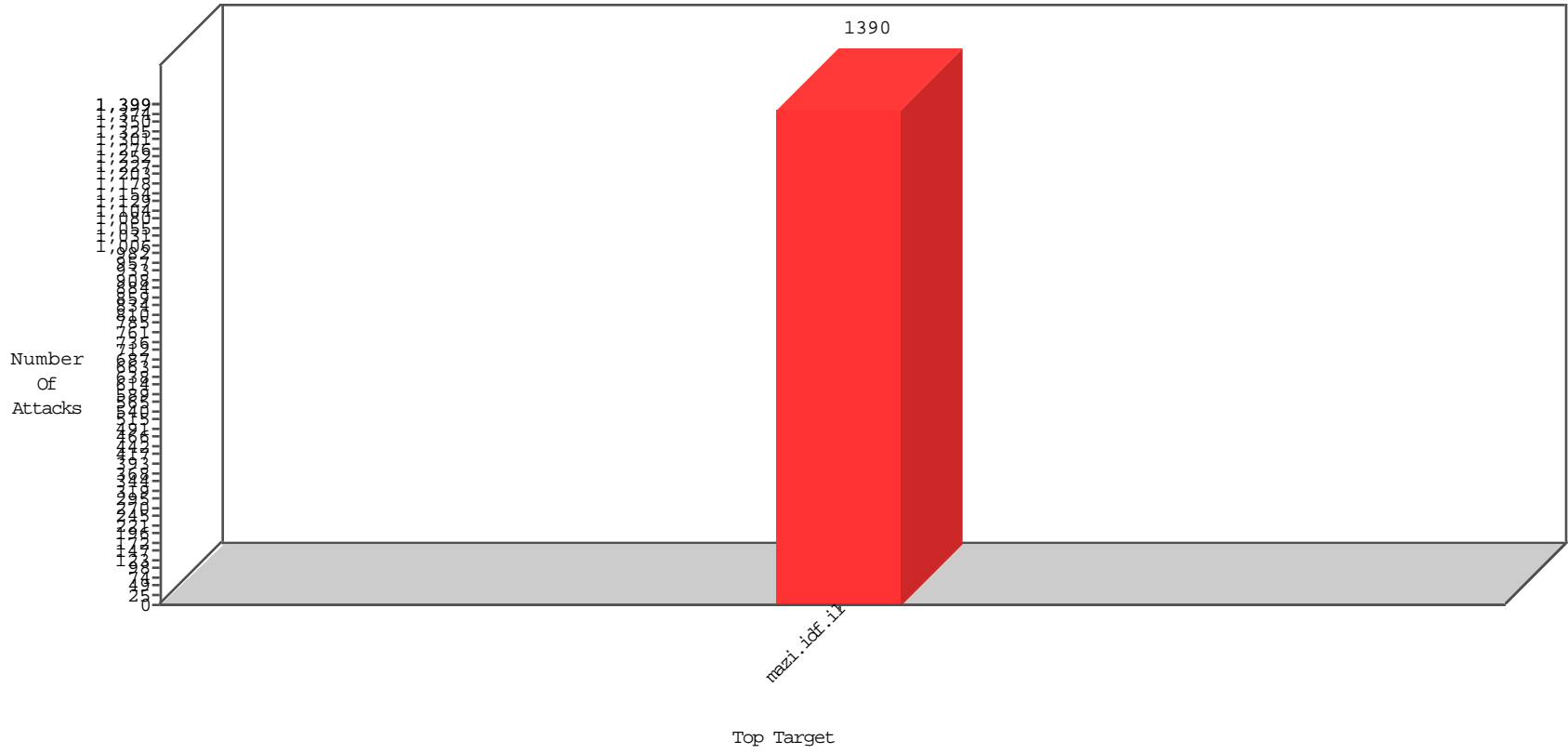


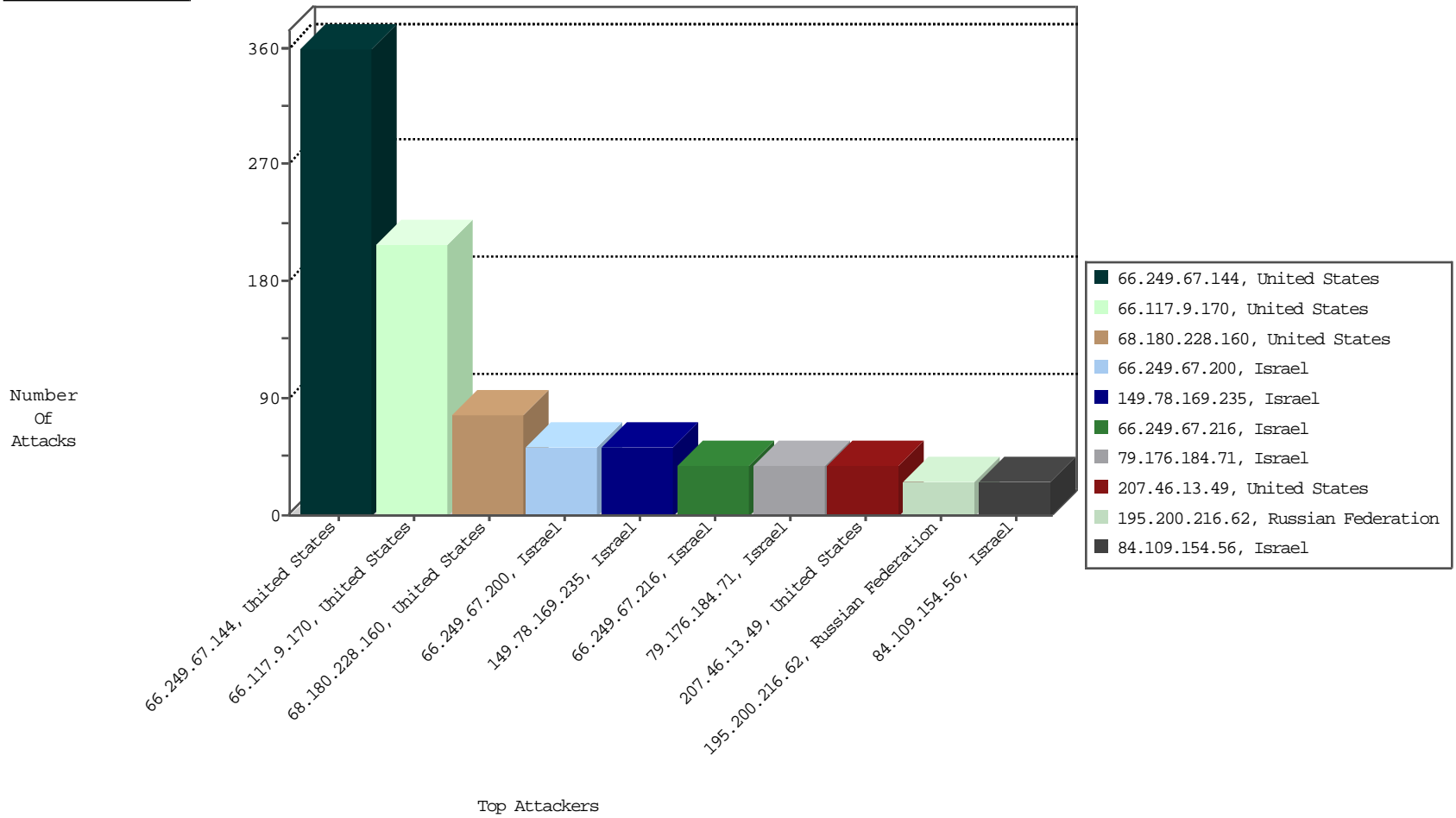
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.67.144	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	358
62.219.254.22	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	15

10-20-2015 to 10-21-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.17	mazi.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

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)	16
66.249.67.135	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.144	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
114.112.90.54	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
159.226.230.13	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
40.115.63.150	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
104.171.122.161	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1
158.75.37.253	Poland	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	1
40.115.63.150	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
40.115.63.150	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.161	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.85.102	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.102	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
31.168.99.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
31.168.99.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
5.22.130.138	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
46.116.252.23	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.209	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.148.84	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
94.230.86.138	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
110.171.37.147	Thailand	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.130.138	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	1
5.22.129.206	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
177.15.128.123	Brazil	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.181.130.142	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
94.230.86.242	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.130.138	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
180.97.63.35	China	147.237.77.17	mazi.idf.i	Directory Traversal	directory traversal overflow	monitor	1
80.246.130.108	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
