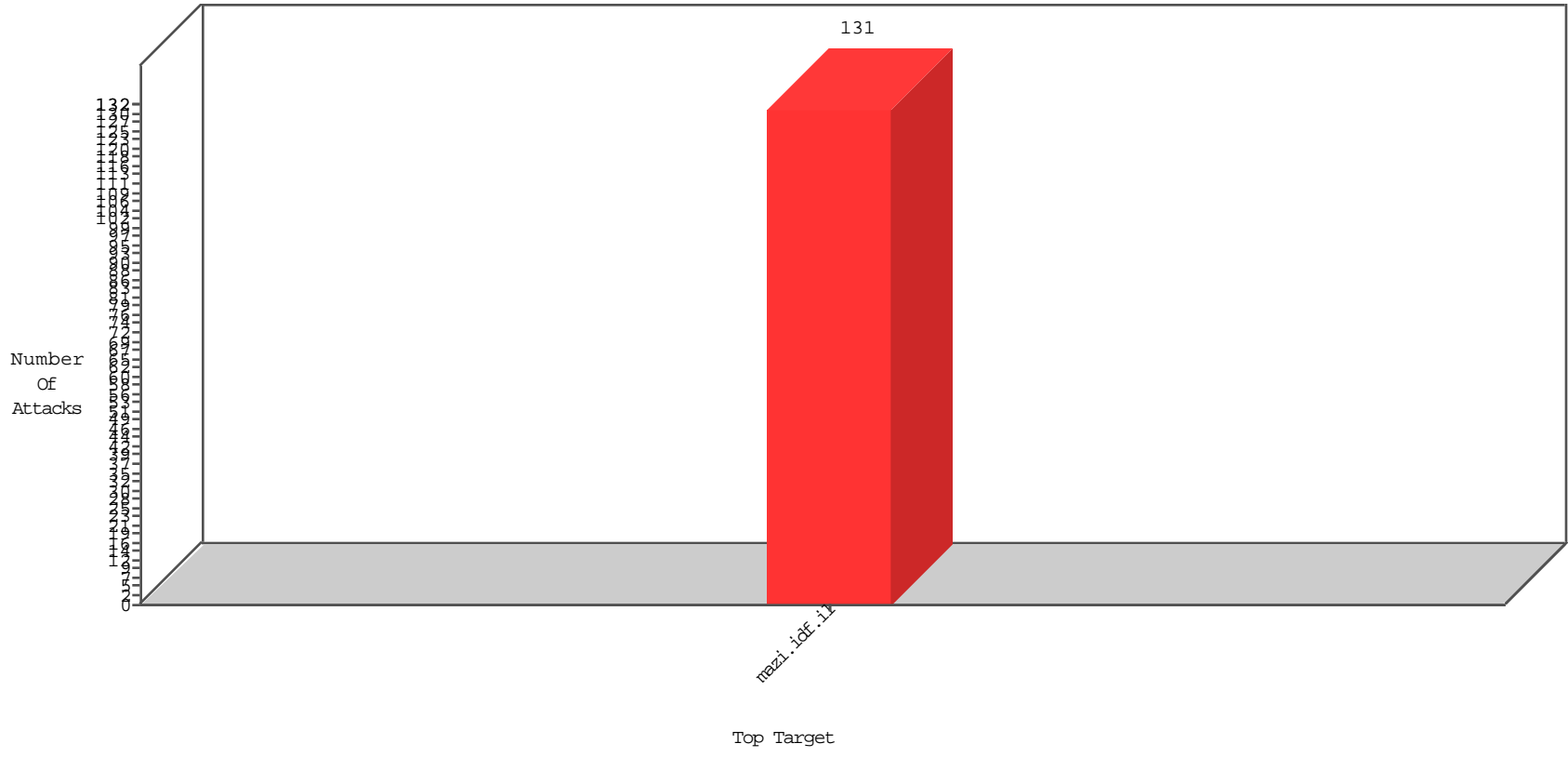


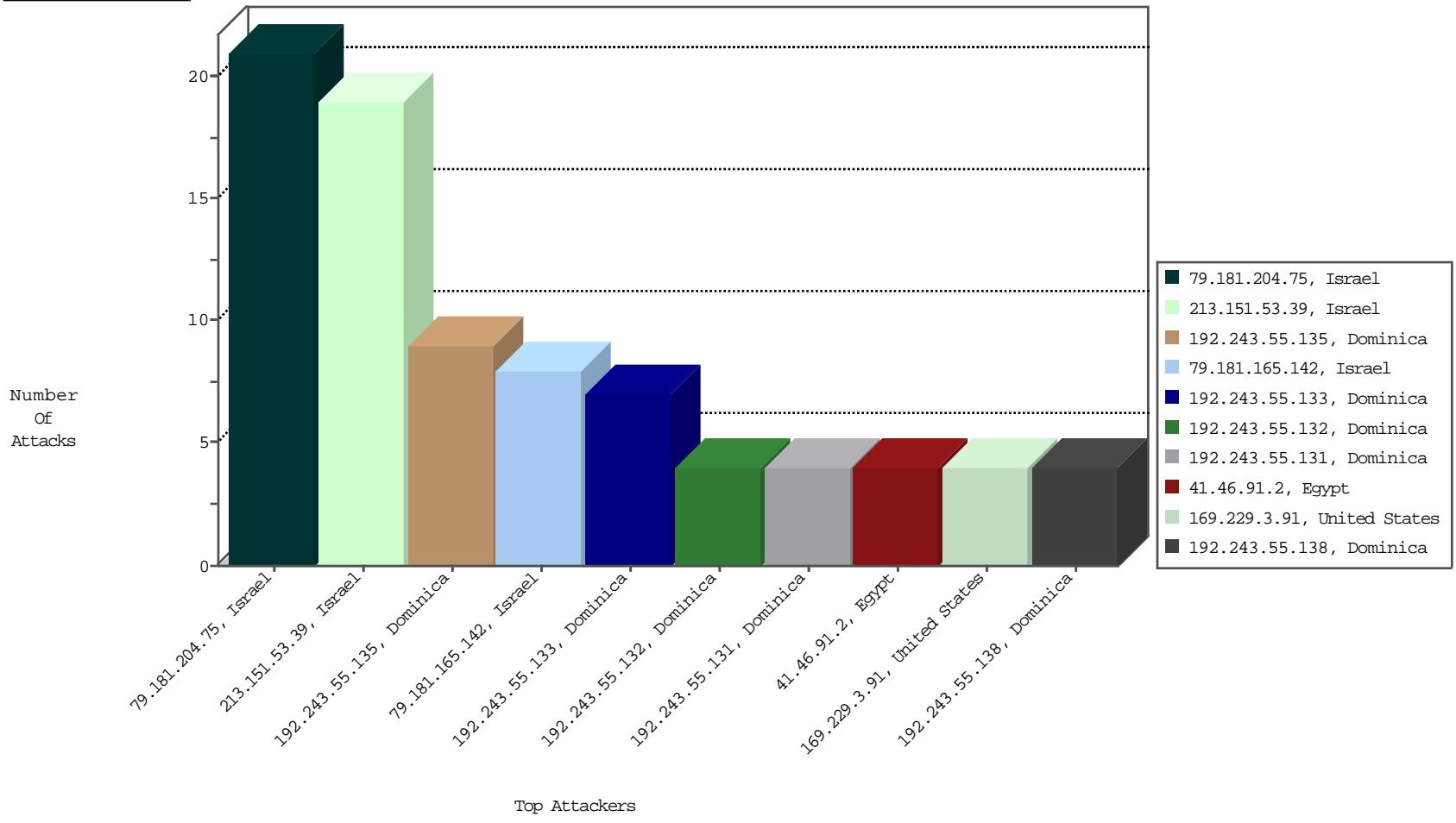
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



02-06-2016 to 02-07-2016

Top Attackers In DDoS-Defence

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

02-06-2016 to 02-07-2016

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	2
151.80.31.147	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
216.201.148.210	United States	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
209.126.116.147	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	2
54.68.171.13	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
54.68.171.13	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.98	United States	147.237.77.17	mazi.idf.il	ET DROP Dshield Block Listed Source	1
218.246.0.97	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
54.68.171.13	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	China	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
46.19.85.59	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
37.26.149.152	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
138.134.102.15	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.179.217.137	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
94.159.147.75	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
46.19.85.146	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.146	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
77.126.167.111	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
2.52.60.141	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.85.59	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	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
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
37.26.146.139	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.85.168	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.168	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
84.111.7.38	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
213.8.204.2	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.38.210	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.186.41.83	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.22	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
79.127.43.190	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
79.127.43.190	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
185.3.147.175	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.91	Israel	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
37.237.208.101	Iraq	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.237.208.101	Iraq	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.166	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.12.33	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
5.22.131.62	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.17.119	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.86.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.46.39.72	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.149.152	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.120.132.129	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
5.22.131.103	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
93.73.250.183	Ukraine	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.47	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.183.165.219	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.214.196.25	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
14.201.25.158	Australia	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.216	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.232	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.176.32	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.30	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.212.163	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
79.176.111.94	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

