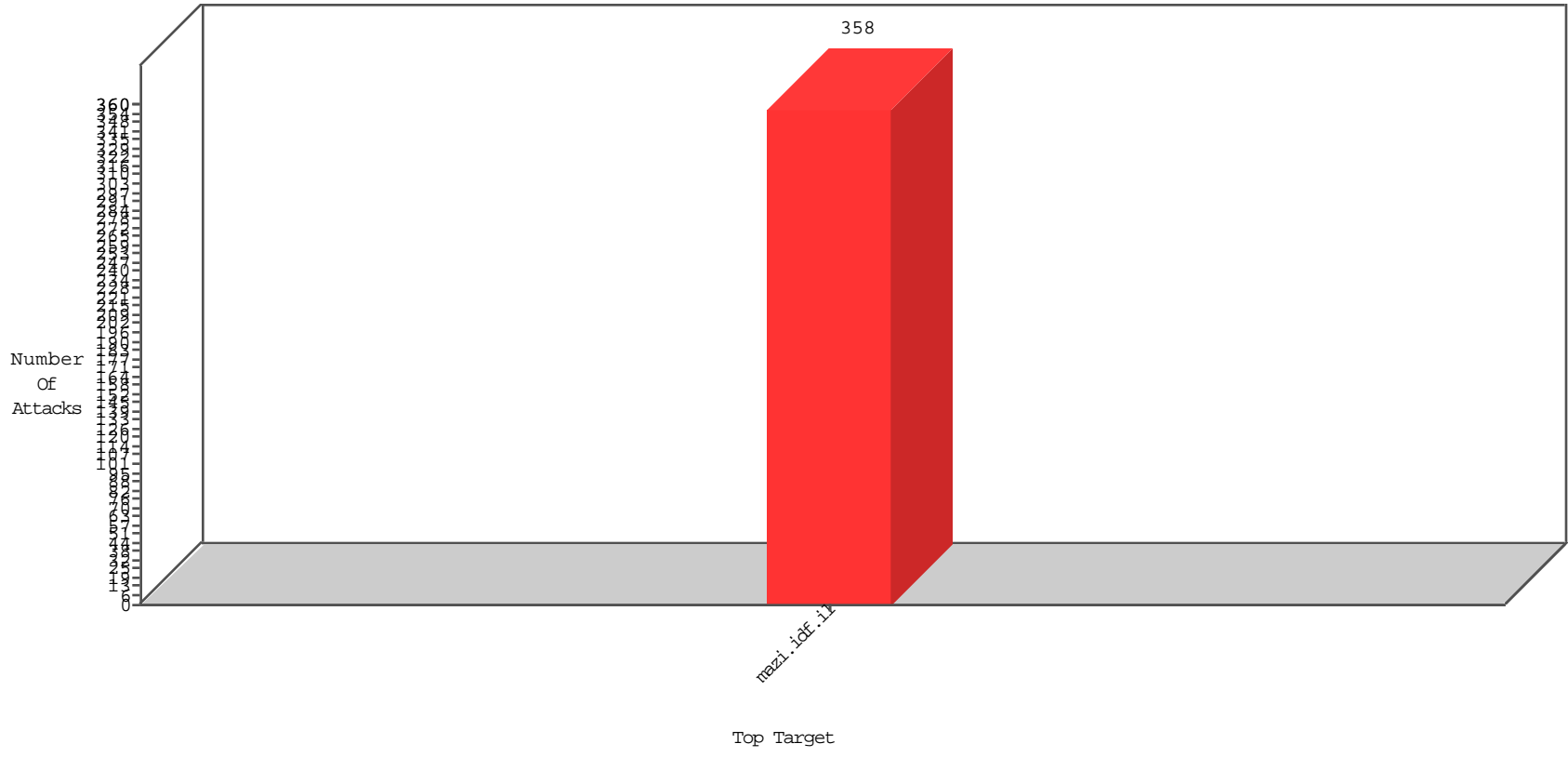


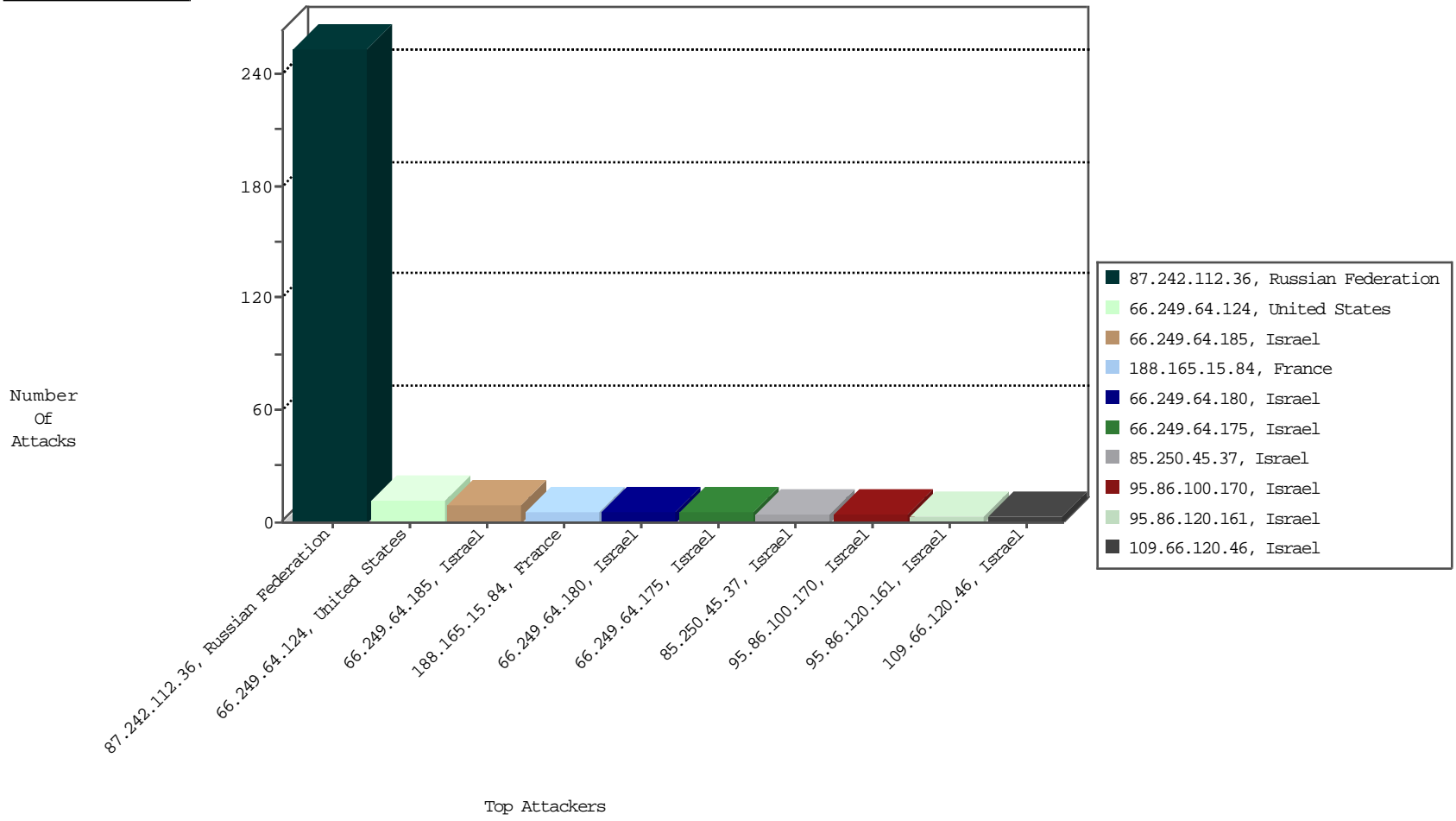
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