95.35.16.78	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
199.203.215.1	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
80.246.130.108	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
31.168.178.170	Israel	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
66.117.9.170	United States	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 66.117.9.170	Block	91
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8344-he	Block	78
149.78.169.235	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	52
66.117.9.170	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	52
79.176.184.71	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4070-11595-he/xžx-xæx\$xa xaxx x*xÿ x*x'x\$xx".aspx	Block	39
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	39
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	39
66.117.9.170	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.117.9.170	Block	39
195.200.216.62	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	26
84.109.154.56	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/resource/userfollowresource/create/	Block	26
31.210.187.229	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in www.mazi.idf.il/14-he/igf.aspx	Block	26
66.117.9.170	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/config/help_new.php	Block	13
157.55.39.251	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/113-11581-he/xæxæ? x'x'x*xæx*x.a.aspx	Block	13
46.116.252.23	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	13
149.78.161.33	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	13
66.249.93.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	13
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	13
207.46.13.49	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4995-he/igf.aspx	Block	13
188.165.15.23	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7713-he	Block	13
157.55.39.109	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6051-he/igf.aspx	Block	13
66.199.231.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	13
199.203.215.1	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/iptac-564d6202f45eddd2ddd5-6204e359e234/s0001/444d5a5c7463333334 333240646d7a65736c--1445325545--3552--1445259543--369cd3d3598e229d89b 12a8e6d6e751d31f2015080c0208877df8ae6a31ffe34/http://mazi.idf.il/webresource.axd	Block	13
