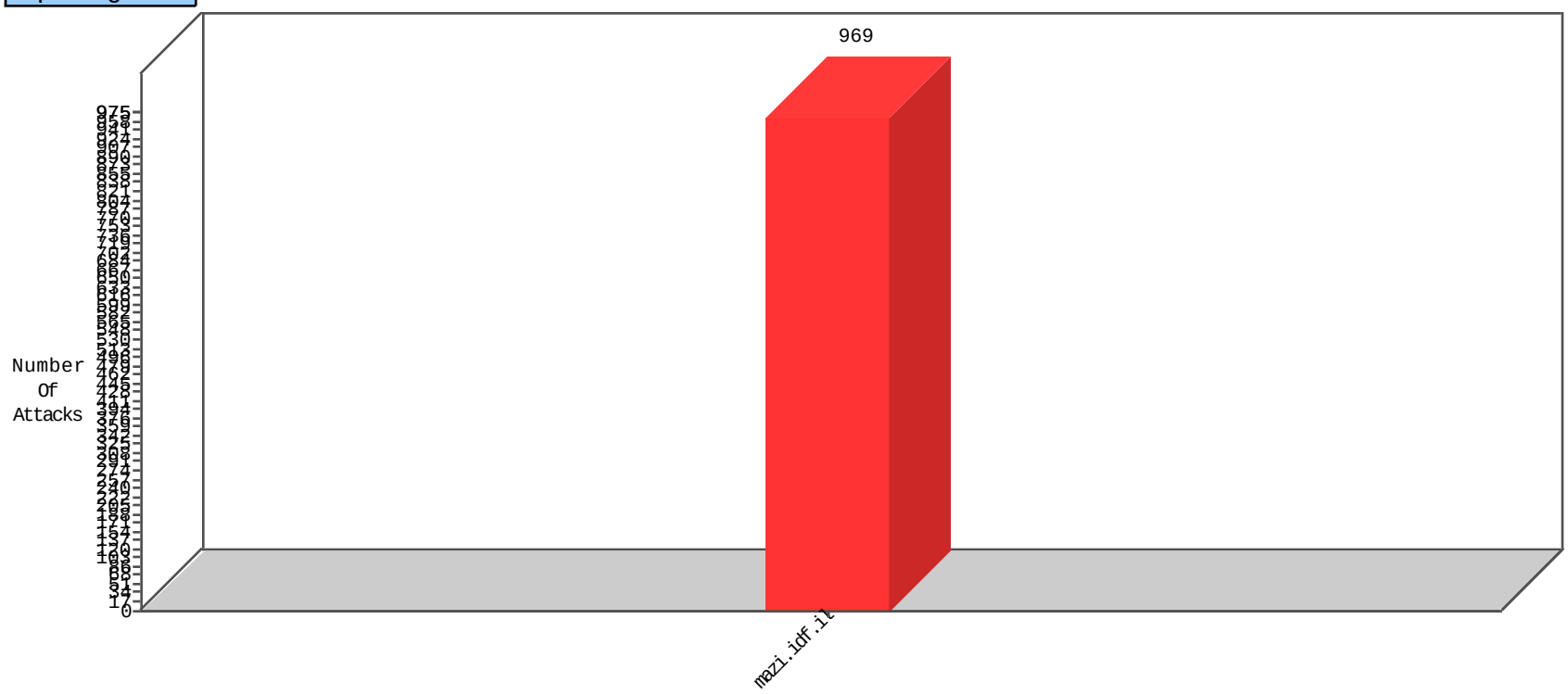
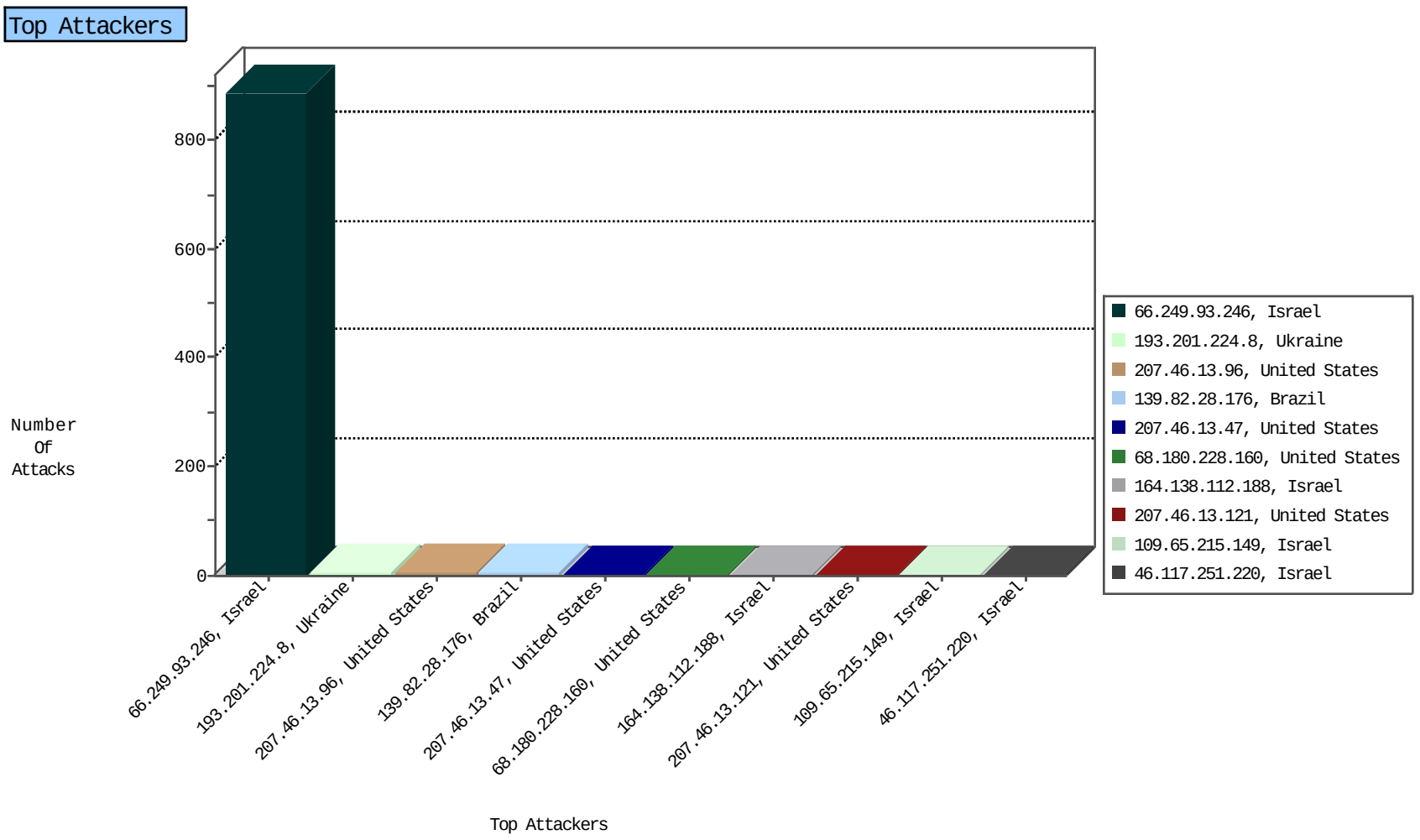
12-02-2015 to 12-03-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-02-2015 to 12-03-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.93.246	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	890
109.65.215.149	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3

