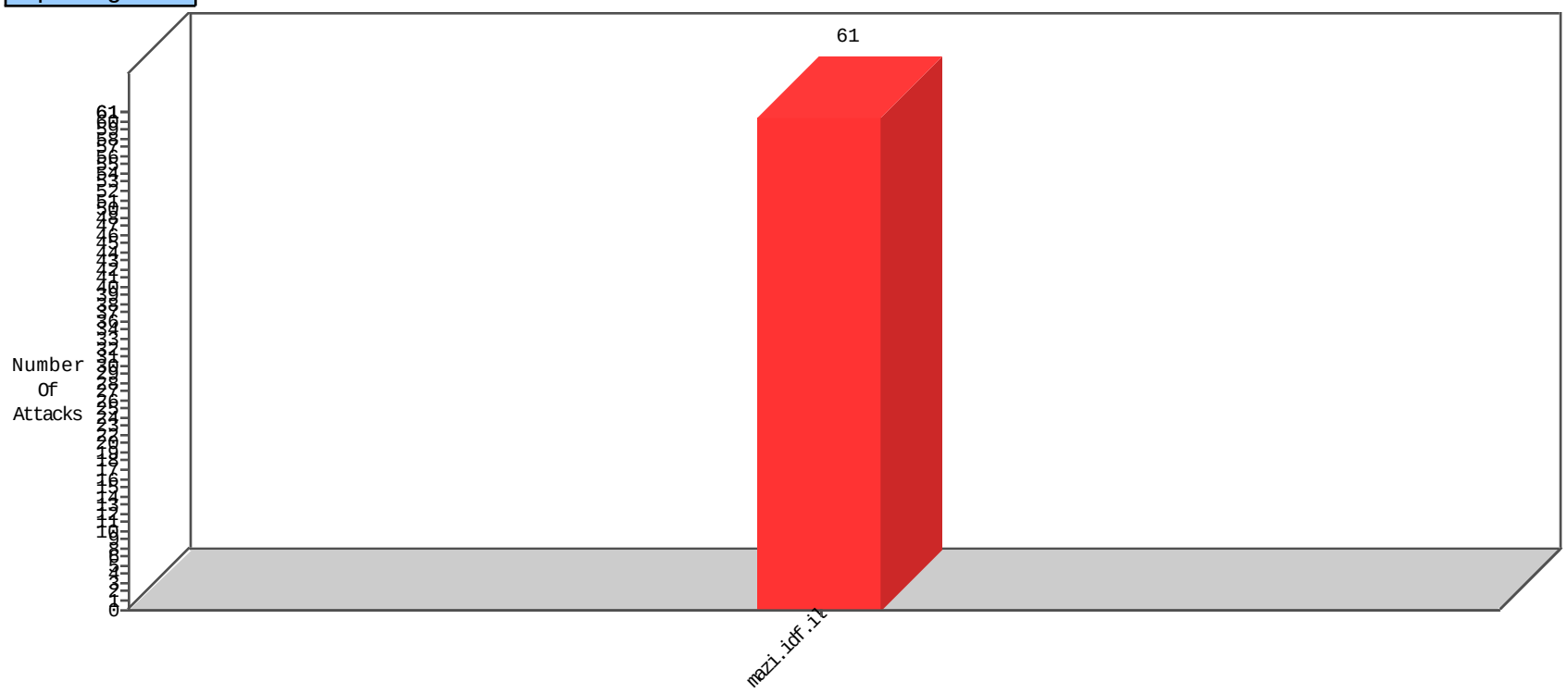
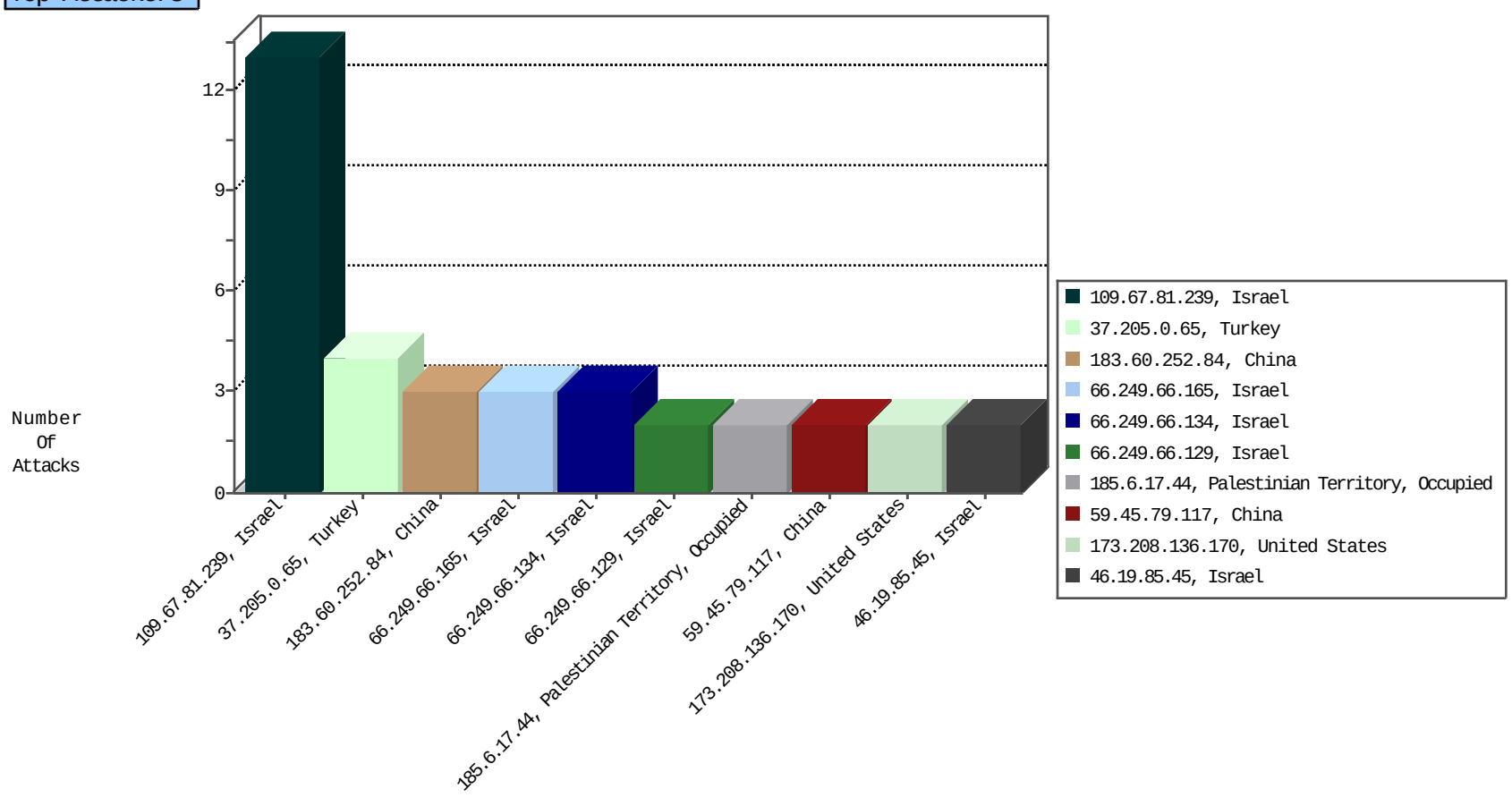
01-13-2016 to 01-14-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-13-2016 to 01-14-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
142.54.168.142	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

