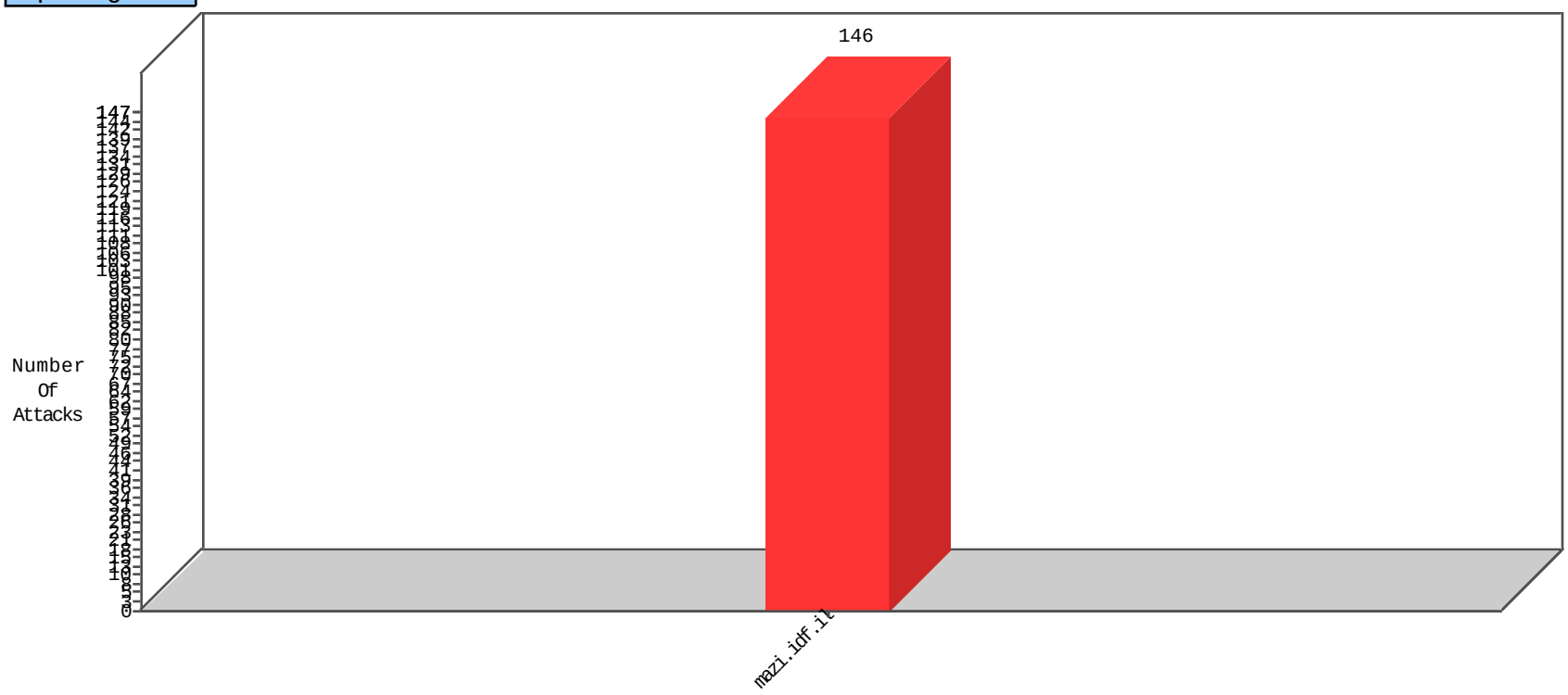
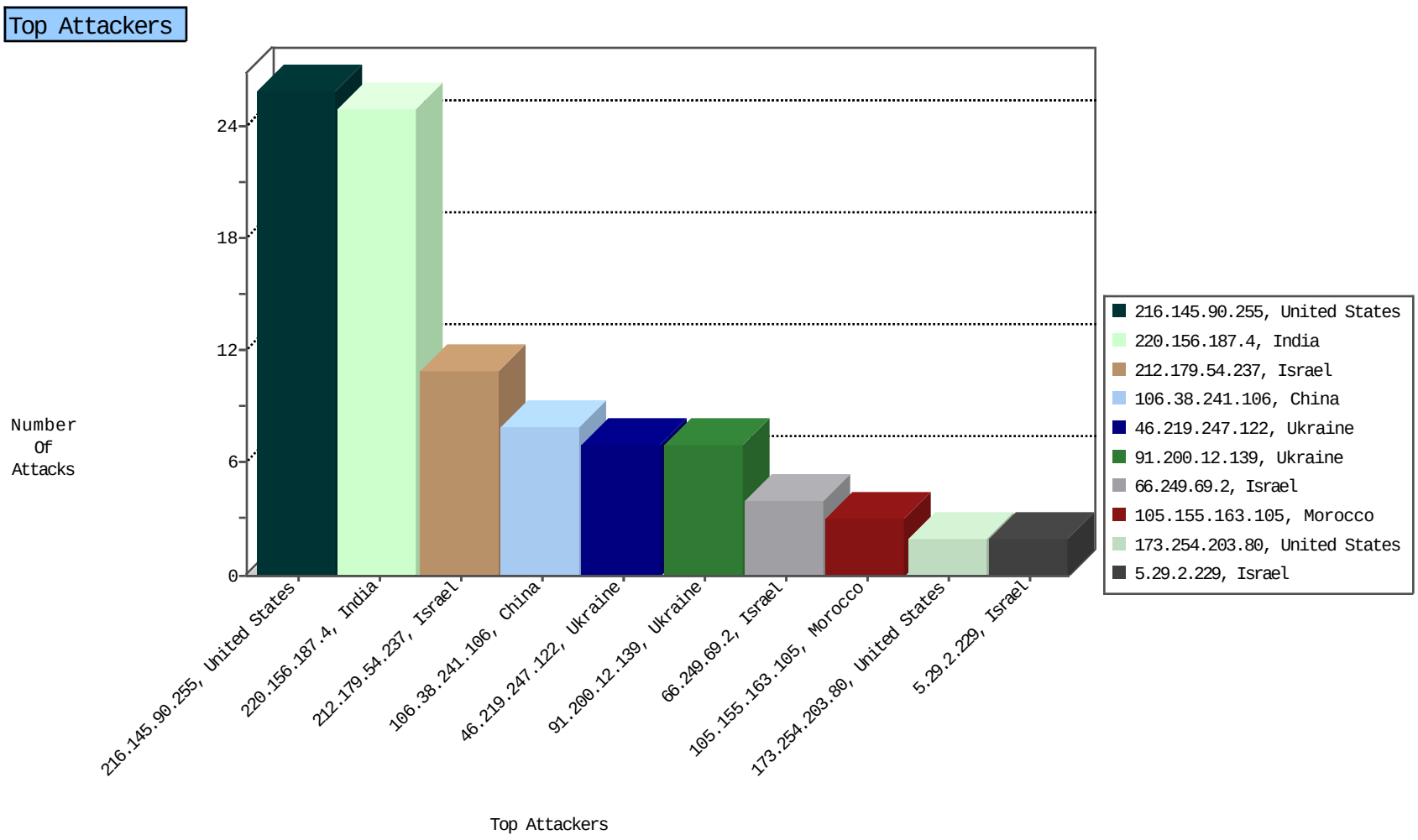
01-20-2016 to 01-21-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-20-2016 to 01-21-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	11

