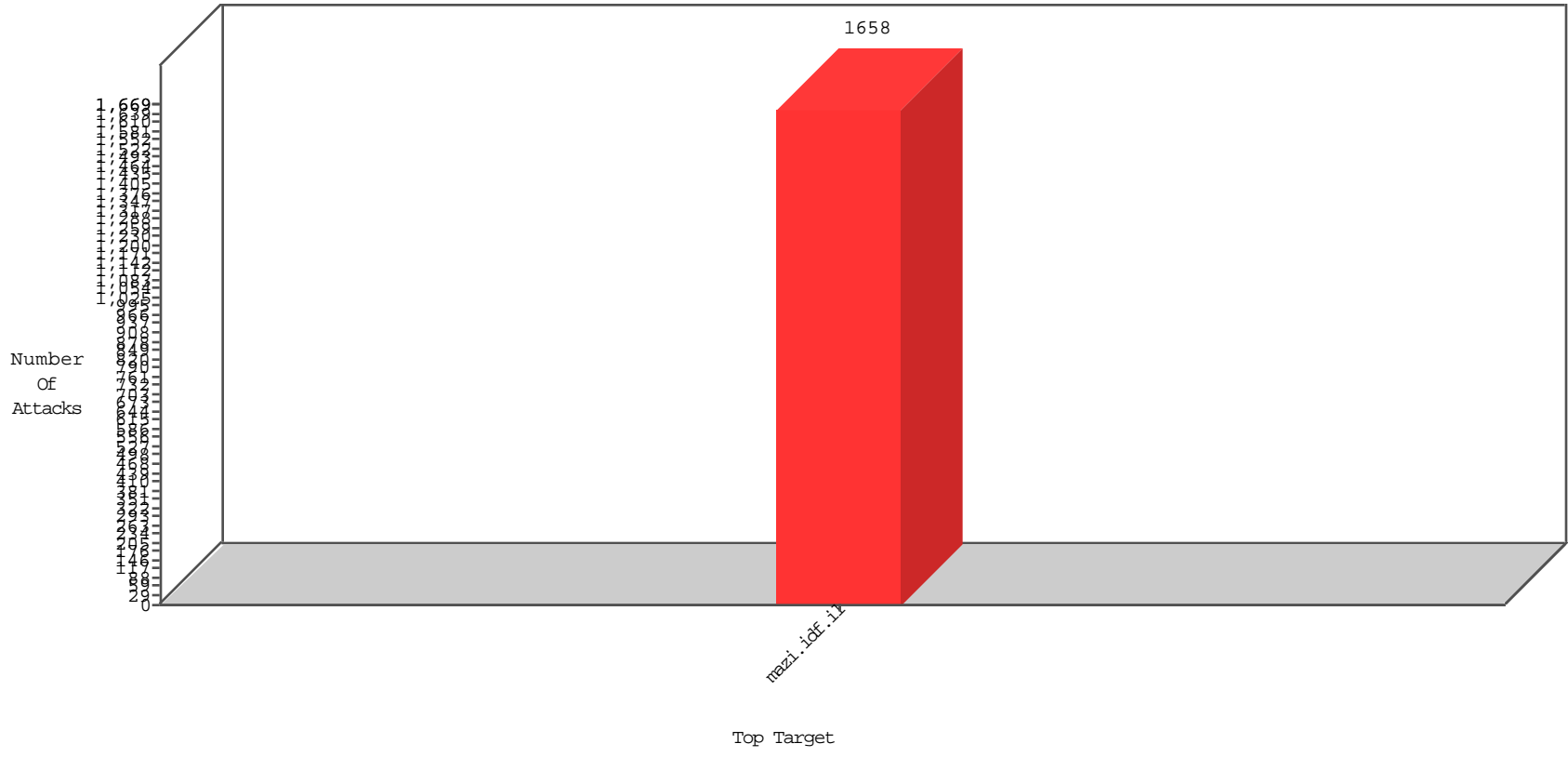


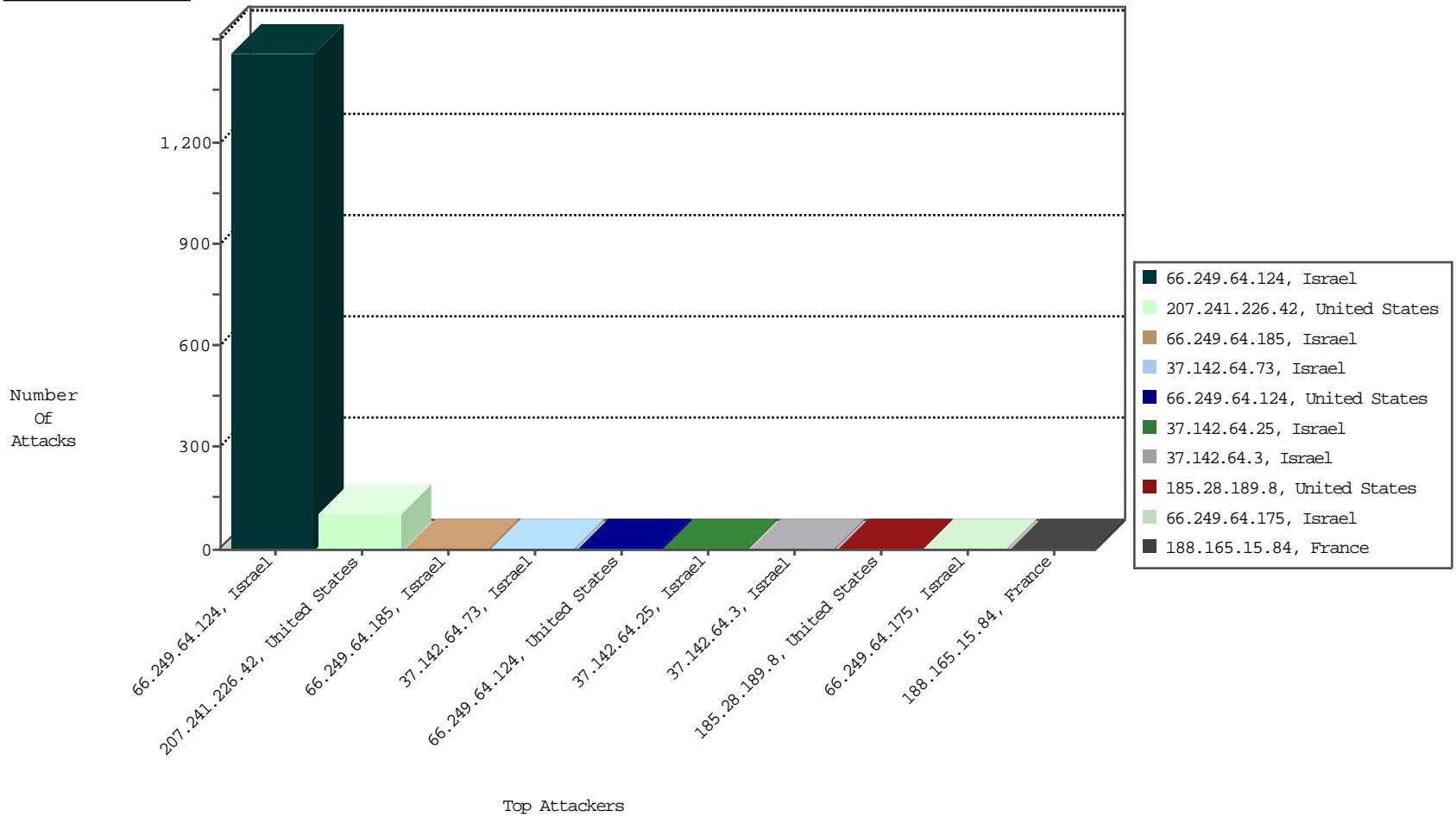
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



11-25-2015 to 11-26-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.64.124	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1464

11-25-2015 to 11-26-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
188.165.15.84	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	3
185.28.189.8	United States	147.237.77.17	mazi.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.64.124	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	4
66.249.64.8	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	2
42.48.224.74	China	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.74.226.90	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
45.63.16.132		147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
193.105.134.220	Sweden	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
208.115.111.75	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	34
81.218.148.177	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	27
46.19.85.80	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.85.164	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.164	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
5.102.254.125	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.6	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.222	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.179.50.221	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.93	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.178.99.208	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
207.241.226.42	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	5
46.19.85.16	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.93	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.96	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.127.161	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.108.45.97	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.147.249	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.133.52	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.130.74	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
94.230.86.181	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.16	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.54.32.118	Israel	147.237.77.17	mazi.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.86.0	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.182	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.111.182.9	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.45.132	Israel	147.237.77.17	mazi.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
5.102.254.135	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.8	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.0.103	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.100	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.154.233.47	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.64.124	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.138.1.218	Germany	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.206	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
46.19.85.200	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
85.130.201.77	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.254.77	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.85.241	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.146.131	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.120	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.163	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.142.172.29	Slovenia	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.110	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.154.233.47	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
79.176.225.22	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.138.17.205	France	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

11-25-2015 to 11-26-2015

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
8.37.70.96	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5078-6077-he/igf.aspx&usg=alkjrhhx8tok6v_keydkq3hpacwgzihskg	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1

11-25-2015 to 11-26-2015