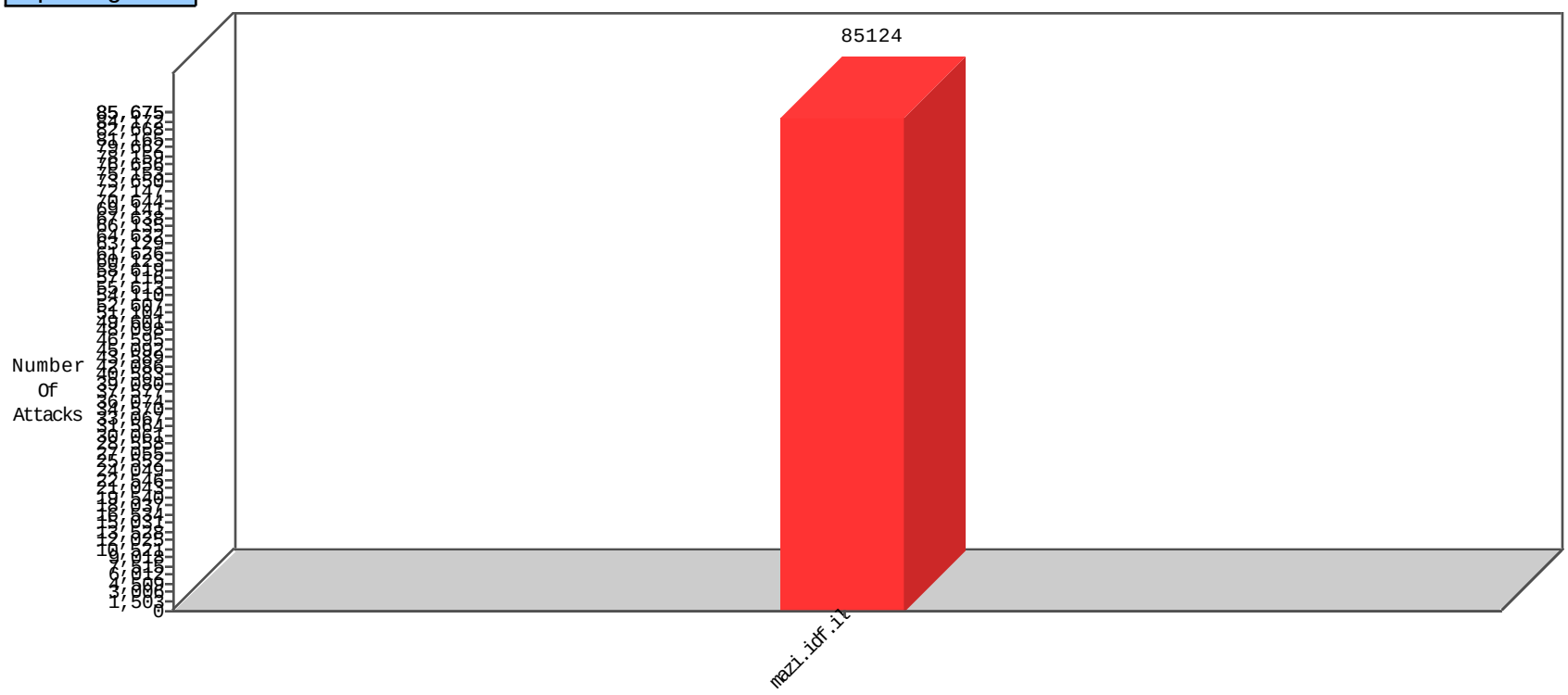
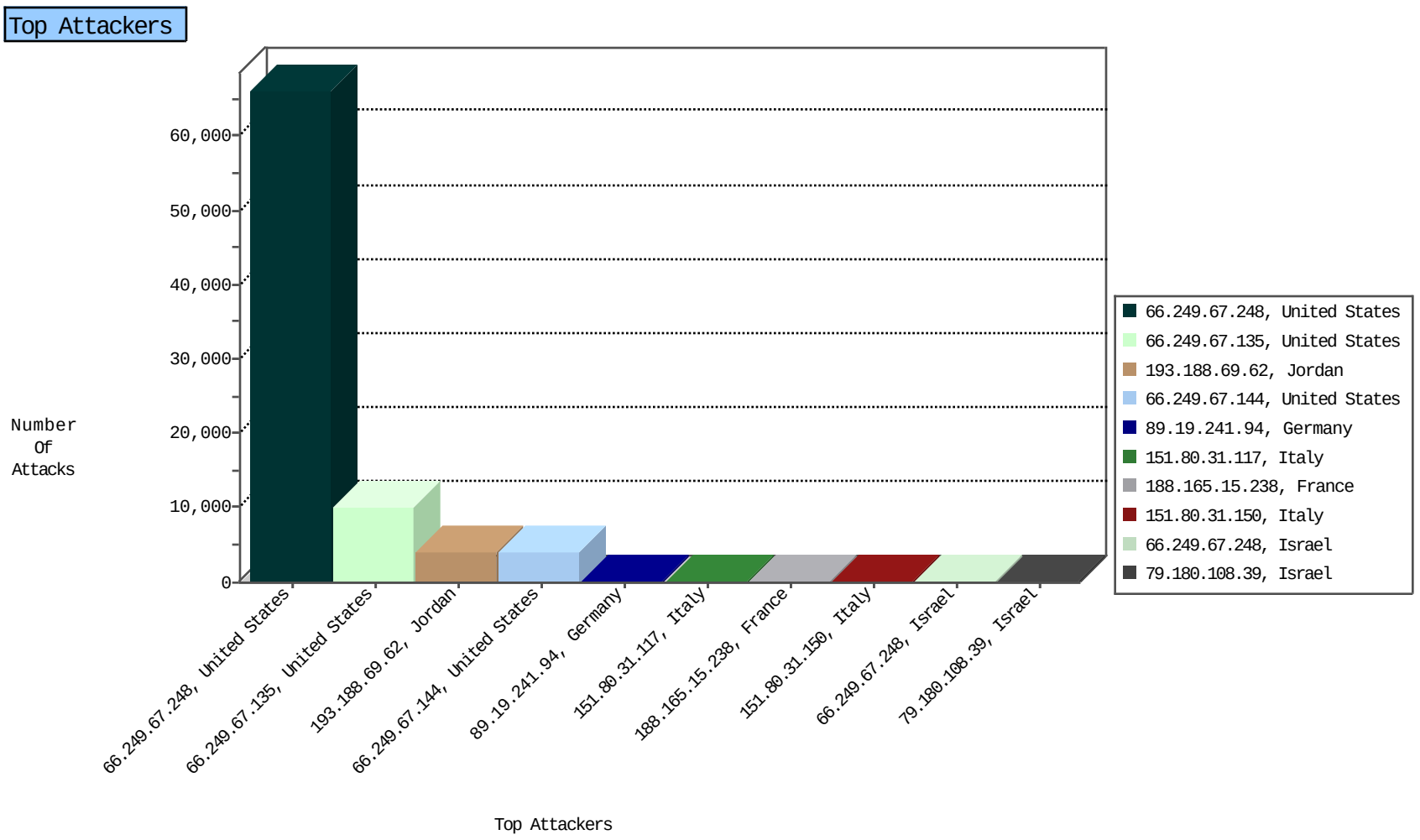
11-16-2015 to 11-17-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-16-2015 to 11-17-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.67.248	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	66255
66.249.67.135	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	10192
193.188.69.62	Jordan	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	4176
66.249.67.144	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	4160
79.180.108.39	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	6
167.88.12.212	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1
167.88.10.194	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1
167.88.12.202	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1
167.88.12.207	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

11-16-2015 to 11-17-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
89.19.241.94	Germany	147.237.77.17	mazi.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	170
151.80.31.117	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	70
188.165.15.238	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	9
151.80.31.150	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	6
151.80.31.145	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
220.156.184.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.235	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-16-2015 to 11-17-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.67.248	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.135	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
115.25.138.225	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
1.235.195.234	Korea, Republic of	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
1.235.195.234	Korea, Republic of	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1
23.102.186.35	United States	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.24.122		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.64.109	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
94.159.177.100	Israel	147.237.77.17	mazi.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	1
116.249.183.6	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
1.235.195.234	Korea, Republic of	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
5.10.74.196	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
40.115.58.160	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.189.8	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.109	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
81.231.190.105	Sweden	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	1

11-16-2015 to 11-17-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
151.80.31.145	Italy	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	53
208.115.111.75	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	42
94.228.34.249	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	41
157.55.39.242	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	30
176.13.19.243	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