01-20-2016 to 01-21-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
216.145.90.255	United States	147.237.77.17	mazi.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	26
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	25
106.38.241.106	China	147.237.77.17	mazi.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	8
5.28.150.110	Israel	147.237.77.17	mazi.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
149.88.53.191	Israel	147.237.77.17	mazi.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
69.30.218.166	United States	147.237.77.17	mazi.idf.il	C106: HTTP: majestic bot	Block	2
79.181.123.166	Israel	147.237.77.17	mazi.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
188.165.15.136	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
207.46.13.122	United States	147.237.77.17	mazi.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.50	United States	147.237.77.17	mazi.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
185.73.39.108		147.237.77.17	mazi.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

01-20-2016 to 01-21-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.65.26	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
46.219.247.122	Ukraine	147.237.77.17	mazi.idf.il	SERVER-WEBAPP admin.php access	1
93.174.93.181	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
172.98.200.238		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1

01-20-2016 to 01-21-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.85.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
94.159.146.86	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
94.159.146.86	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
37.26.148.213	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	16
46.19.85.55	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
149.88.53.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	12
149.88.53.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.55	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
84.108.100.95	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.179.159.253	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
185.3.147.245	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
193.169.70.108	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.106.194	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.196	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.106	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
84.108.100.95	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
37.26.148.213	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.4.41	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.67.136.156	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.136	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
37.26.147.153	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
5.22.129.246	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.134.229	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.56	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
188.120.148.89	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.115.178	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.95	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.176.158.232	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
185.3.147.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.126	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
31.168.213.5	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.249.75.146	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
188.120.148.203	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.218	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
37.26.149.157	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.139.53.165	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.153.19	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
81.218.251.250	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
62.90.122.234	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.153	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.158.200	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.77	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
91.200.12.139	Ukraine	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 91.200.12.139	Block	4
109.65.165.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	2
91.200.12.139	Ukraine	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
46.219.247.122	Ukraine	147.237.77.17	mazi.idf.i	PHP Attempt	Block	2
149.78.29.73	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
46.219.247.122	Ukraine	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.219.247.122	Block	2
105.155.163.105	Morocco	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
5.29.2.229	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
79.181.211.119	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.75.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7713-he	Block	1
217.69.133.223	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	Block	1
157.55.39.50	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/5580-7562-he/igf.asp	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
46.19.86.53	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
79.179.3.160	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
66.249.69.98	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113	Block	1
195.62.53.168	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /admin/login	Block	1
128.70.102.149	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation lang in mazi.idf.il/forums/templates/forums/forum.aspx	Block	1
5.29.2.229	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
105.155.163.105	Morocco	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
79.181.211.119	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/general/x"	Block	1
173.254.203.80	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-10782-he/igf.aspx	Block	1
46.219.247.122	Ukraine	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
109.160.253.22	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
79.181.203.252	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.69.114	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.249.69.114	Block	1
207.46.13.117	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.65.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
5.29.227.158	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
105.155.163.105	Morocco	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-admin/admin-ajax.php	Block	1
84.108.184.59	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
68.180.230.40	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
173.254.203.80	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/wp-login.php	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6637-he/bayabasha.aspx	Block	1
46.219.247.122	Ukraine	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 46.219.247.122	Block	1
109.160.253.22	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
91.200.12.139	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he/igf.aspx/xmlrpc.php	Block	1
79.181.203.252	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.69.114	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3834-7267-he/igf.aspx.74	Block	1
212.29.203.226	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
157.55.39.49	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
66.249.65.245	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5039-he/igf.aspx	Block	1
5.29.227.158	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
109.65.56.39	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
84.108.184.59	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
79.179.3.160	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
188.162.40.177	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in mazi.idf.il/3793-he/igf.aspx	Block	1
128.70.102.149	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation ForumId in mazi.idf.il/forums/templates/forums/forum.aspx	Block	1