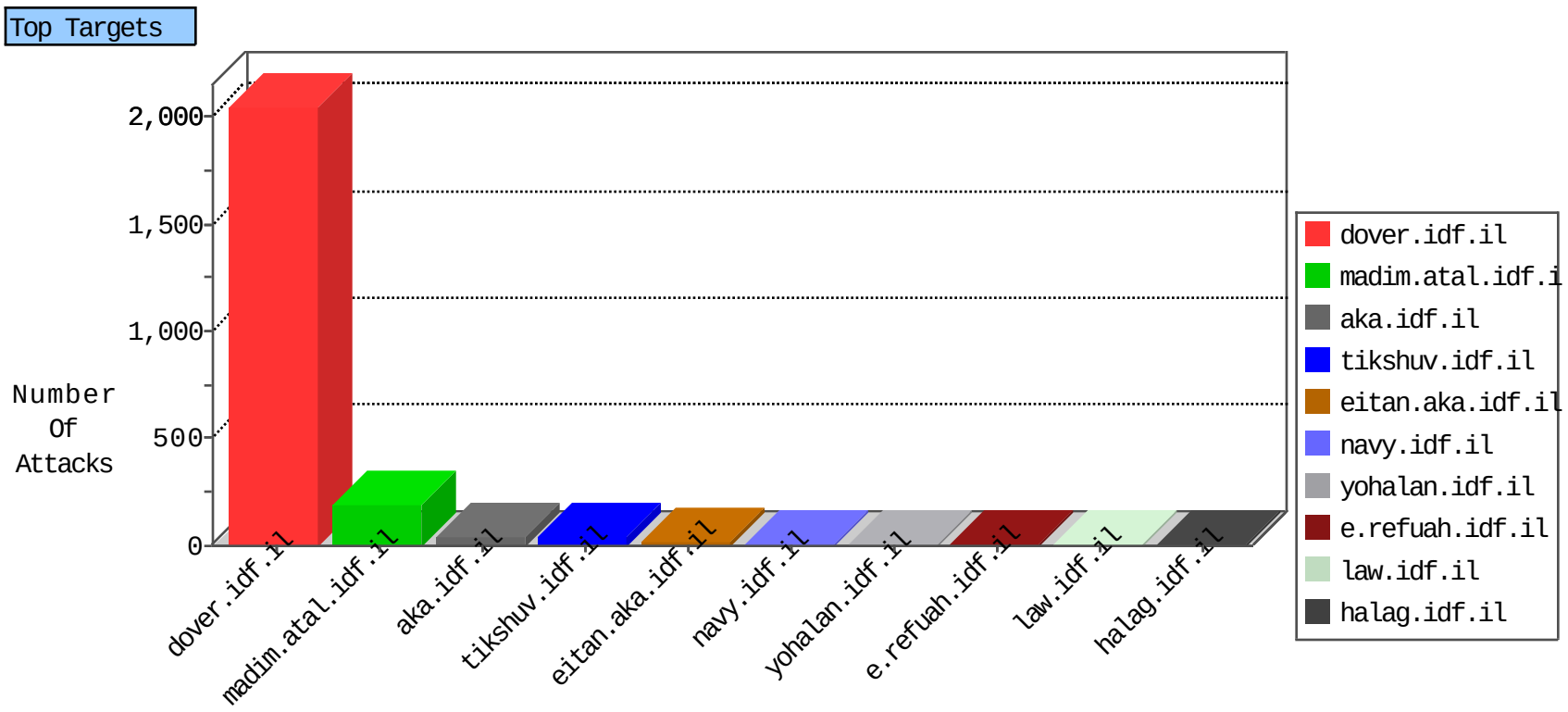
01-13-2016-03:04:09 to 01-13-2016-04:04:09

