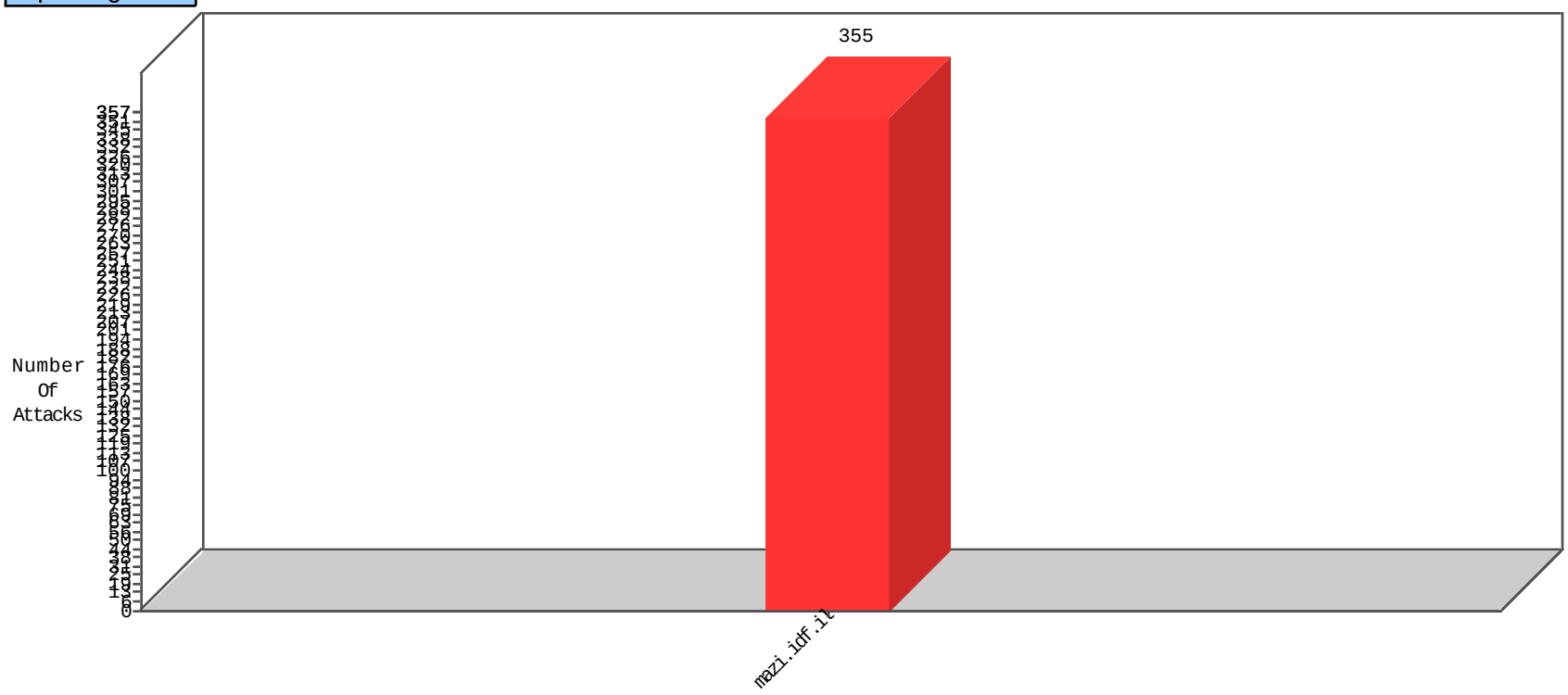
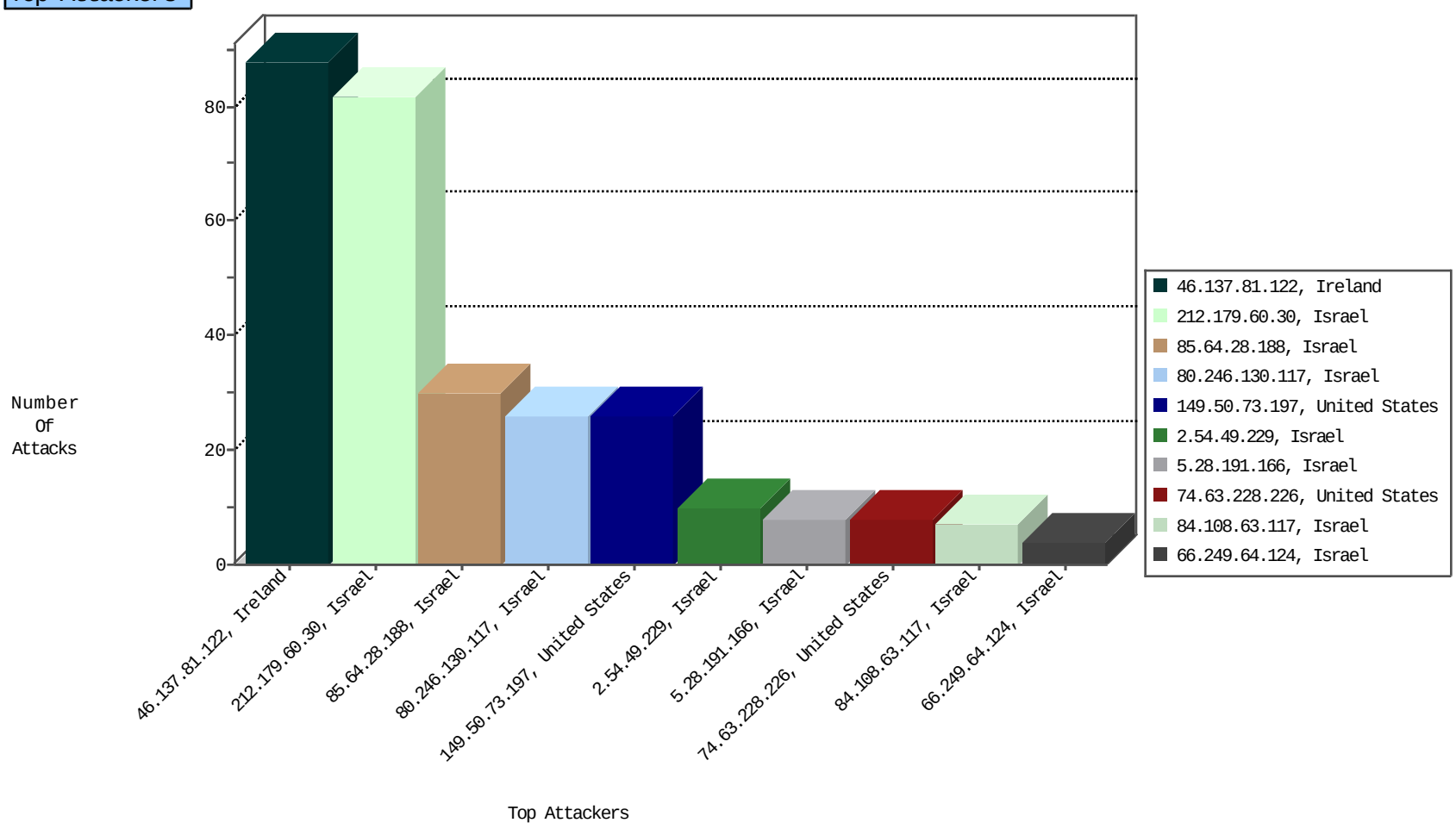
02-18-2016 to 02-19-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-18-2016 to 02-19-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.46.189	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3

