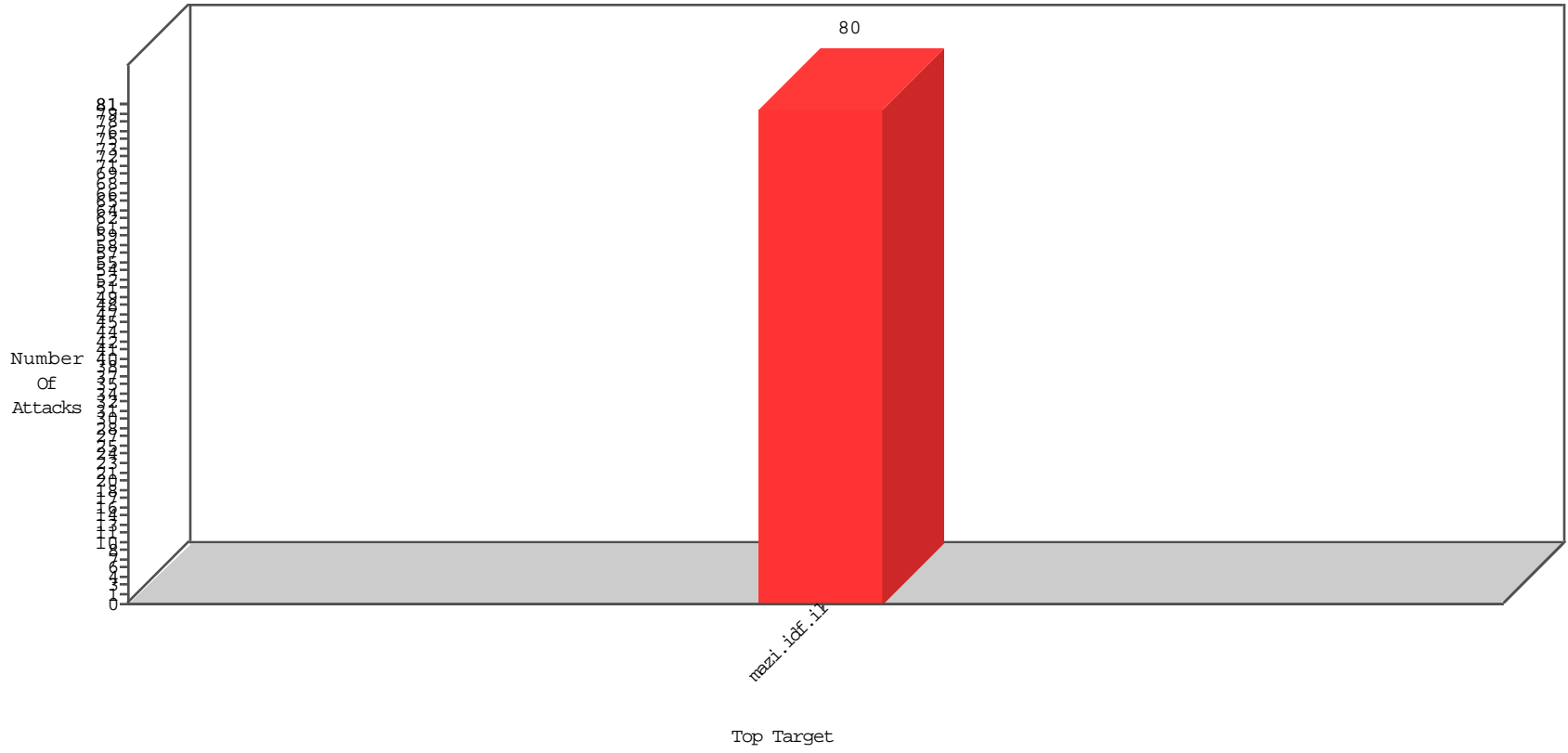


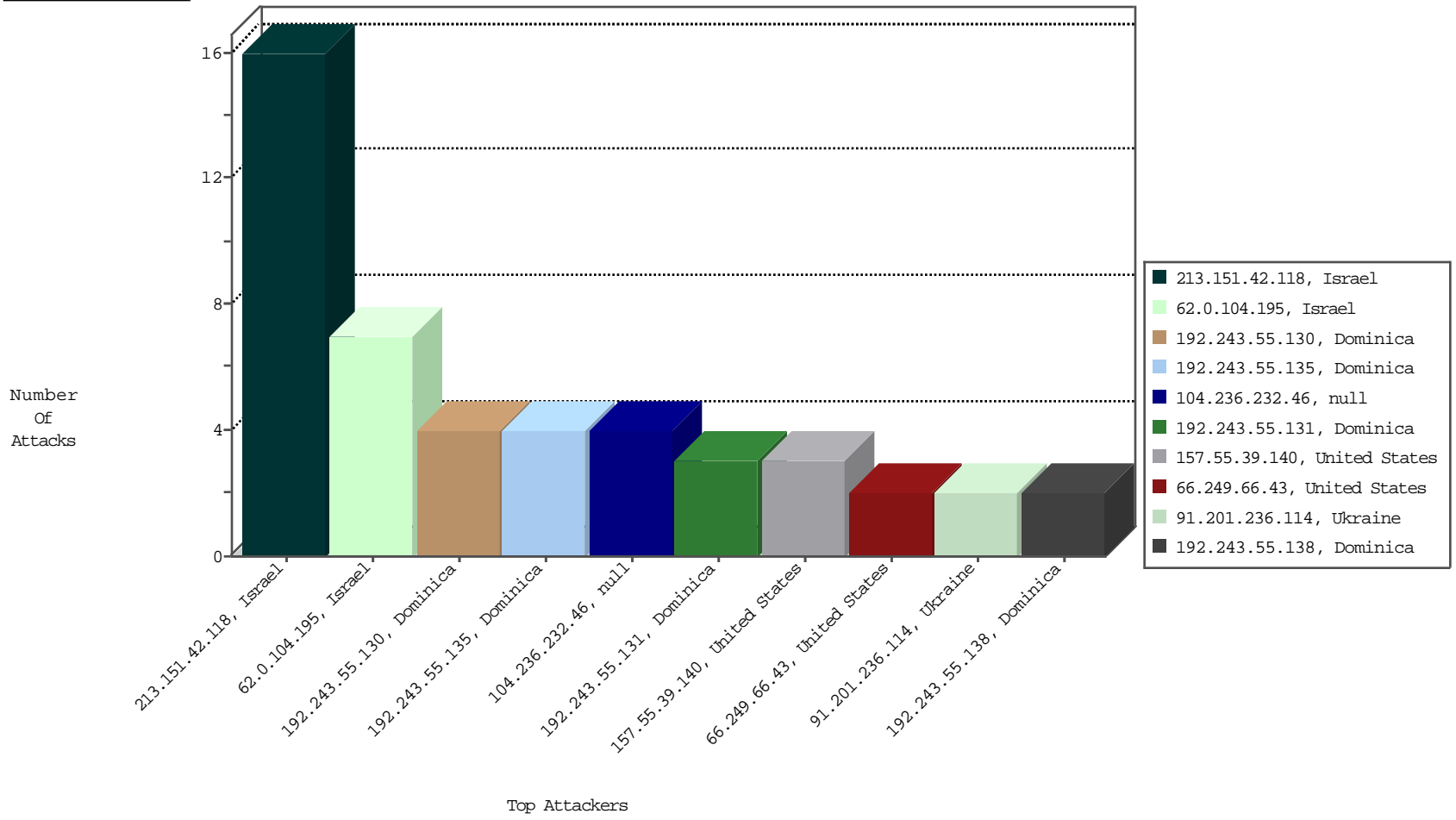
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
62.0.104.195	Israel	147.237.77.17	mazi.idf.il	L4 Source or Dest Port Zero	drop	BEL-Israel	7
128.68.47.144	Russian Federation	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	1
202.112.51.96	China	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BEL-Frankfurt	1

01-10-2016 to 01-11-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.66.43	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	2
91.201.236.114	Ukraine	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
199.191.56.187	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 3072	1
91.201.236.114	Ukraine	147.237.77.17	mazi.idf.i	ET DROP Spamhaus DROP Listed Traffic Inbound	1
146.185.250.2	Russian Federation	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
210.79.69.181	China	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.78.34.240	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
2.52.35.87	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.85	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
176.228.34.229	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.222	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.3.88	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.86.166	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.52.43.197	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
37.26.149.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
62.0.104.195	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.85.133	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.206	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.222	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.99	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.117.180.120	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	3
2.54.37.70	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
185.3.144.84	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.198	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
2.54.39.104	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.189.87	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
157.55.39.140	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.132	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.145.103	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
207.46.13.18	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.14.250	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
157.55.39.160	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
212.76.127.4	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
94.230.86.172	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
194.90.119.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
5.22.130.123	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
71.183.108.102	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.248	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.240.73	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.255.6.220	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.191.182	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.210.89	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
80.246.133.69	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.155.218	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

