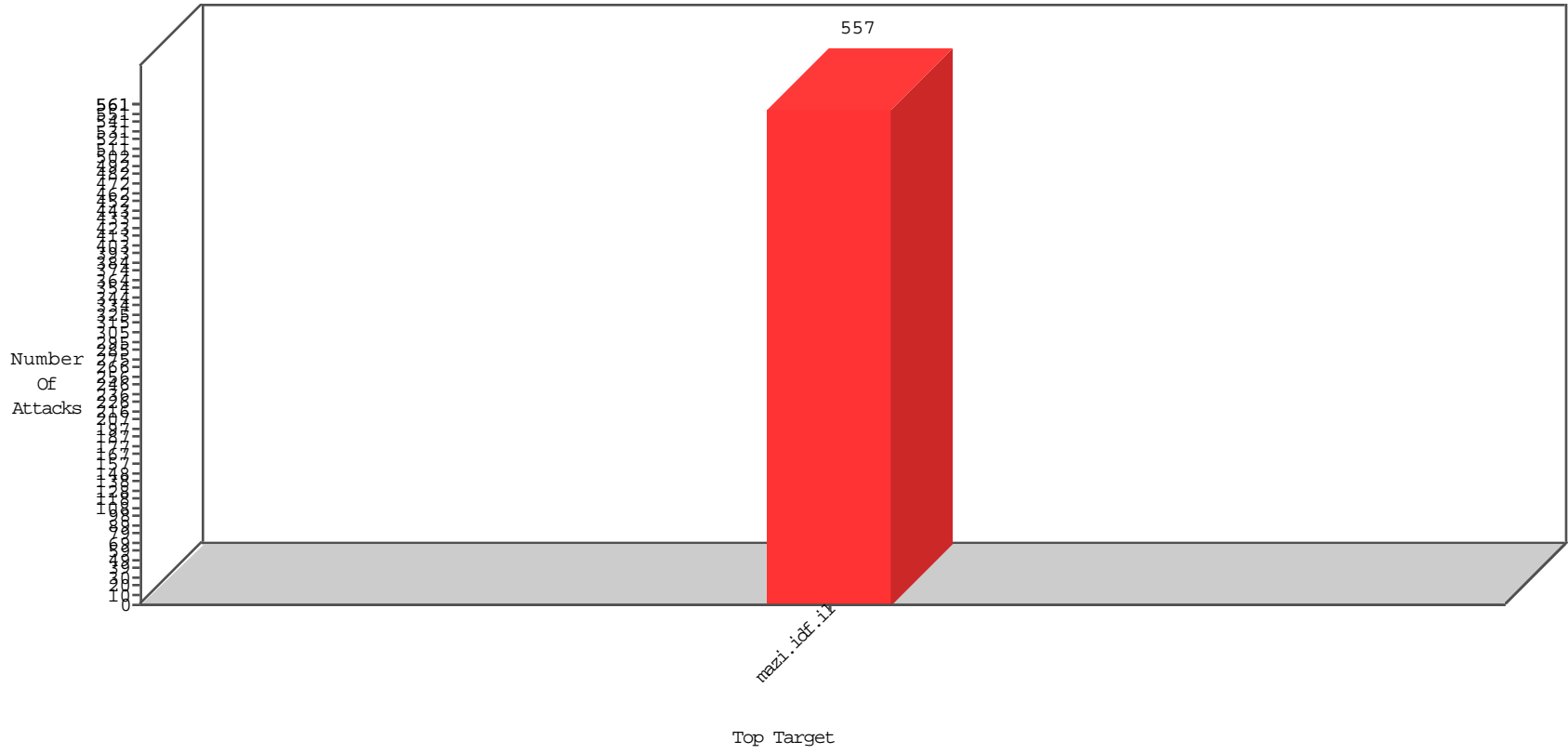


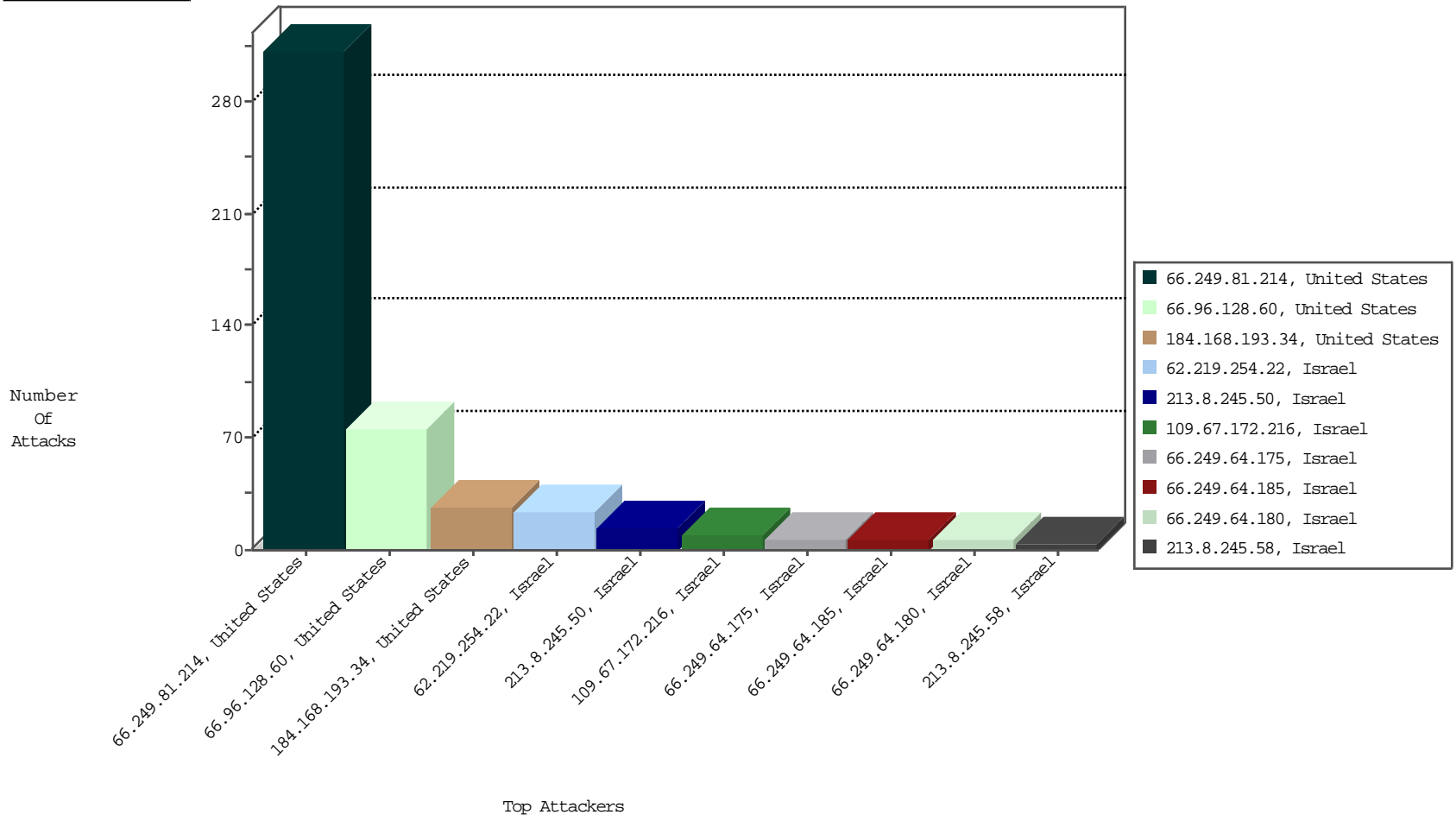
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.81.214	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	312
62.219.254.22	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	24

11-24-2015 to 11-25-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
66.96.128.60	United States	147.237.77.17	mazi.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	18
66.96.128.60	United States	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
188.165.15.84	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	3
220.156.184.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
91.142.253.133	Netherlands	147.237.77.17	mazi.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.96.128.60	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	40
184.168.193.34	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	26
66.249.64.8	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.124	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
91.142.253.133	Netherlands	147.237.77.17	mazi.idf.il	SQL Injection - Select From	2
46.228.207.18	Germany	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
90.2.140.139	France	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
93.113.125.11	Romania	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
208.80.155.223	United States	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	1
112.33.8.16	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
185.92.72.23		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
188.165.15.66	France	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	56
109.66.196.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
77.125.126.119	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
184.168.193.34	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	17
46.19.85.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.73	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
93.113.125.11	Romania	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
46.116.240.156	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.57.134.190	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.72	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.117.101.252	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.134.190	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.47	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.159.61	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.247	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.73	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.175	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.39.230	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
71.126.144.58	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.186.15.181	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.182.162.204	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
208.54.4.130	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.138.17.205	France	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.102.254.242	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.196	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.199.63.46	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.167	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
31.168.71.249	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.10.160	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.86.169	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.81.80	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.196	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
74.82.47.26	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.108	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.156.105	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.117.85.241	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.167	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
112.74.67.109	China	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.113.125.11	Romania	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.134	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
80.246.130.134	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.81.219	Israel	147.237.77.17	mazi.idf.i	Directory Traversal	directory traversal overflow	monitor	1
176.12.142.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.171.12	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.100	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.134	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

