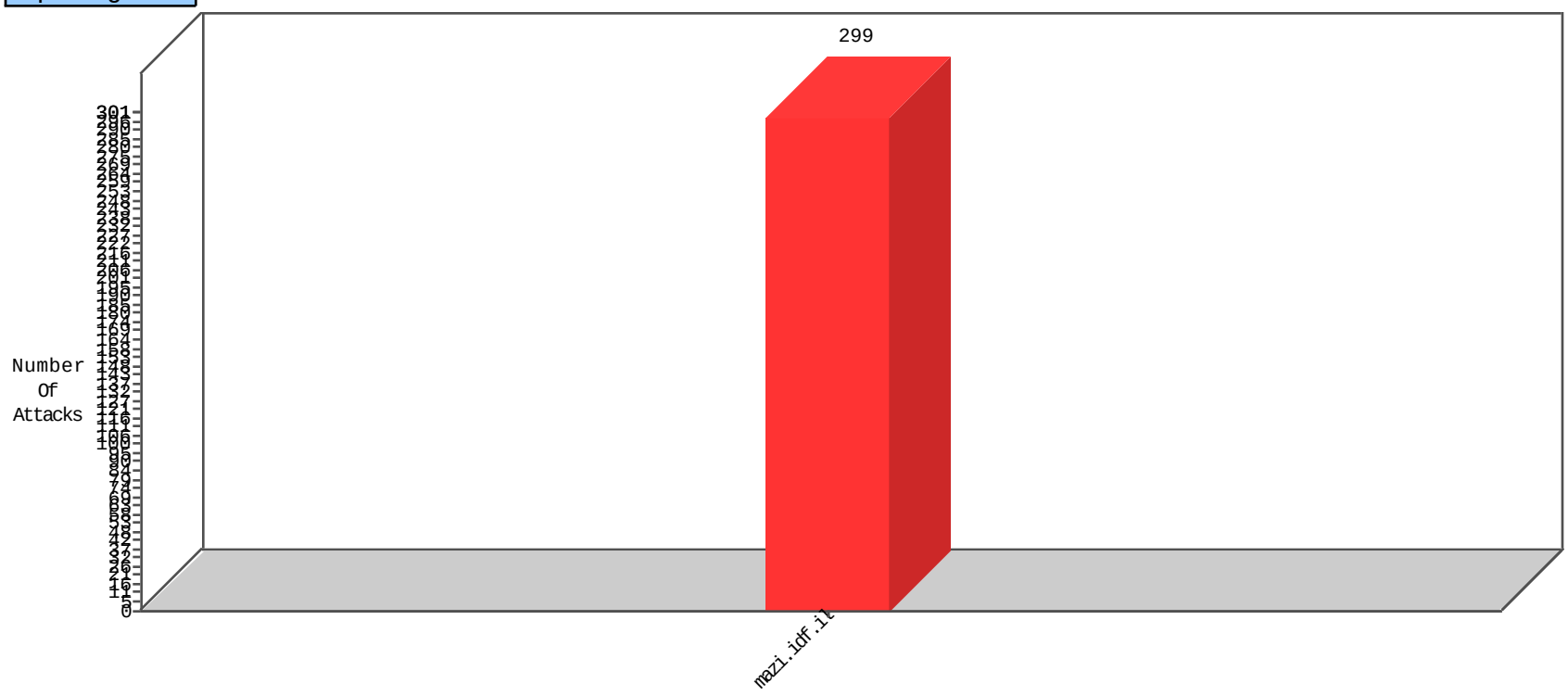
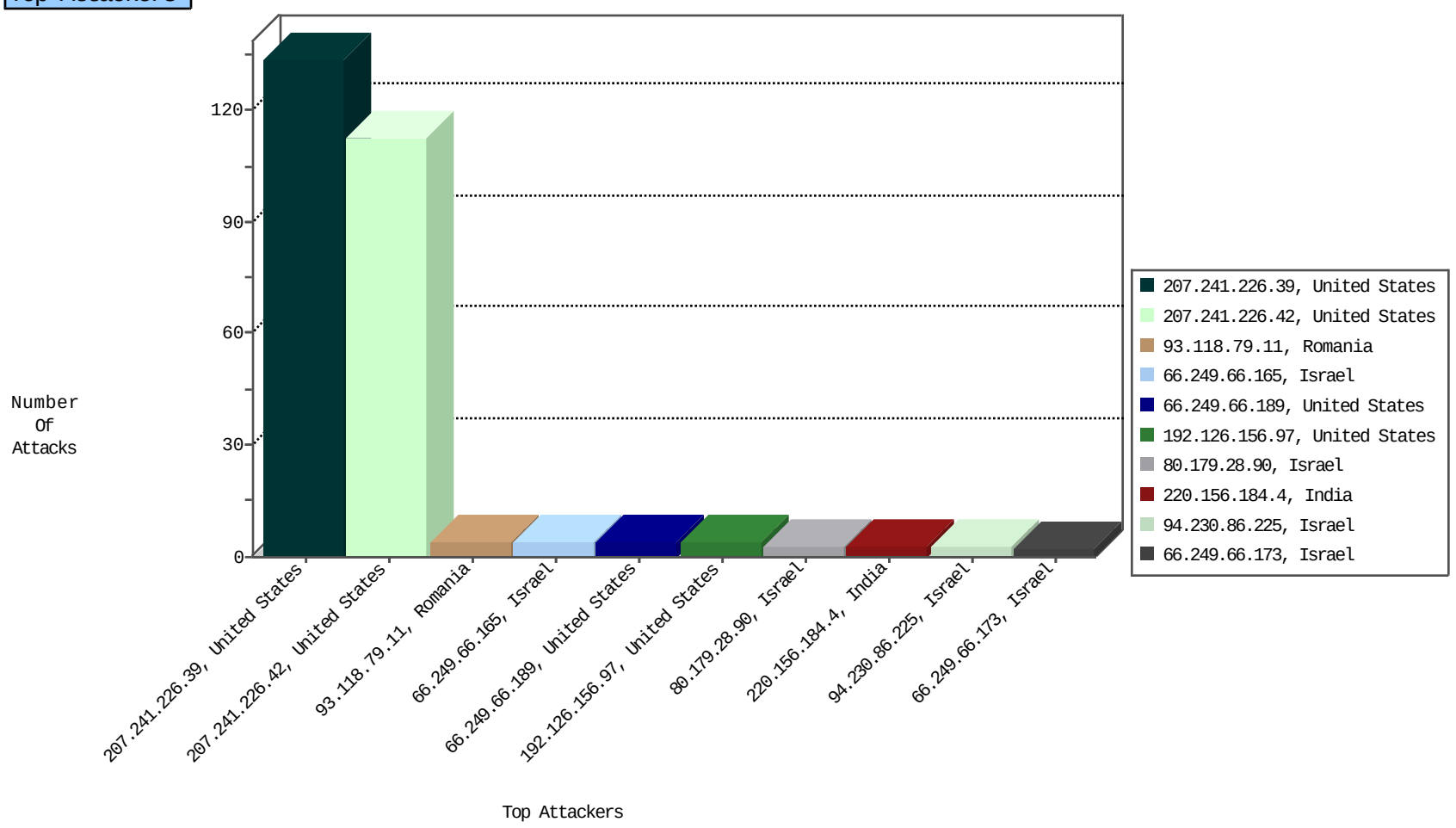
12-14-2015 to 12-15-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-14-2015 to 12-15-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.179.6.184	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	2
37.46.171.237	Sweden	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1