02-18-2016 to 02-19-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.60.30	Israel	147.237.77.17	mazi.idf.il	C1000004: HTTP: options method (Microsoft)	Block	82
46.137.81.122	Ireland	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	52
85.64.28.188	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	30
80.246.130.117	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	26
149.50.73.197	United States	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	26
46.137.81.122	Ireland	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	10
2.54.49.229	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
5.28.191.166	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
74.63.228.226	United States	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
187.45.240.105	Brazil	147.237.77.17	mazi.idf.il	C1000003: HTTP: phpMyAdmin access	Block	3
66.249.64.124	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	3
151.80.31.150	Italy	147.237.77.17	mazi.idf.il	C1000228: HTTP: AhrefBot crawler	Block	2
66.249.64.2	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.153	Italy	147.237.77.17	mazi.idf.il	C1000228: HTTP: AhrefBot crawler	Block	2
66.249.64.8	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
2.54.139.180	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
199.244.88.182	United States	147.237.77.17	mazi.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
172.86.83.125		147.237.77.17	mazi.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
187.45.193.205	Brazil	147.237.77.17	mazi.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1

02-18-2016 to 02-19-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
46.137.81.122	Ireland	147.237.77.17	mazi.idf.il	SQL Injection - Select From	26
74.63.228.226	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	4
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.124	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.77.17	mazi.idf.il	ET DROP Dshield Block Listed Source	1

02-18-2016 to 02-19-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
87.69.255.49	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	128
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	60
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
212.76.127.10	Israel	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	45
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	40
52.7.46.16	United States	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	40
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	38
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	38
54.173.9.10	United States	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	37
212.76.127.219	Israel	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	32
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
84.228.101.7	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	30
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	28
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
84.228.101.7	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	24
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	20
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
54.85.198.156	United States	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	20
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	20
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
185.120.125.59		147.237.77.17	mazi.idf.il	drop	SAM rule	drop	18
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17

02-18-2016 to 02-19-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.108.63.117	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	7
66.87.78.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/3/5703.jpg.	Block	3
195.122.198.110	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
62.90.176.150	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
176.13.11.118	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in www.mazi.idf.il/14-he/igf.aspx	Block	2
95.86.110.135	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
40.77.167.12	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-11269-he/×¨×•×‘×•˜, ×″×“×•×¨ ×″×‘×?.aspx	Block	1
192.243.55.138	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8346-he	Block	1
192.243.55.133	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/www.idiegogo.com/projects/121440	Block	1
109.226.22.161	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
87.69.255.49	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
208.115.113.82	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-10104-he	Block	1
66.249.64.2	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.249.64.2	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
185.3.144.112	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
95.86.116.44	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/6510-9858-he/igf.aspx&sa=u&ved=0ahukewim1akeiollahxj1rqkhfmqdagqfggnmae&usg=afqjcnegtmrkn8v_e2u6e2z2fiyp4sgngw	Block	1
80.246.133.59	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
46.19.86.94	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	Block	1
109.226.44.156	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3849-5035-he/igf.aspx	Block	1
91.193.51.151	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/0/10310.jpg.com	Block	1
212.117.154.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
66.249.64.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-7712-he	Block	1
2.52.179.176	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7713-he	Block	1
185.3.144.112	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
104.131.46.154	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 104.131.46.154	Block	1
207.46.13.190	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3728-11581-he/Ã–Å“Ã–Å“Ã–Â? Ã–â€™Ã–â€˜Ã–â€¢Ã–Å“Ã–â€¢Ã–Âª.aspx	Block	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
157.55.39.95	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8338-he	Block	1
95.86.71.225	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4054-he/igf.aspx&sa=u&ved=0ahukewjv9y2khollahxceq8khr0xbmiqfggtmaq&usg=afqjcnfd4el7gd2fasjauco8ynofvfzn7q	Block	1
213.8.57.201	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.64.124	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4983-he	Block	1
31.154.158.89	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
192.243.55.137	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/general/×″	Block	1
185.27.105.160	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
104.131.46.154	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	Block	1
84.228.101.7	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8347-he	Block	1
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1

02-18-2016 to 02-19-2016