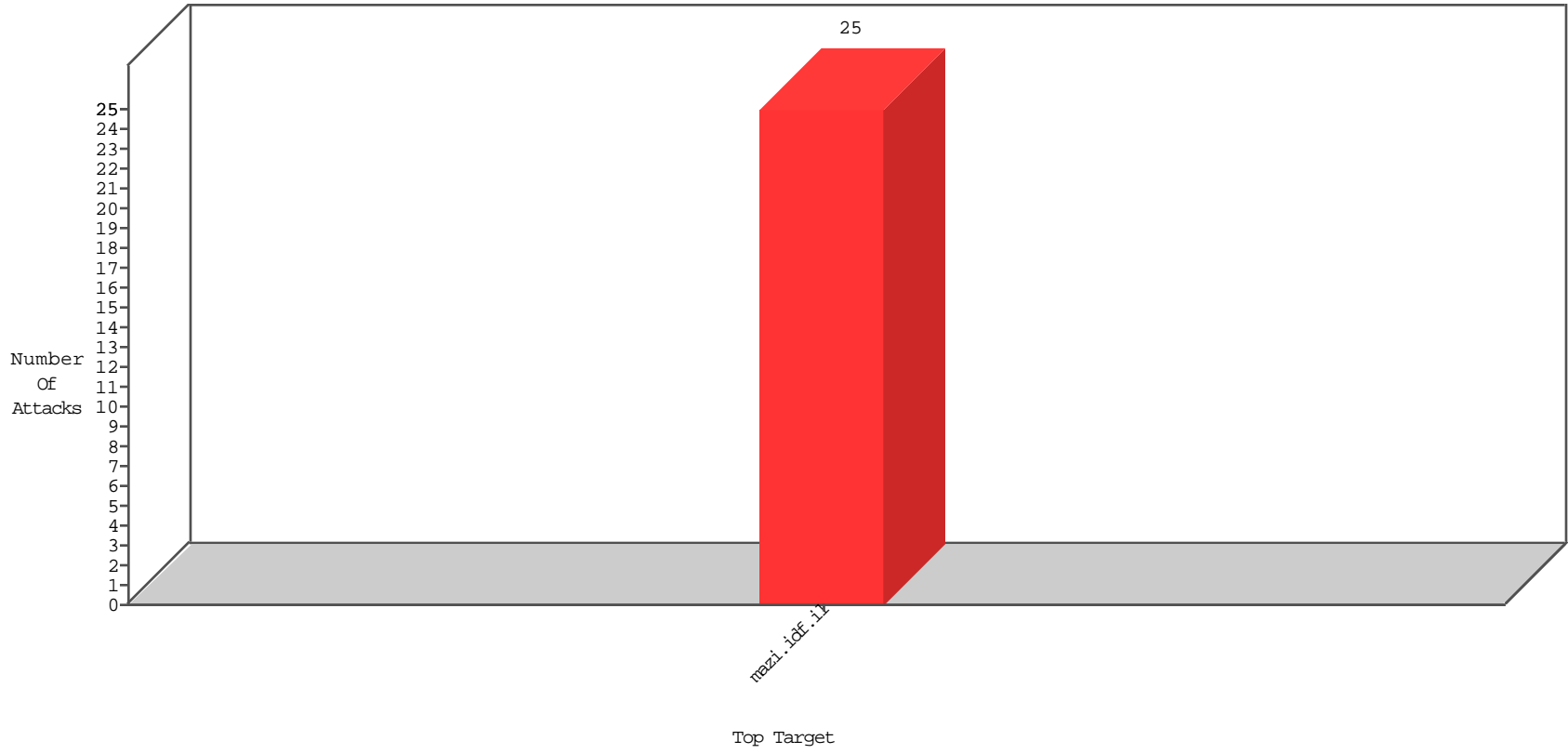


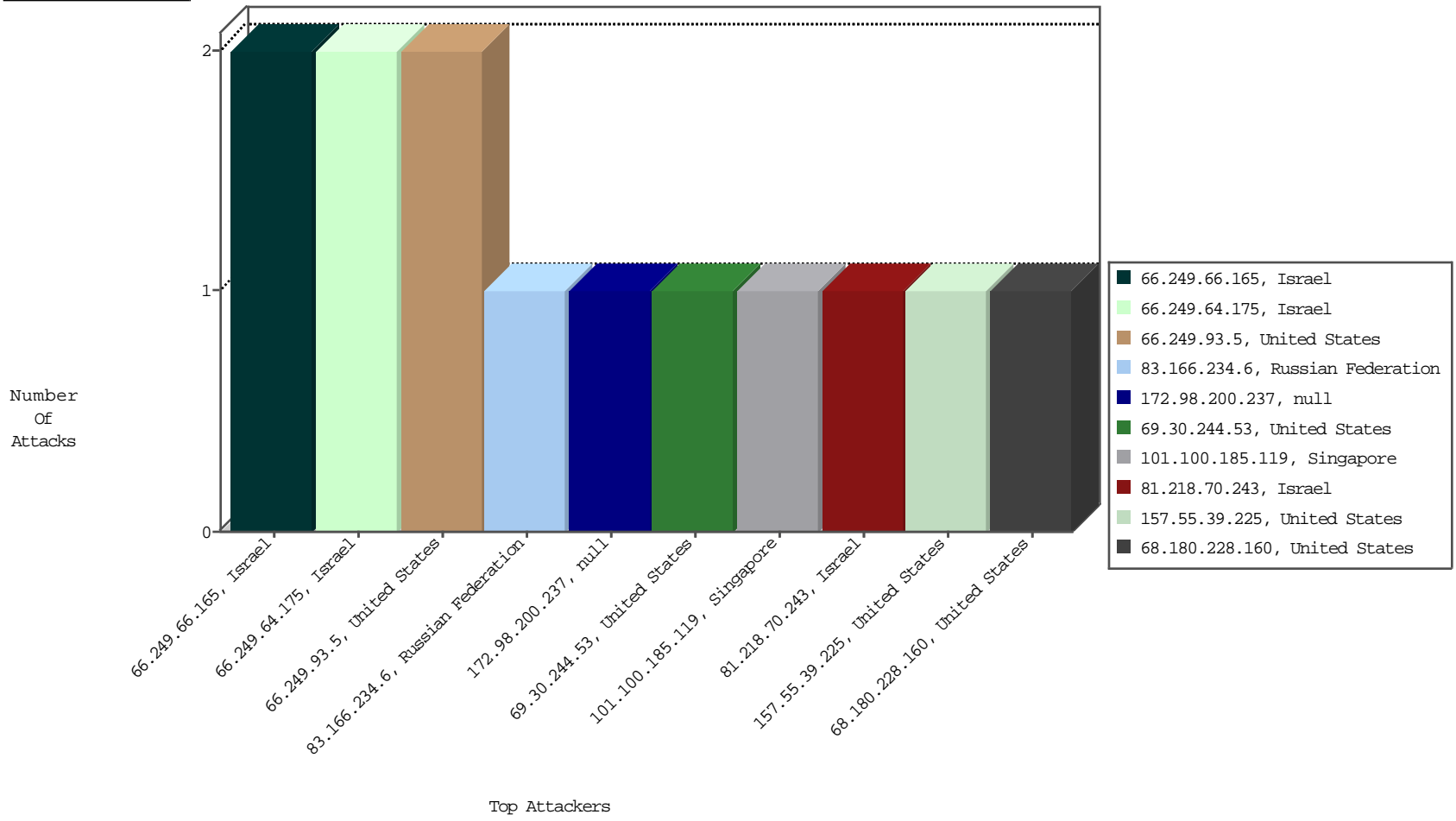
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



01-17-2016 to 01-18-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
------------------	--------------	----------------	------	-----------	---------------	----------------------	-------

01-17-2016 to 01-18-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.93.5	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
172.98.200.237		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
101.100.185.119	Singapore	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	81
149.78.198.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
201.175.20.39	Mexico	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
37.26.146.172	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
212.48.81.89	United Kingdom	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	17
46.19.85.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.117.108.59	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
80.250.155.217	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
5.22.135.136	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
5.102.254.126	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.86.125	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.86.223	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.66.168.249	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.142.171.176	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.166	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.129	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
89.138.123.150	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.142.171.176	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.119.176	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.137	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
77.126.60.144	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.166	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.168.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.46	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.211.34.236	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	3
46.117.108.59	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
2.54.8.231	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
109.66.168.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.131.49	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.85.156	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
84.109.137.130	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
80.179.9.7	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.13.100.117	Ireland	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
162.216.46.148	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.64	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.45.18.178	United States	147.237.77.17	mazi.idf.i	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
216.218.206.91	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.103	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.80.180.229	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.61	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
69.30.244.53	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.212	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.254.63	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.198.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

01-17-2016 to 01-18-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.181.13.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
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	1
87.69.220.100	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
69.30.244.53	United States	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	1
46.117.24.241	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
157.55.39.3	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
81.218.70.243	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 81.218.70.243	Block	1
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
89.138.123.150	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/3/1613.jpg	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4146-he/igf.aspx	Block	1
157.55.39.225	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1
83.166.234.6	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
67.149.1.135	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	1
109.65.137.88	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
79.180.211.145	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	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
85.158.139.228	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-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/14-8333-he	Block	1
141.212.122.81	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /x	Block	1

01-17-2016 to 01-18-2016