180.97.63.35	China	147.237.77.17	mazi.idf.i	URL is Above Root Directory mazi.idf.il/./shared/clientscripts/jquery.min.js	Block	13
46.121.88.210	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3849-5035-he/igf.aspx	Block	13
66.249.93.245	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/571-he/igf.aspx	Block	13
207.46.13.167	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-9151-he/igf.aspx	Block	13
188.165.15.230	France	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 188.165.15.230	Block	13
157.55.39.222	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6050-he/igf.aspx	Block	13
66.249.67.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	13
66.249.67.95	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to ww.mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	13
207.46.13.49	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/	Block	13
180.97.106.162	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	13
62.210.247.93	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	Block	13
157.55.39.69	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/62-he/igf.aspx	Block	13
207.46.13.167	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5013-9133-he/igf.aspx	Block	13
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	13
188.165.15.230	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3697-9630-he/igf.aspx 10 x'x x*x'xžx'x" 2010	Block	13
157.55.39.223	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/120-he/igf.aspx	Block	13
89.139.168.197	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/xæxæ? x'x'x*xæx* x.a.aspx	Block	13
66.249.93.239	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/571-he/igf.aspx	Block	13
66.249.67.144	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	13
207.46.13.49	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/101-he/igf.aspx	Block	13
183.57.153.133	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/webresource.axd%3fd	Block	13
66.117.9.170	United States	147.237.77.17	mazi.idf.i	Admin Blocking	Block	13
157.55.39.69	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	13
77.126.16.213	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation _EVENTTARGET in mazi.idf.il/700-he/igf.aspx	Block	13
212.76.99.253	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	13
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	13