12-02-2015 to 12-03-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
151.80.31.131	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-02-2015 to 12-03-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
42.48.224.74	China	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.192.90.145	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
149.202.186.50	Germany	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
218.199.48.58	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
54.224.149.230	United States	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	1
128.199.54.170	Singapore	147.237.77.17	mazi.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.57.129.160	Israel	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1

12-02-2015 to 12-03-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.85.89	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	68
46.19.85.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	68
46.19.85.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	64
46.19.85.89	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	64
46.19.85.230	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	40
46.19.85.230	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.86.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.105	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
203.133.169.212	Korea, Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.178	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
85.250.238.143	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.46	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.3.146	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.228	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.151	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.120.126.111		147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
93.172.148.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.86.242	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.94	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.176	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.16.20	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.228	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.201	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.176	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.249	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.154.155.160	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
151.80.109.45	Italy	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	3
2.54.166.137	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
198.20.69.74	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.95	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.46	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.160	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.207	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
91.107.167.232	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.176.178.107	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.92	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.130.227.133	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.190	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.121	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
5.102.254.207	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
46.19.85.245	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.141.118	Netherlands	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.200	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.255	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
212.25.83.133	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.147.228	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
139.82.28.176	Brazil	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 139.82.28.176	Block	4
207.46.13.96	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.46.13.96	Block	3
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 68.180.228.160	Block	2
46.117.251.220	Israel	147.237.77.17	mazi.idf.i	Unauthorized HTTP Method	Block	2
193.201.224.8	Ukraine	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 193.201.224.8	Block	2
164.138.112.188	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4980-he	Block	2
193.201.224.8	Ukraine	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
207.46.13.121	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/workarea/java/ektron.site-data.js.ashx	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-10540-he/igf.aspx	Block	1
207.46.13.47	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/workarea/csslib/ektroncss.ashx	Block	1
193.201.224.8	Ukraine	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 193.201.224.8	Block	1
52.29.144.27	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
31.210.187.202	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
157.55.39.136	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/legacy	Block	1
93.172.148.5	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
207.46.13.96	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ajax/checkuserlogin/	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
207.46.13.47	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.46.13.47	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4170-he/igf.aspx	Block	1
173.252.102.115	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/397-he/igf.aspx&h=191&w=624&tbnid=-tqzbc2p5g3hwm:&docid=rowqtrjgpsmoem&ei=x_9evscqkyquaqrco5gm&tbm=isch&ved=0ahukewiaqpktsb3jahuklxokhsrucmmqmwgdkaewaq	Block	1
139.82.28.176	Brazil	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
2.54.2.91	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
213.57.49.5	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
66.249.67.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
52.29.144.27	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-login.php	Block	1
37.29.48.134	Russian Federation	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
164.138.112.188	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 164.138.112.188	Block	1
109.67.168.165	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
207.46.13.121	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5078-6081-he/igf.aspx	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5184-he/igf.aspx	Block	1
207.46.13.47	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
193.201.224.8	Ukraine	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
46.117.251.220	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/	Block	1
31.184.132.24	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/www.idiegogo.com/projects/121440	Block	1
66.249.78.161	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/general/×″	Block	1
207.46.13.96	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
197.37.10.159	Egypt	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.66.43	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6053-he/igf.aspx	Block	1
37.29.48.134	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
109.67.168.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
207.46.13.121	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/reussir/public/gzip2.php	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5484-7277-he/igf.aspx	Block	1
207.46.13.47	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he/	Block	1
46.120.58.56	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
157.55.39.136	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
31.210.187.202	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 31.210.187.202	Block	1
79.178.138.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
66.249.78.164	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/×œ×œ×? ×’×‘×•×œ×•×ª.aspx	Block	1
207.46.13.96	United States	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	1
197.37.10.159	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9065-he/igf.aspx	Block	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templ@es/homepage/homepage.aspx	Block	1
173.252.102.113	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/6/5826.jpg&imgrefurl=	Block	1
128.199.54.170	Singapore	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1

12-02-2015 to 12-03-2015