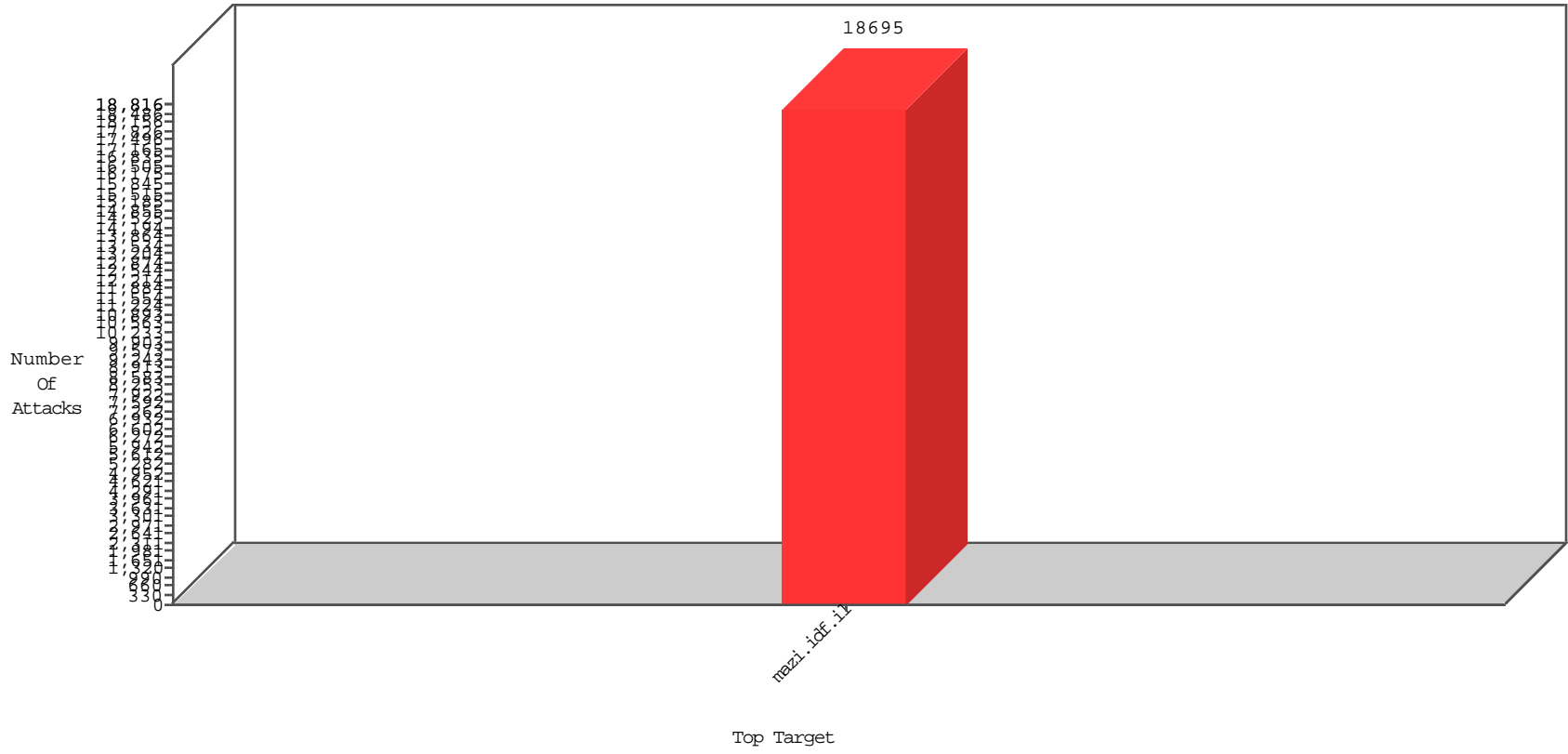


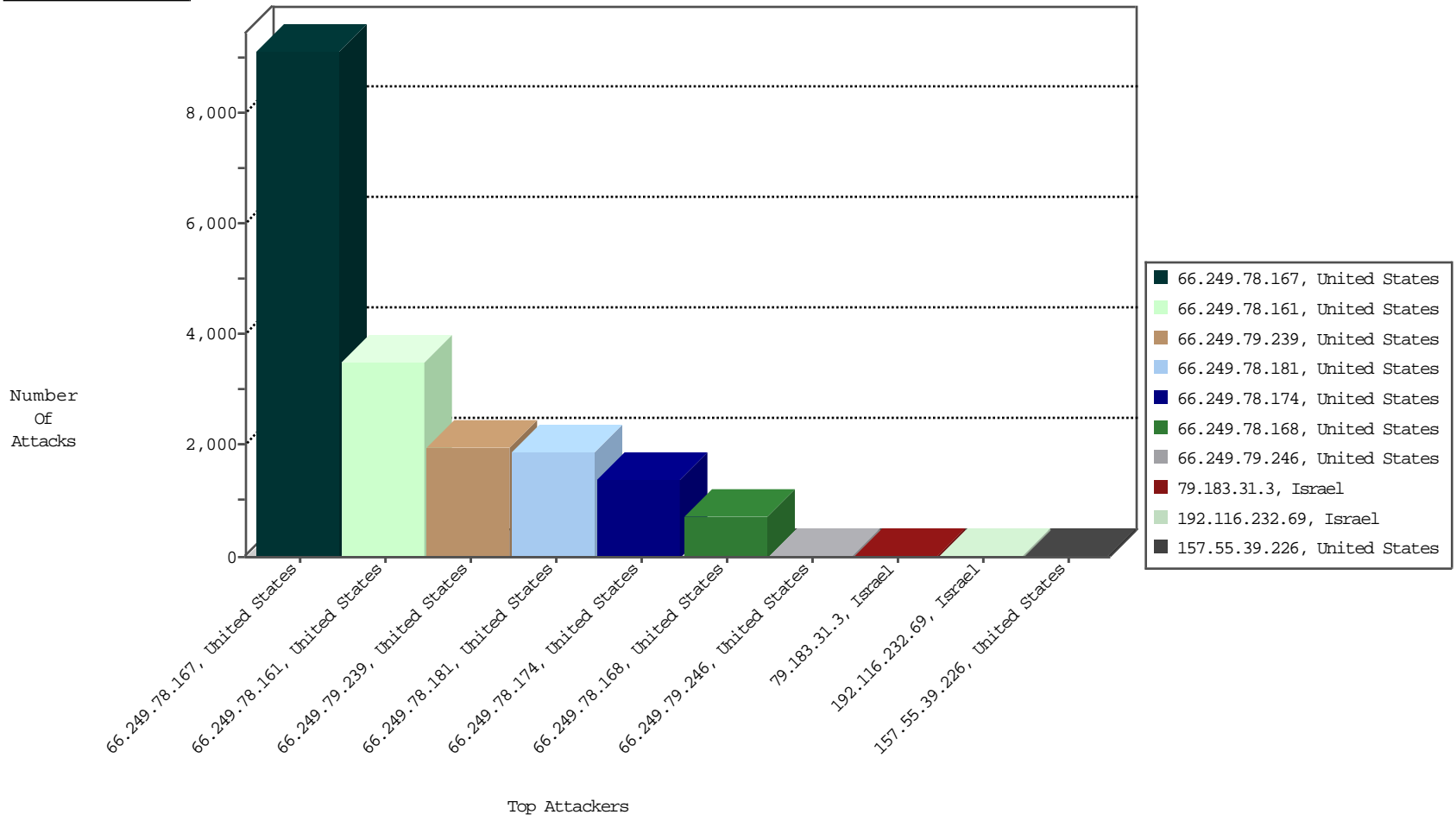
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.78.167	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	9132
66.249.78.161	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	3497
66.249.79.239	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	1989
66.249.78.181	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	1887
66.249.78.174	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	1394
66.249.78.168	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	707
66.249.79.246	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	32
79.183.31.3	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	13

11-18-2015 to 11-19-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
151.80.31.117	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.238	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.78.181	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	4
74.117.209.136	United States	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
54.223.62.240	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
74.117.209.135	United States	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.86.215	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1676
80.215.200.36	France	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1326
199.203.35.178	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	785
80.215.200.36	France	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	571
80.215.200.36	France	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	538
46.19.86.155	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	178
94.228.34.249	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	129
54.244.22.103	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	100
176.13.1.17	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	81
79.182.51.237	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
176.12.149.184	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
91.231.192.149	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
46.116.77.69	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
46.19.85.110	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
46.116.77.69	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	50
80.246.133.7	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
54.244.22.103	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	49
94.228.34.249	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	42
68.180.228.160	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
46.19.85.153	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
79.176.5.137	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
37.26.149.156	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
176.13.2.91	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.153	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
203.133.170.214	Korea, Republic of	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
138.134.102.16	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
46.19.85.118	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
82.166.146.155	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
176.13.2.91	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.87	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
82.166.146.155	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	25
176.13.1.17	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
194.90.25.122	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