11-26-2015 to 11-27-2015

Top Attackers In DDoS-Defence

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

11-26-2015 to 11-27-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
87.242.112.36	Russian Federation	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	188
87.242.112.36	Russian Federation	147.237.77.17	mazi.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	15
188.165.15.84	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	6
95.86.100.170	Israel	147.237.77.17	mazi.idf.il	Cl000004: HTTP: options method (Microsoft)	Block	4
188.165.15.129	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
87.242.112.36	Russian Federation	147.237.77.17	mazi.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
87.242.112.36	Russian Federation	147.237.77.17	mazi.idf.i	SQL Injection - Select From	50
66.249.64.124	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	12
66.249.64.2	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	2
111.49.145.192	China	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
176.60.67.55	Belarus	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
181.54.250.11	Colombia	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.43.236.38	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 3072	1
122.96.31.28	China	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.22.179.67	Brazil	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
208.115.111.75	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	42
104.191.128.135	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
37.26.146.194	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
176.106.45.85	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	22
79.183.10.109	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.120.156.245	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.86.71	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.146.200	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
87.69.208.74	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.1	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.139.5	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
5.29.58.35	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
213.57.139.5	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.168.80.114	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
194.114.146.227	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
157.55.39.117	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.141.14	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.57.148.200	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.108.120.67	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
171.99.187.71	Thailand	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.71	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.51	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
78.15.116.53	Italy	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.174	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.117.154.144	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
157.55.39.61	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.13	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
85.130.133.7	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.132.42.23	Netherlands	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
80.246.133.33	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.115.248.2	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.191.249	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.249.64.2	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.131	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.120	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.51	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.182	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
128.177.161.163	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.107	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.64.112	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.110.7.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
212.179.57.94	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.117.154.144	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.117	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.36	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.164	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.83.149	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
2.54.155.120	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
85.250.45.37	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ufi/reaction/	Block	4
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	4
95.86.120.161	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	3
185.120.126.89		147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
213.151.36.250	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/675-he/igf.aspx&sa=u&ved=0ahukewic6ouk4kzjahvdxqbqkhcjrddqfgglmae&sig2=ijh3yh2ouimhdtydrihlzq&usg=afqjcnhattfpq7lqglywg5qdmstes23ic_q	Block	2
66.249.64.8	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.249.64.8	Block	2
95.86.120.56	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/4/1154.pdf&sa=u&ved=0ahukewinu7hs063jahwctbokhv4zbnicfggmmmai&usg=afqjcnh-nqmojsmdiqkoy4ziipogorku9a	Block	2
8.37.71.31	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/41-he/igf.aspx&usg=alkjrhix5y3csxqjimsy3_wdvr3suvwg	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-7591-he/igf.aspx	Block	1
157.55.39.117	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
46.19.85.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1
79.176.1.76	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
31.210.189.252	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
5.29.58.35	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9318-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
66.249.64.8	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/591-he/mazi.aspxs	Block	1
84.108.145.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
37.142.188.69	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
8.37.71.59	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5078-6077-he/igf.aspx&usg=alkjrhix8tok6v_keydkq3hpcwgezihskg	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5484-7282-he/igf.aspx	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9554-he/igf.aspx	Block	1
46.19.86.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
87.69.165.43	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/ufi/reaction/	Block	1
79.176.176.247	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/	Block	1
37.46.39.101	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
8.37.70.83	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/62-he/igf.aspx&usg=alkjrhnbwdwjchxjk9kxzjgefesz4nugqa	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/165-7456-he/igf.aspx	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-6976-he/igf.aspx	Block	1
157.55.39.58	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he/	Block	1
66.249.64.26	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in igf.idf.il/5010-he/igf.aspx	Block	1
37.142.188.69	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
85.65.185.40	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.64.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-5475-he	Block	1
8.37.71.95	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/70-he/igf.aspx&usg=alkjrhgggluzxd0hoesxwn8w-vmlzyxykla	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
213.8.71.26	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/7/6117.jpg	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-6165-he/igf.aspx	Block	1
46.31.103.54	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
87.69.204.136	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
79.176.197.151	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ufi/reaction/	Block	1
37.46.39.101	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
8.37.70.99	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/70-he/igf.aspx&usg=alkjrhikfow6bbrhzip25tier0rrf6xqqiq	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-9547-he/igf.aspx	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4932-5689-he/igf.aspx	Block	1
157.55.39.58	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/599-he/totchanim.aspx	Block	1
66.249.64.124	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-7710-he	Block	1
40.77.167.84	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
85.65.185.40	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9357-he/igf.aspx	Block	1
31.210.189.252	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
5.22.134.154	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4932-8181-he/igf.aspx	Block	1
79.182.16.176	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
37.142.123.31	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1