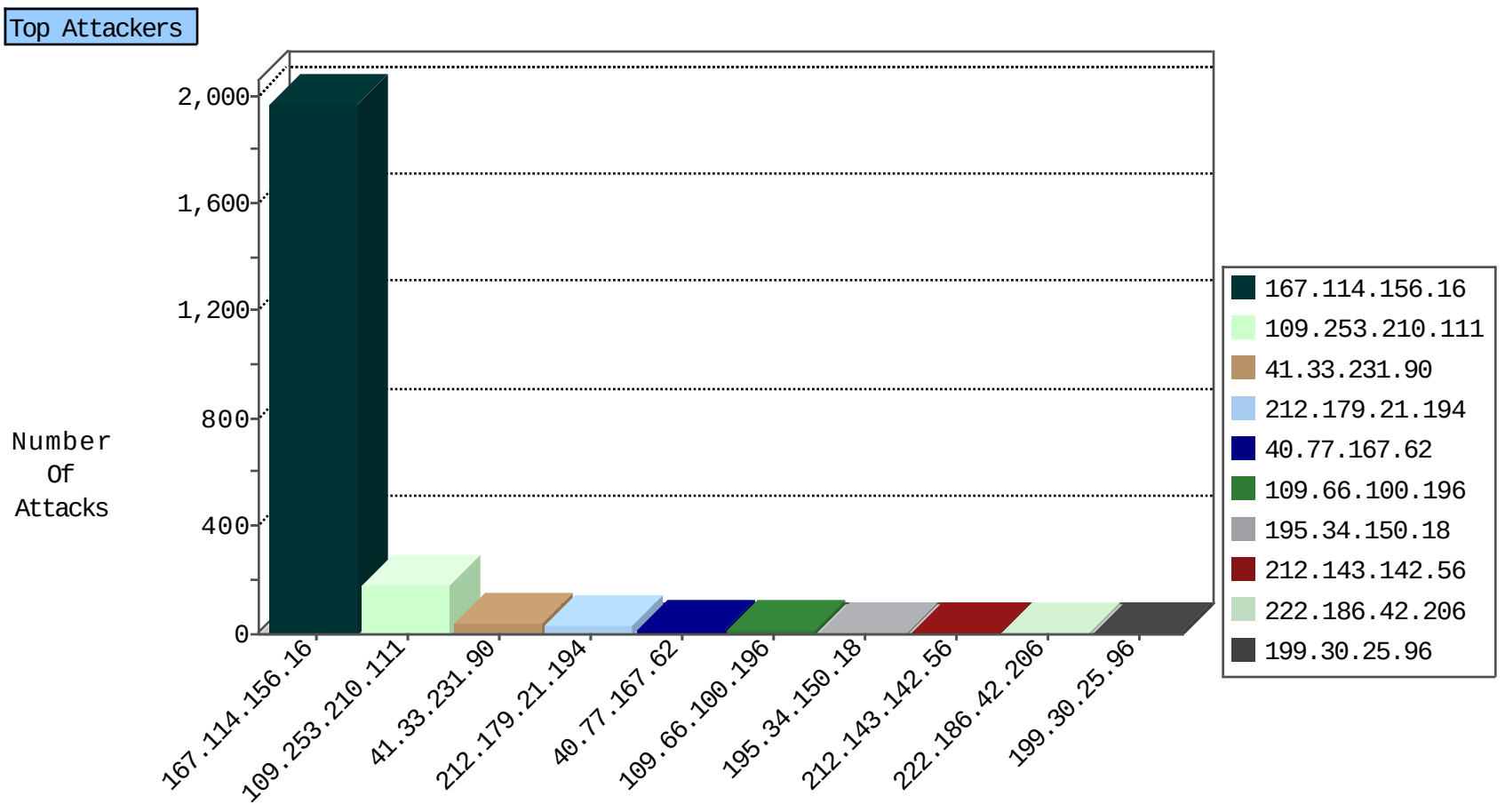
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-13-2016-03:04:09 to 01-13-2016-04:04:09

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	3004
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
222.186.21.181	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
185.35.62.62	Switzerland	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
198.167.140.112	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

01-13-2016-03:04:09 to 01-13-2016-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-13-2016-03:04:09 to 01-13-2016-04:04:09

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
113.59.33.61	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
182.163.103.210	147.237.76.34	Bangladesh	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
50.204.188.142	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
177.158.254.148	147.237.77.234	Brazil	halag.idf.il	ET SCAN NMAP -sS window 2048	1
5.39.222.196	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.42.206	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
177.158.254.148	147.237.77.234	Brazil	halag.idf.il	ET SCAN NMAP -f -sS	1
222.186.42.206	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
158.255.6.220	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.206	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
113.171.23.126	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
60.214.212.20	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.163.103.210	147.237.76.34	Bangladesh	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
50.204.188.142	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
182.163.103.210	147.237.76.34	Bangladesh	yohalan.idf.il	ET SCAN NMAP -f -sS	1
5.39.222.196	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
177.158.254.148	147.237.77.234	Brazil	halag.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.206	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.206	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.206	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
194.187.249.70	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
113.171.23.126	147.237.76.86	Vietnam	navy.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1

01-13-2016-03:04:09 to 01-13-2016-04:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
40.77.167.62	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.100.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
199.30.25.96	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
118.70.212.142	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.78.62	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.168.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.120.125.56		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.159.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.64.90.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
141.212.122.158	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.75.199.187	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.207	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.179	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
61.242.114.58	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.255.6.220	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.158	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.65.0.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
216.218.206.118	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.144.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
38.229.1.15	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.180	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.36.197	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
65.55.212.88	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.159	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.65.0.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
73.10.31.200	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.3.147.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.181	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.155	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.67.1.25	United States	147.237.0.33	idf.il	drop		drop	1
65.55.212.92	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.159	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.10.31.200	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.188	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.156	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.67.1.25	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.91	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.178	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

01-13-2016-03:04:09 to 01-13-2016-04:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.210.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
109.253.210.111	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.210.111	Block	84
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	33
93.173.228.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.187.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.108.98.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
197.231.221.211	Liberia	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
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
183.79.221.36	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.201.152.248	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.79.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
185.75.56.104		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
195.154.194.111	France	147.237.77.74	law.idf.il	PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.228.234.180	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
195.154.194.111	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3480.jpg	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=cd0d9b8akkkkkkk_cd0d9b8a	Block	1
85.25.103.119	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

01-13-2016-03:04:09 to 01-13-2016-04:04:09