12-14-2015 to 12-15-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.184.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	3

12-14-2015 to 12-15-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.66.189	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	4
117.206.133.246	India	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
210.117.121.60	Korea, Republic of	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
87.81.210.189	United Kingdom	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
137.117.34.247	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
80.0.165.64	United Kingdom	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1

12-14-2015 to 12-15-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
94.230.86.225	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	33
46.19.86.216	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
149.88.148.16	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
37.26.147.242	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.52.11.227	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
185.3.144.129	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.139	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.125	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.26.146.140	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
149.88.148.16	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.57.160.27	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
5.22.129.100	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.105.24	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
213.57.129.200	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.193	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.162.121	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.129.200	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.193	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.146.140	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.129.200	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
188.120.148.131	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.66.189	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.146.213	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.193	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
149.88.188.68	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.7	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.146.140	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
149.88.188.68	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.57	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.33.12	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
216.218.206.90	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.58	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
95.35.41.52	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.219	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
79.179.205.112	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.142.105.42	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.225.231.122	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.242	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.110	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.77	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.43	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
87.69.181.229	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

12-14-2015 to 12-15-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
207.241.226.42	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.241.226.42	Block	75
207.241.226.39	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.241.226.39	Block	71
207.241.226.39	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	62
207.241.226.42	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	37
192.126.156.97	United States	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	4
93.118.79.11	Romania	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	4
80.179.28.90	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 80.179.28.90	Block	3
94.230.86.225	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	3
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	2
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-9347-he/igf.aspx	Block	1
136.243.36.96	Germany	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
79.178.19.188	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-7123-he/igf.aspx	Block	1
207.241.226.42	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5551-7550-he/piwik.php	Block	1
84.108.105.24	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
69.30.244.186	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/503-he/igf.aspx	Block	1
207.241.226.39	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/4315-he/piwik.php	Block	1
136.243.36.96	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/5551-11516-he/×ž×©×œ×‘×™×? ×§×”×™×œ×” .aspx	Block	1
79.178.19.188	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
37.26.149.171	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
207.46.13.46	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
69.30.244.186	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-login.php	Block	1
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-10288-he/igf.aspx	Block	1
141.212.122.64	United States	147.237.77.17	mazi.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.189	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
77.75.76.172	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
141.212.122.97	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /x	Block	1
82.81.81.214	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in mazi.idf.il/4170-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/templates/general/×”	Block	1

12-14-2015 to 12-15-2015