01-13-2016 to 01-14-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
37.205.0.65	Turkey	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-13-2016 to 01-14-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
37.205.0.65	Turkey	147.237.77.17	mazi.idf.il	SQL Injection - Select From	3
66.249.81.220	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	2
183.60.252.84	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
45.32.36.233		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.252.84	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
195.24.37.185	Bulgaria	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
40.115.58.160	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	Ukraine	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.252.84	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1

01-13-2016 to 01-14-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.143.170.69	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	900
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
212.235.28.71	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	36
54.244.22.103	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
46.19.85.226	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.226	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
54.244.22.103	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
46.19.85.201	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
37.26.146.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
149.78.93.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
54.244.22.103	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.91	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
37.26.146.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
149.78.93.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
54.244.22.103	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
37.26.147.254	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
54.244.22.103	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
37.26.147.254	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
176.12.160.2	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.181.144.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.117.141.208	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.254	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
173.208.136.170	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
78.211.51.11	France	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.130.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.13	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.170.124	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
2.54.171.15	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
149.88.37.126	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
149.88.37.126	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.153.50	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
93.172.169.153	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.19.119.186	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.3.144.56	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.228.62.132	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.6	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.42	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.76.15.34	China	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.3	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.228.222	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.148	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.178.145.134	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.240.144.67	China	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
185.35.62.186	Switzerland	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.120.70.24	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
171.25.193.132	Sweden	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

01-13-2016 to 01-14-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.67.81.239	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/images/transvideocounter.gif	Block	9
109.67.81.239	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 109.67.81.239	Block	2
109.67.81.239	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
46.19.85.45	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/×œ×œ×? ×’ ×‘×•×œ×•×ª.aspx	Block	2
66.249.66.134	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.249.66.134	Block	2
185.6.17.44	Palestinian Territory, Occupied	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/robots.txt	Block	1
66.249.66.129	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8334-he	Block	1
193.169.86.17	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
173.208.136.170	United States	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 173.208.136.170	Block	1
77.75.79.109	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.66.153	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6510-9854-he/igf.aspx	Block	1
5.29.88.158	Israel	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	1
187.161.187.84	Mexico	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /tmunblock.cgi	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
66.249.66.129	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	Block	1
207.46.13.35	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
173.208.136.170	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 173.208.136.170	Block	1
79.182.139.115	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
188.143.232.26	Russian Federation	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 188.143.232.26	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-9220-he/igf.aspx	Block	1
207.46.13.93	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6221-9268-he/igf.aspx	Block	1
185.6.17.44	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 185.6.17.44	Block	1
84.228.29.54	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/resource/userfollowresource/create/	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5039-he/igf.aspx	Block	1
66.249.66.49	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
192.118.92.3	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/sip_storage/files/7/11467.jpg	Block	1
141.212.122.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	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
66.249.66.134	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	Block	1
212.179.42.225	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1

01-13-2016 to 01-14-2016