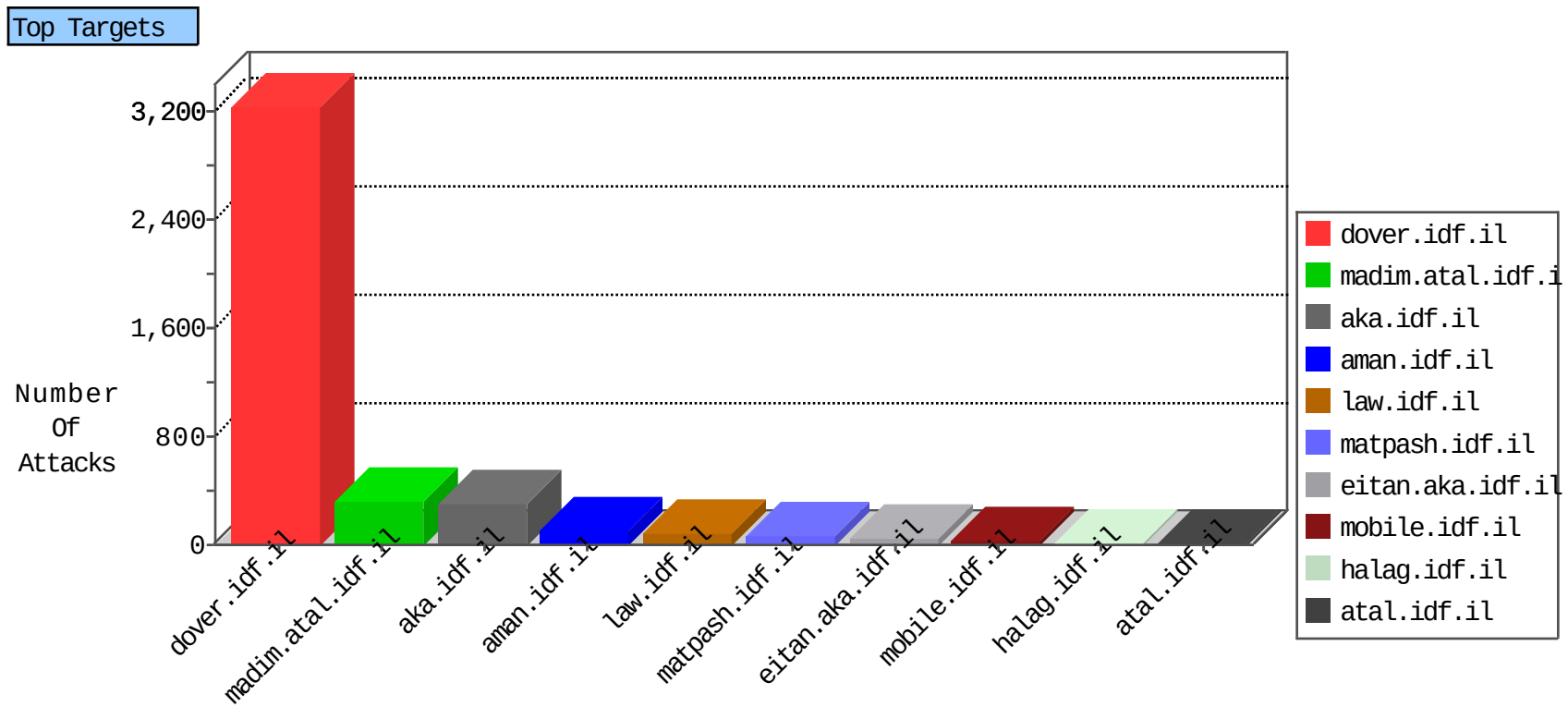
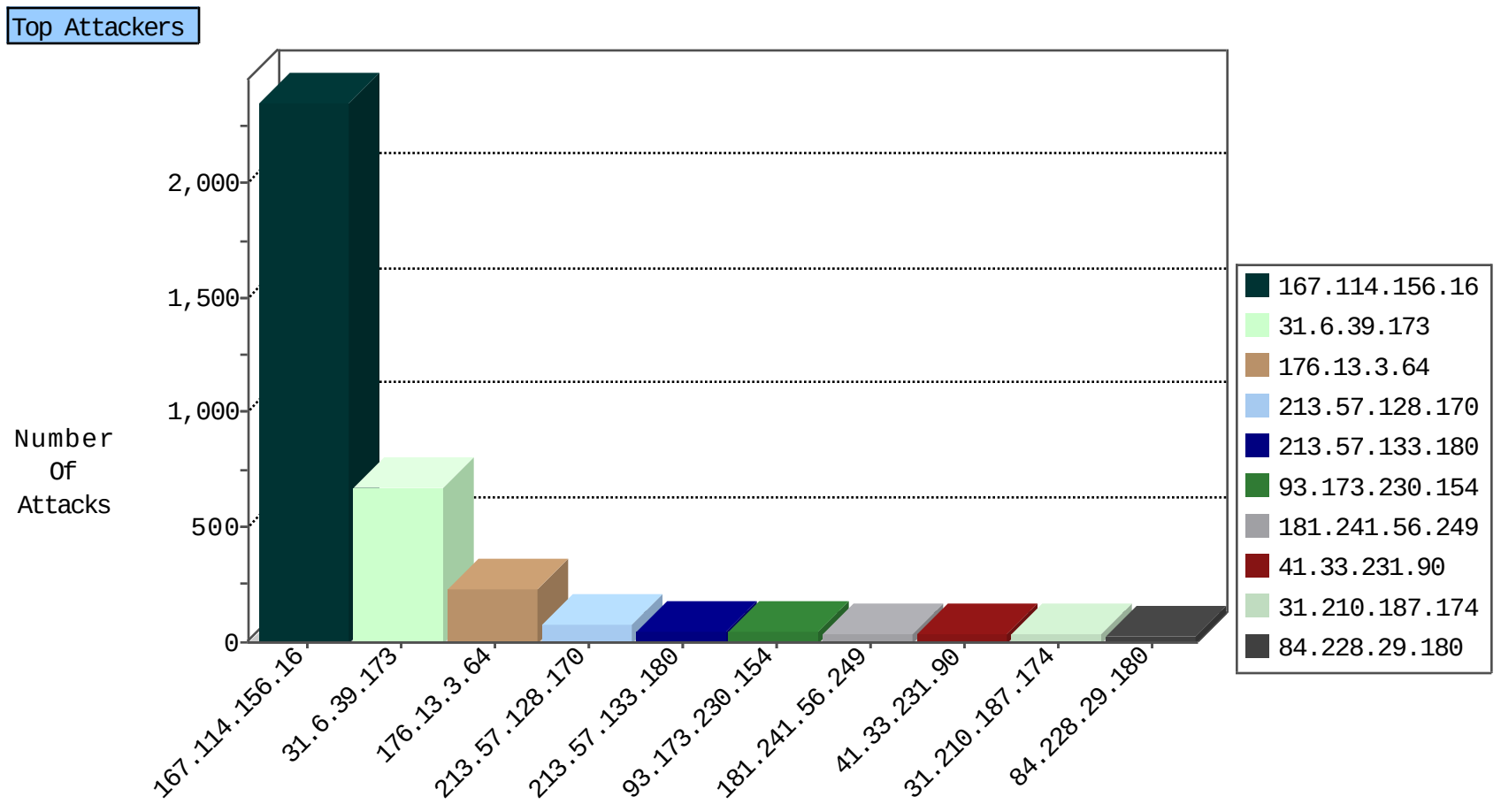
11-28-2015-16:04:01 to 11-28-2015-17:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-28-2015-16:04:01 to 11-28-2015-17:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.6.39.173	Spain	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	6265
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3694

