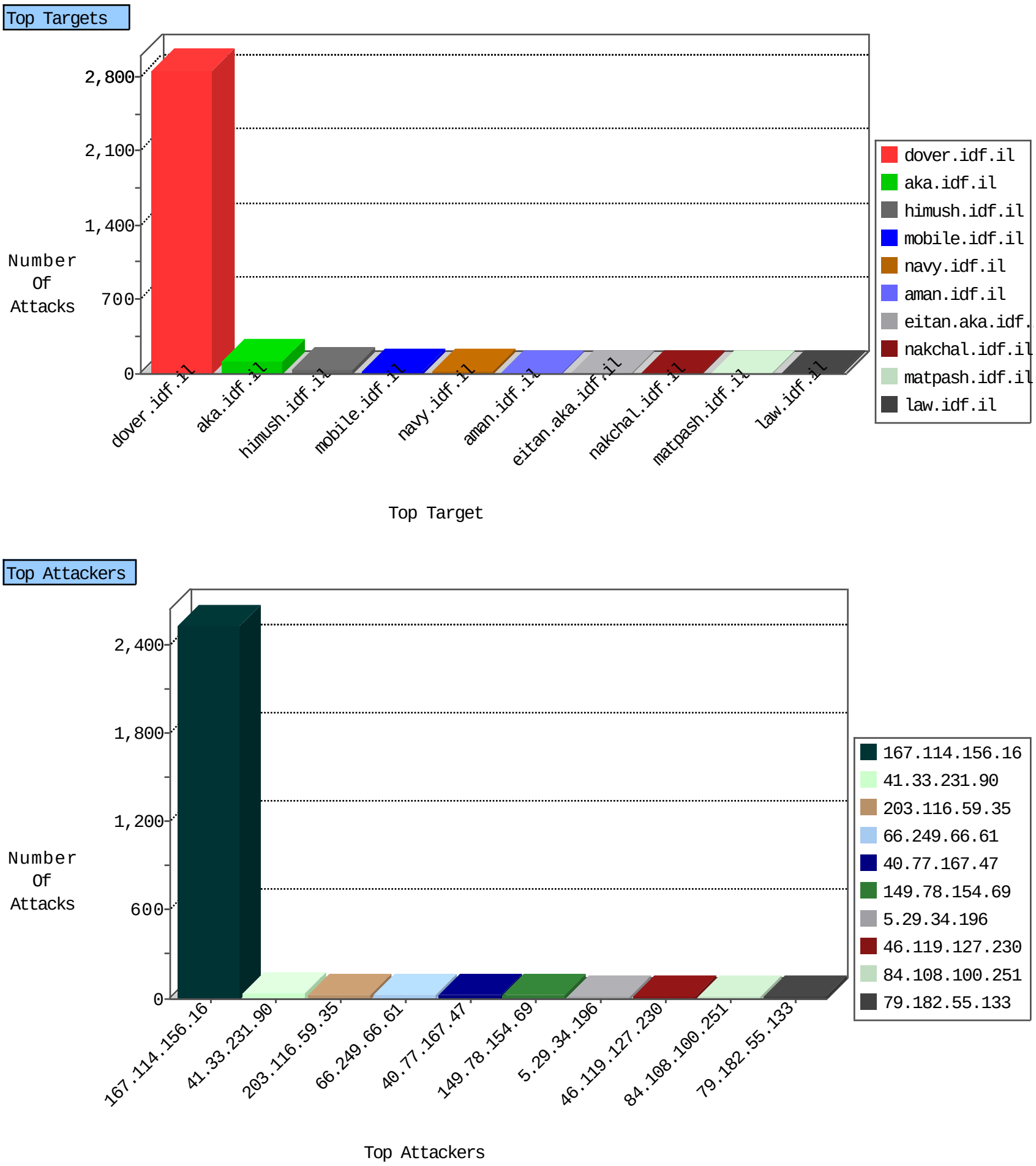
12-15-2015-03:04:02 to 12-15-2015-04:04:02

IDF Under Attack
Daily Report



12-15-2015-03:04:02 to 12-15-2015-04:04:02

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	4833
183.60.48.25	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.106.94.126		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1

12-15-2015-03:04:02 to 12-15-2015-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.85.77	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-15-2015-03:04:02 to 12-15-2015-04:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
208.90.155.46	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
196.47.173.21	147.237.76.30	Cote D'Ivoire	himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.7	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
23.97.172.218	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
104.209.183.157	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1

12-15-2015-03:04:02 to 12-15-2015-04:04:02

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	796
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
40.77.167.47	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
79.182.55.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
183.79.221.201	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
68.100.242.101	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
40.77.167.47	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.34.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
74.110.208.43	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.42.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
207.46.13.169	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.66.61	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.100.251	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
207.46.13.104	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
84.108.100.251	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.125.118.245	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.108.100.251	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.68.49.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.193.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.189	United States	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.81	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.177.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.129.237	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
68.180.229.239	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
208.115.113.92	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.23	United States	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
86.50.110.141	Finland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.95.212.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
180.149.143.17	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
61.135.169.56	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
115.239.212.134	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.34.196	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	12
208.115.111.74	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	6
46.119.127.230	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
46.119.127.230	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.119.127.230	Block	5
109.253.146.114	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
157.55.39.3	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.61	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
84.94.26.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
98.137.84.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english/1.doc.	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
66.249.66.81	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
180.76.15.159	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	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
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
46.119.127.230	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
208.90.155.46	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 208.90.155.46 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
98.139.14.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/daily_statistics/english/1.doc.	Block	1
220.227.161.85	India	147.237.77.216	dover.idf.il	PHP External Variable Manipulation SERVER Parameter	Block	1
66.249.66.83	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
183.79.221.201	Japan	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
79.181.193.211	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.60	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
208.90.155.46	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	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
66.249.66.87	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
203.217.72.86	Australia	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/mas.aspx	Block	1
141.212.122.64	United States	147.237.0.15	kosher-kravi.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.77	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.88	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.137	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
141.212.122.64	United States	147.237.76.31	nakchal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
86.50.110.141	Finland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
180.76.15.157	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	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
141.212.122.64	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 141.212.122.64	Block	1

12-15-2015-03:04:02 to 12-15-2015-04:04:02