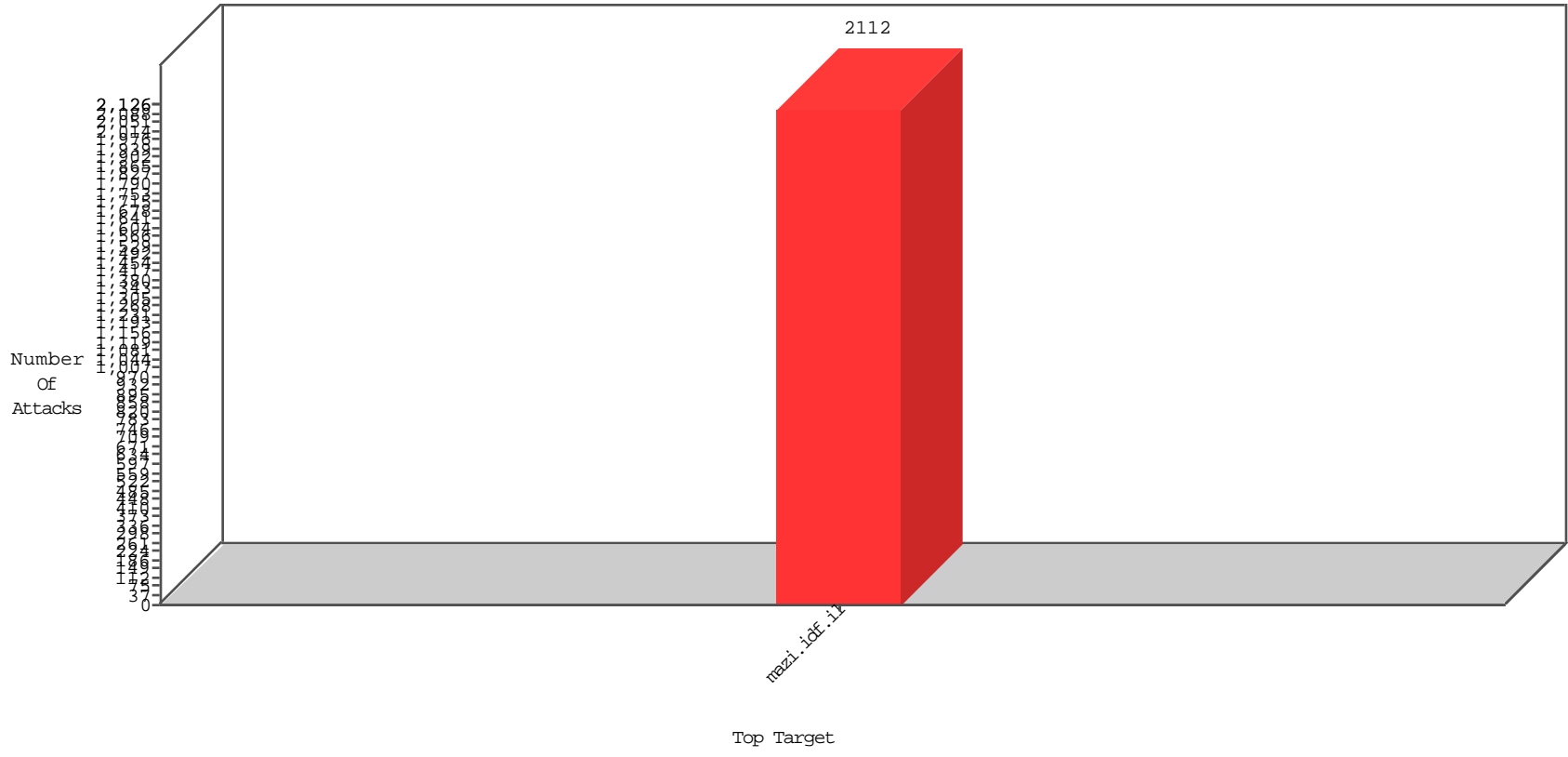


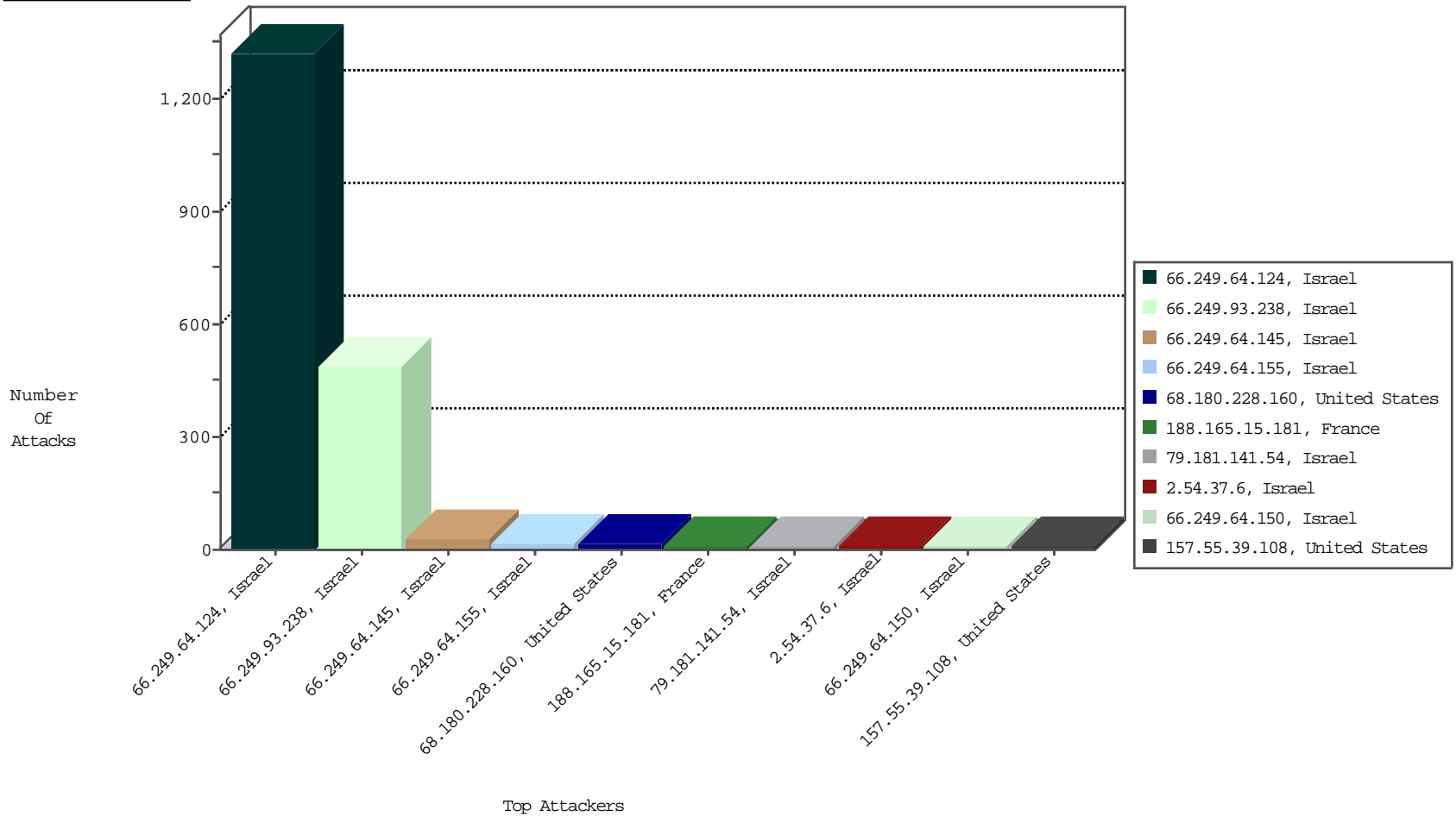
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