11-28-2015-16:04:01 to 11-28-2015-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.113.244	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
195.154.180.69	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
78.135.79.101	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
195.154.188.74	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.188.158	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
91.121.60.119	France	147.237.0.34	tikshuv.idf.i	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
195.154.180.24	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-28-2015-16:04:01 to 11-28-2015-17:04:01

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
218.104.49.211	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.74.97	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.104.49.211	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
51.254.46.129	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.76.176	Poland	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.104.49.211	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
195.154.188.158	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	1
51.254.46.129	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
51.254.46.129	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 1024	1

11-28-2015-16:04:01 to 11-28-2015-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.128.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	44
213.57.133.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	43
181.241.56.249	Colombia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.128.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
84.228.29.180	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.0.229		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	23
100.100.62.233		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
213.57.29.52	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
213.57.40.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.103.223		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.111.147		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
100.100.32.148		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
193.194.86.119	Algeria	147.237.77.216	dover.idf.il	drop		drop	7
46.19.86.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.168.144.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.136.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.136.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.15.0		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
5.29.19.108	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.247.36.124	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
37.46.39.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.61.123	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.172.241.58	Portugal	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
94.230.86.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
181.134.16.115	Colombia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.123.117.68	United Kingdom	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
87.69.208.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.133.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.173.230.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.175.218	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.177.211.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.6.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.27.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.141.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.94.99.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.139.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.131.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.27.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

11-28-2015-16:04:01 to 11-28-2015-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.3.64	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.3.64	Block	114
176.13.3.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
93.173.230.154	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
31.210.187.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
176.13.3.64	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.3.64	Block	13
185.32.179.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
77.126.220.155	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.220.155	Block	7
109.160.204.186	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	5
76.12.219.39	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
173.44.38.200	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
75.98.175.89	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
188.166.250.183	Russian Federation	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
166.63.124.152	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
80.246.136.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
173.44.38.200	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 173.44.38.200	Block	3
162.249.4.102	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
186.202.161.32	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
54.229.137.156	Ireland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
185.96.93.157		147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
198.46.81.15	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
79.180.27.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.231.201.171	Switzerland	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
5.157.84.15	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
81.218.205.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.170.205.27	Norway	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
175.107.174.1	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
27.121.104.121	Australia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
162.249.4.102	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	2
186.202.161.32	Brazil	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
46.116.86.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
93.172.40.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
84.228.29.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.96.93.157		147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
54.229.137.156	Ireland	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
198.46.81.15	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	2
176.13.19.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
75.98.175.89	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 75.98.175.89	Block	2
175.107.174.1	Australia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
85.250.36.152	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
166.63.124.152	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 166.63.124.152	Block	2
149.88.241.92	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1531.jpg	Block	2
46.231.201.171	Switzerland	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	2
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	2
5.157.84.15	Netherlands	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
188.166.250.183	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
54.229.137.156	Ireland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.229.137.156	Block	2
185.96.93.157		147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 185.96.93.157	Block	2
176.13.9.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2

11-28-2015-16:04:01 to 11-28-2015-17:04:01