	Indonesia	147.237.77.216	dover.idf.il	Too Many Cookies in a Request - 447 cookies	Block	1
109.64.206.78	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.229.124	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9641-he/refuah.aspx	Block	1
202.169.46.52	Indonesia	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name <HTML><HEAD><TITLE>Bad Request</TITLE>	Block	1
37.26.146.191	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
91.227.165.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
202.169.46.52	Indonesia	147.237.77.216	dover.idf.il	Unknown HTTP Request Method <!DOCTYPE in URL html	Block	1
64.108.192.96	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.20.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
186.64.155.245	Costa Rica	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.186.40.191	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
202.169.46.52	Indonesia	147.237.77.216	dover.idf.il	Illegal HTTP Version PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
146.94.254.34	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-15-2016-06:04:05 to 03-15-2016-07:04:05