08-29-2015 to 08-30-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.64.124	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1324
66.249.93.238	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	490

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
5.102.197.171	Israel	147.237.77.17	mazi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.67.109.2	Israel	147.237.77.17	mazi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
79.181.97.154	Israel	147.237.77.17	mazi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
149.78.201.158	United States	147.237.77.17	mazi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
81.218.144.203	Israel	147.237.77.17	mazi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
93.173.5.156	Israel	147.237.77.17	mazi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
37.26.149.192	Israel	147.237.77.17	mazi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.64.124	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	8
198.36.50.80	United States	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
91.220.163.43	Ukraine	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
95.106.119.24	Russian Federation	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
183.60.175.149	China	147.237.77.17	mazi.idf.i	ET SCAN NMAP -f -sS	1
183.60.175.149	China	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 3072	1
189.202.241.84	Mexico	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 4096	1
196.47.173.21	Cote D'Ivoire	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 4096	1
94.102.48.193	Netherlands	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
121.15.202.84	China	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.175.149	China	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 2048	1
189.202.241.84	Mexico	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 3072	1
196.47.173.21	Cote D'Ivoire	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
31.210.186.159	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
5.29.178.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.82	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.48	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.98	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.56	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
5.102.254.204	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.55	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.65	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
81.218.144.203	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
79.183.55.69	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.230	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.17	mazi.idf.i	drop		drop	4
46.19.86.95	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.245	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
54.244.22.103	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	3
213.57.166.252	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
213.57.166.252	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
194.225.185.5	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.221	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.238	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.46.39.211	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Response out of state	monitor	1
194.225.185.5	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.20	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.155	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.48	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.193	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.149	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.46.39.47	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

08-29-2015 to 08-30-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.54.37.6	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	12
79.181.141.54	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	12
66.249.64.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-8769-he/igf.aspx	Block	6
66.249.64.145	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4146-he/igf.aspx	Block	6
180.76.15.149	China	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/	Block	6
180.76.15.5	China	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/	Block	6
157.55.39.108	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	6
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/igf.aspx	Block	6
188.165.15.181	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/70-he/igf.aspx	Block	6
66.249.64.150	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6369-9586-he/igf.aspx	Block	6
66.249.64.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	6
180.76.15.25	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	6
157.55.39.237	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/113-11269-he/x"x"x"x"x", x"x"x"x"x" x"x"x"x?.aspx	Block	6
85.250.85.119	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	6
66.249.64.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	6
180.76.15.156	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	6
66.249.64.145	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4170-he/igf.aspx	Block	6
180.76.15.10	China	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/	Block	6
157.55.39.108	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/4/3544.jpg	Block	6
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /	Block	6
207.46.13.76	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	6
66.249.64.150	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	6
66.249.64.16	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in igf.idf.il/3793-he/igf.aspx	Block	6
180.76.15.135	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	6
157.55.39.253	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-7712-he	Block	6
93.172.155.193	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	6
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-10104-he	Block	6
188.165.15.136	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/594-he/igf.aspx	Block	6
66.249.64.145	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4439-he/igf.aspx	Block	6
180.76.15.12	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	6
157.55.39.180	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/8/7588.jpg	Block	6
66.249.64.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4623-he/igf.aspx	Block	6
66.249.64.145	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	6
180.76.15.143	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	6
157.55.39.253	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3728-11581-he/xæxæx? x'x'x'x'xæxæxæxæx.a.aspx	Block	6
109.253.159.82	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	6
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8335-he	Block	6
188.165.15.181	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-he/igf.aspx	Block	6
66.249.64.145	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5222-6398-he/igf.aspx	Block	6
5.102.197.171	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	6
180.76.15.19	China	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/	Block	6
157.55.39.181	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/6/7406.jpg	Block	6
81.218.144.203	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	6

08-29-2015 to 08-30-2015