192.117.110.196	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
66.249.81.217	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
192.117.110.196	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
66.102.9.91	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.85.233	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
91.197.103.1	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
94.230.86.212	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
91.197.103.1	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	16
188.120.148.152	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
2.52.3.186	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
66.249.81.220	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
157.55.39.70	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
207.46.13.139	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
66.249.67.144	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
31.154.94.17	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	9
149.78.49.220	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
31.154.94.17	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
157.55.39.242	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	8
5.22.134.127	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
94.228.34.249	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	6
46.117.152.77	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
157.55.39.88	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
212.117.143.250	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.67.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.67.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.95	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
207.232.27.5	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
213.244.82.139	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.81.216	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
190.195.57.99	Argentina	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.3.186	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
81.218.38.70	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.111.66.45	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
84.108.212.18	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.19.103.247	France	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
2.52.3.186	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.23.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.250.135.233	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.12.157	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
110.171.55.158	Thailand	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.1	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
81.218.38.70	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
2.54.142.171	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.148	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

11-16-2015 to 11-17-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	3
95.86.123.37	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	2
132.70.66.9	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	Block	2
66.249.67.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	2
109.186.160.79	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4223-he/igf.aspx	Block	1
207.46.13.139	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8347-he	Block	1
66.249.67.135	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	1
5.28.166.217	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
141.0.10.1	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
66.249.67.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
157.55.39.70	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4085-he/	Block	1
40.117.44.123	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
110.4.66.170	Korea, Republic of	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in URL /5772-8123-he/igf.aspx	Block	1
85.64.1.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.67.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5013-he/igfhistory.aspx	Block	1
207.46.13.172	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/4070-11595-he/×ž×—×œ×§×ª ×ª×›× ×• ×Ÿ ×•×'×§×¨×″.aspx	Block	1
5.102.221.115	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
157.55.39.61	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 157.55.39.61	Block	1
104.128.144.131	Canada	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	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
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
207.46.13.21	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8671-he	Block	1
46.117.152.77	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
110.93.162.90	Korea, Republic of	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in URL /4169-he/igf.aspx	Block	1
94.229.74.91	United Kingdom	147.237.77.17	mazi.idf.i	Parameter Type Violation FileID in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
66.249.67.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/591-he/handasa.aspx	Block	1
207.46.13.177	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
5.102.250.209	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
157.55.39.61	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
104.236.220.248		147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on /	Block	1
68.180.229.218	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-he	Block	1
207.46.13.139	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
49.238.140.171	Korea, Republic of	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in URL /7006-11075-he/igf.aspx	Block	1
94.229.74.91	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-he/igf.aspx'	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5222-he/igf.aspx	Block	1
210.112.96.116	Korea, Republic of	147.237.77.17	mazi.idf.i	Distributed Illegal Byte Code Character in URL	Block	1
37.26.147.213	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
157.55.39.70	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
79.178.141.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/	Block	1

11-16-2015 to 11-17-2015