208.115.111.75	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	23
157.55.39.226	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
176.13.19.3	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
203.133.170.214	Korea, Republic of	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
85.250.38.39	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
80.246.130.117	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
176.13.5.132	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
188.120.148.221	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
157.55.39.9	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
66.249.78.174	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
81.141.215.146	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
81.141.215.146	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
66.249.93.140	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
81.218.173.126	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
79.181.210.86	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
212.179.242.80	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
138.134.102.15	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.116.232.69	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.116.232.69	Block	7
5.28.130.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/	Block	2
141.212.121.192	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
79.180.150.1	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
195.154.146.225	France	147.237.77.17	mazi.idf.i	Multiple Illegal HTTP Version from 195.154.146.225	Block	1
157.55.39.226	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/5580-7562-he/igf.asp	Block	1
93.173.24.141	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
66.249.79.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5039-he/igf.aspx	Block	1
141.212.122.96	United States	147.237.77.17	mazi.idf.i	Multiple Malformed URL from 141.212.122.96	Block	1
85.64.1.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
40.77.167.39	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4983-he	Block	1
176.228.128.105	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
95.86.73.240	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7322-11795-he/mazi.aspx&sa=u&ved=0cbiqfjadahukewjjsaqs6jrjahwhaxqk hqr2dni&usg=afqjcngb9i08tw3fbb4lqxjmi_tdvhcb7w	Block	1
66.249.79.238	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
194.153.113.13	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
157.55.39.226	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 157.55.39.226	Block	1
85.64.32.148	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ufi/reaction/	Block	1
46.19.85.62	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
185.25.151.159	Poland	147.237.77.17	mazi.idf.i	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
107.150.55.51	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /	Block	1
68.180.229.218	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
195.154.146.225	France	147.237.77.17	mazi.idf.i	Illegal HTTP Version HTTP/	Block	1
157.55.39.226	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3697-9630-he/igf.aspx 10 Ã-âe~Ã-Ã Ã-âe çÃ-âe~Ã-Ã¼Ã-âe~Ã-Ã" 2010	Block	1
87.69.238.243	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/xœxœx? x'x'x•xœx• xª.aspx	Block	1
66.249.67.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4070-11595-he/xžx-xœxšxª xªx>x x•xŸ x•x'xšx"x".aspx	Block	1
188.120.148.222	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1