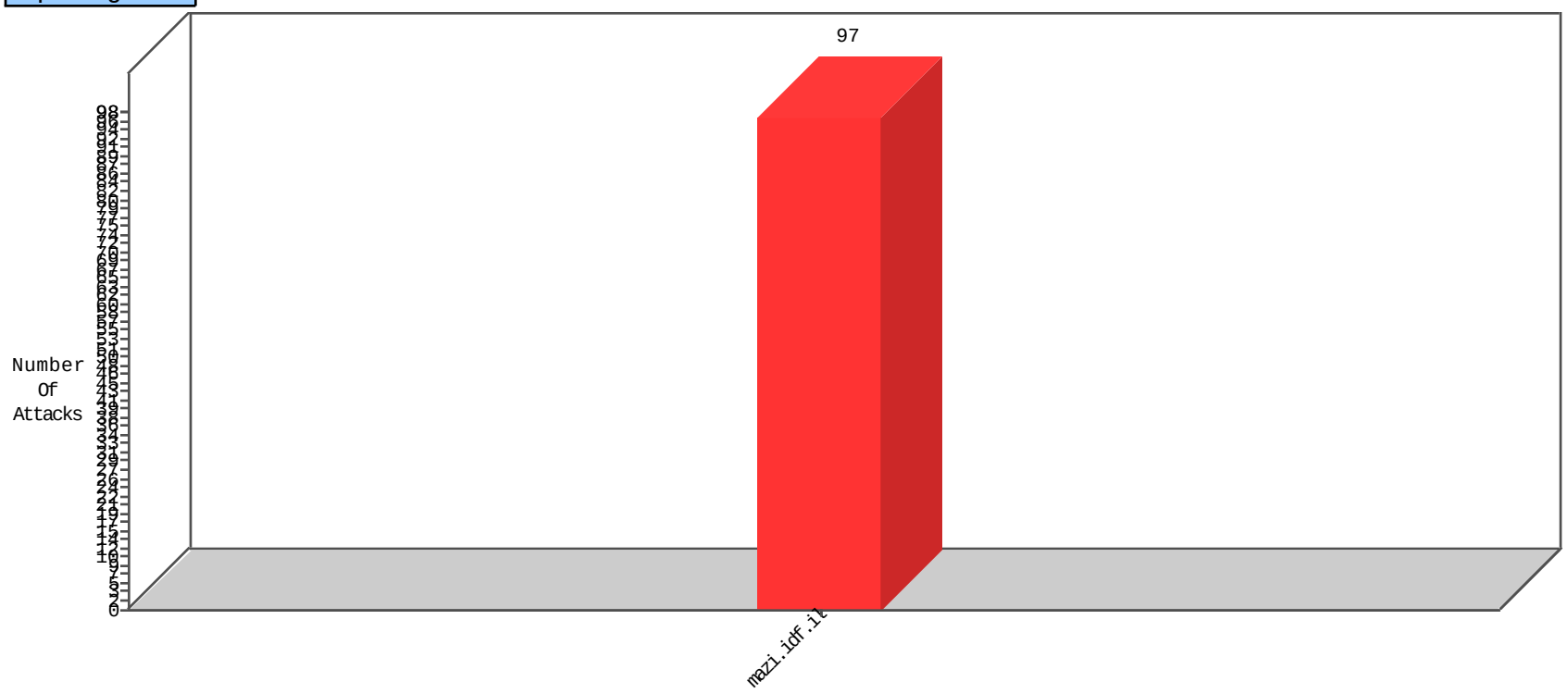
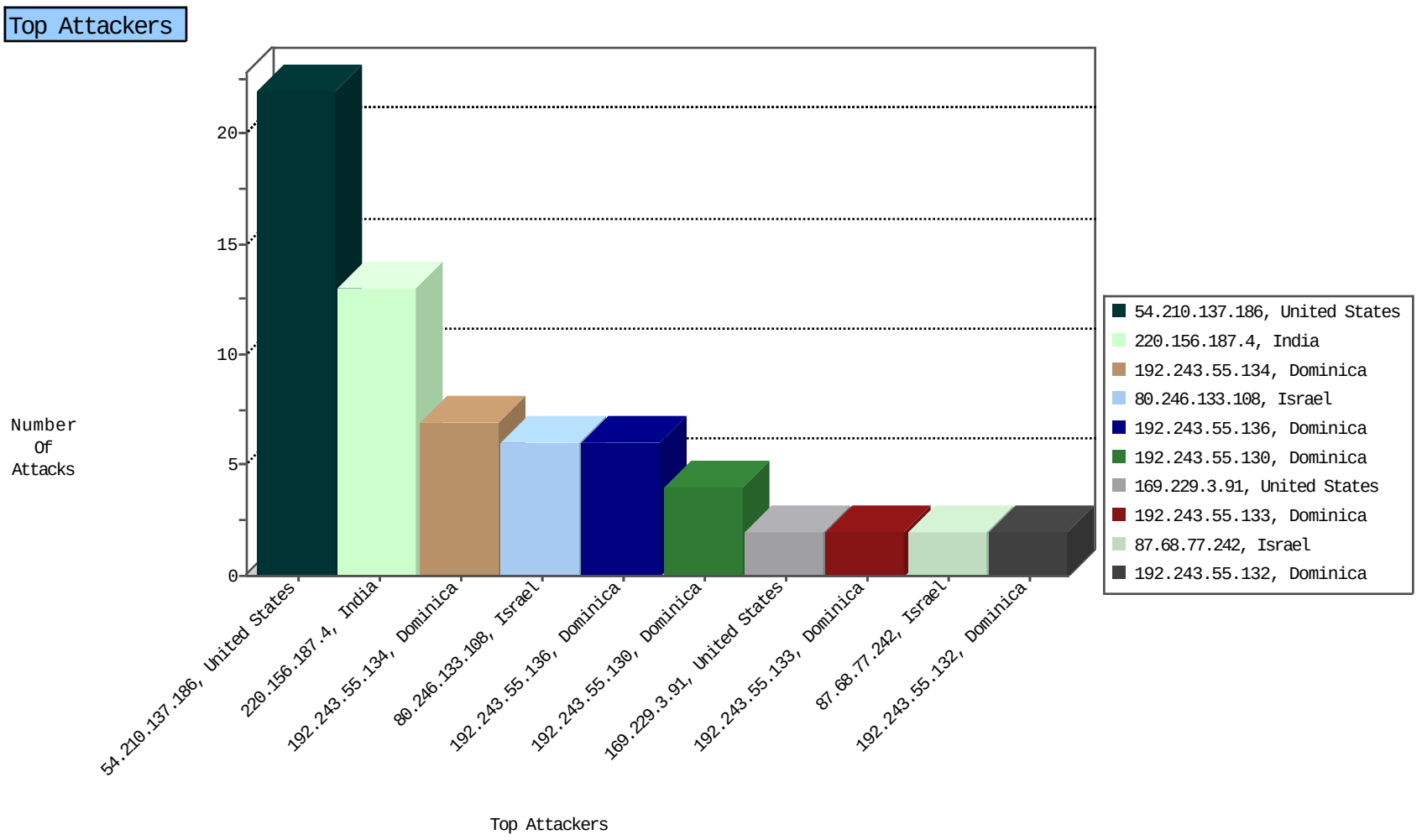
02-05-2016 to 02-06-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-05-2016 to 02-06-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

02-05-2016 to 02-06-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	13
202.69.240.221	Hong Kong	147.237.77.17	mazi.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

02-05-2016 to 02-06-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
89.248.172.154	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
183.22.40.161	China	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
111.137.177.143	China	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.6.142.254	Hungary	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

02-05-2016 to 02-06-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	117
54.210.137.186	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	38
194.73.99.35	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
85.65.173.131	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.116.6.234	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
217.132.36.147	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.32	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
85.64.24.193	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.32	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	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
85.64.24.193	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.34	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
212.29.197.181	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
46.19.85.34	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.110.109.98	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
149.78.138.192	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
87.68.245.100	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
84.110.109.98	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.173	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.173	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.75	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.144.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
79.183.110.73	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.144.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.131.43	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.158	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.191.130	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	4
5.102.254.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.196	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.120.219.220	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.196	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.173.131	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
2.54.132.54	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.56	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.29.197.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
5.22.131.75	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
54.72.73.168	Ireland	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.239	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.48	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.11.105	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
212.76.127.122	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.2	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.120.86.79	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	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
54.210.137.186	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 54.210.137.186	Block	11
54.210.137.186	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	8
80.246.133.108	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	6
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.134	Block	3
87.68.77.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
81.218.130.54	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
46.120.32.184	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
2.52.51.154	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7710-he	Block	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/newslist/newslist.in.aspxundefined	Block	1
194.73.99.35	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
79.176.13.32	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/www.idiegogo.com/projects/121440	Block	1
54.210.137.186	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/113-he/piwik.php	Block	1
5.102.254.141	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
192.243.55.132	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8335-he	Block	1
185.49.14.190	Poland	147.237.77.17	mazi.idf.i	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8350-he	Block	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7711-he	Block	1
54.167.183.116	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5222-he/igf.aspx	Block	1
2.54.154.19	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/4944-he/igf.aspx	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4980-he	Block	1
149.78.138.192	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
217.132.36.147	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
79.181.18.45	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
54.210.137.186	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-he/piwik.php	Block	1
192.243.55.133	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7713-he	Block	1
40.77.167.8	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
192.243.55.129	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
87.68.245.100	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
68.173.144.90	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/5551-11516-he/×ž×©×œ×‘×™×? ×§×″×™ ×œ×″.aspx	Block	1
2.54.186.73	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8346-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Abnormally Long Request from 169.229.3.91	Block	1
54.210.137.186	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/piwik.php	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7712-he	Block	1
192.243.55.133	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8345-he	Block	1
46.116.6.234	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
93.172.157.62	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-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/4070-11595-he/×ž×—×œ×§×ª ×ª×›× ×•× ×Ÿ ×•×‘×§×¨×″.aspx	Block	1
192.243.55.137	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/general/×″	Block	1
2.54.191.130	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
192.243.55.132	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.132	Block	1