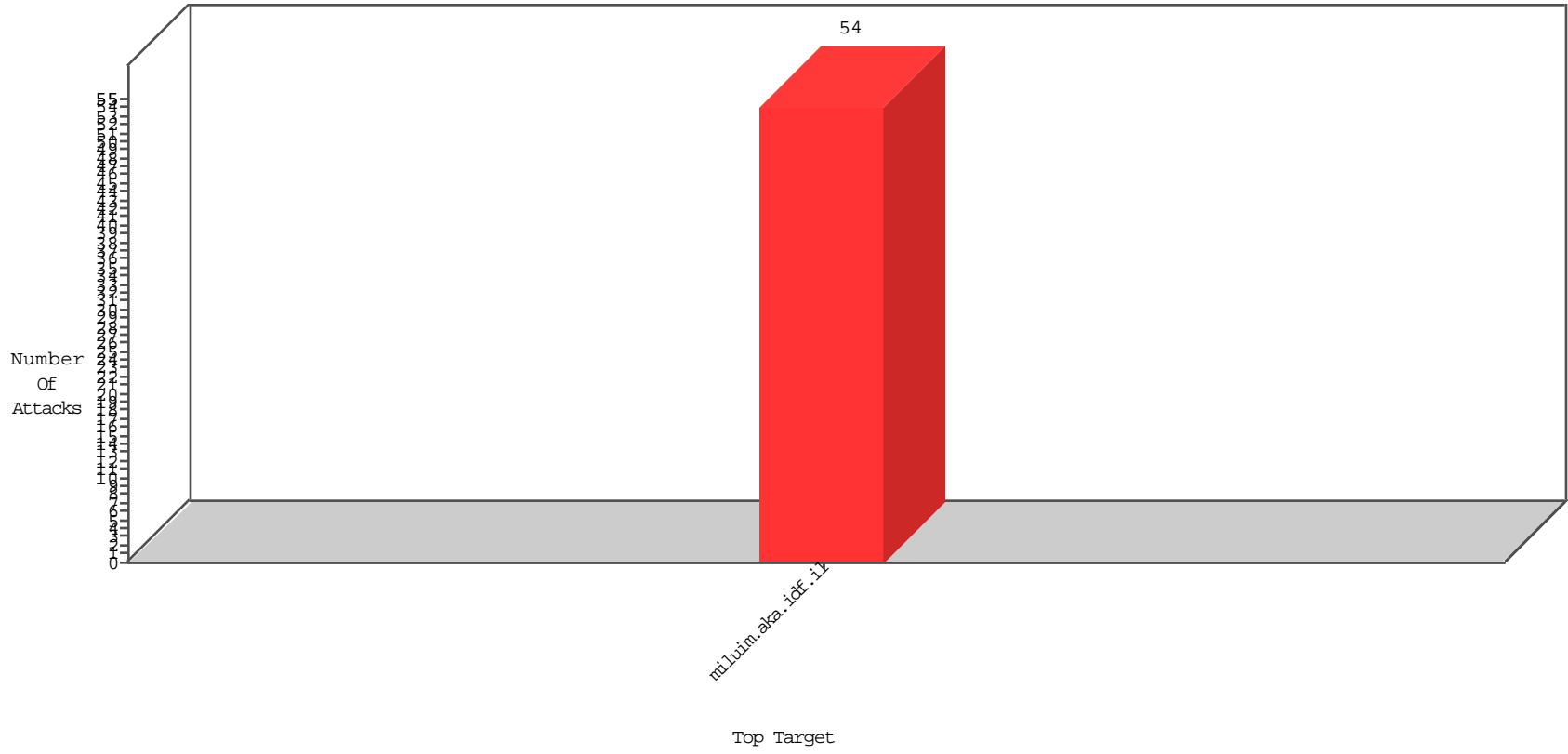


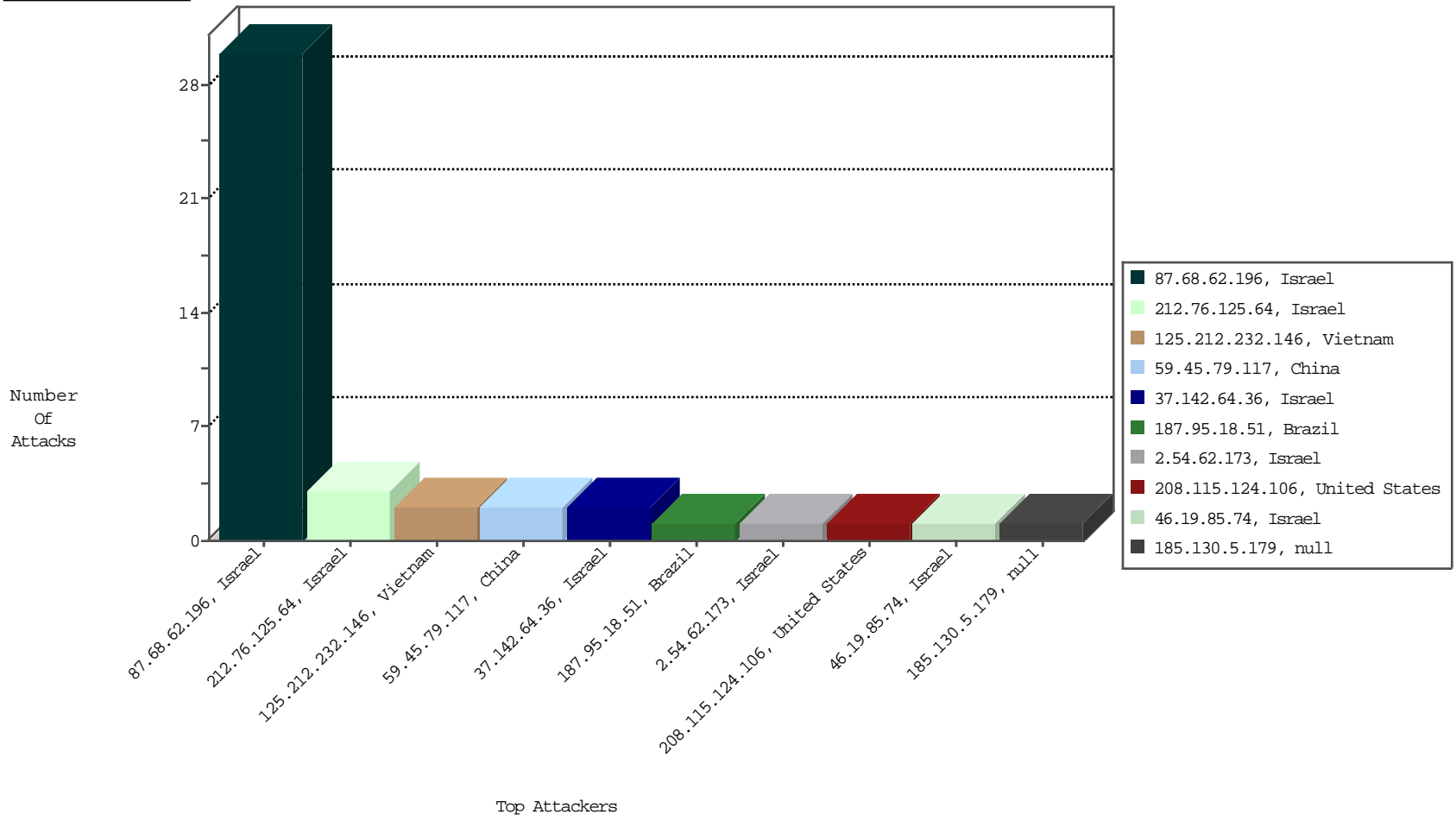
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



02-12-2016 to 02-13-2016

Top Attackers In DDoS-Defence

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

02-12-2016 to 02-13-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
188.165.15.64	France	147.237.0.120	miluim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.27	France	147.237.0.120	miluim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.45.79.117	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	2
74.122.192.101	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.146	Vietnam	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
187.95.18.51	Brazil	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
208.115.124.106	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.146	Vietnam	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.179		147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
195.88.209.6	Russian Federation	147.237.0.120	miluim.aka.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
79.178.152.38	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4823
79.176.128.44	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
109.65.25.52	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2025
2.54.181.0	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	612
2.54.174.92	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
149.78.43.80	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
109.67.41.186	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.179.206.138	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
109.64.117.68	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
46.19.86.2	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	193
185.120.125.57		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.181.118.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.228.111.120	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.65.185.186	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.179.55.114	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.182.142.9	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.228.202.188	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
46.19.85.92	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	65
80.74.107.118	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.86.2	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	37
5.22.131.71	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	36
5.22.131.71	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
149.78.146.229	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.18	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
79.182.59.44	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.30	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
37.46.38.23	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
37.142.64.29	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.182.160.49	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.18	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
149.78.192.193	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
149.78.192.193	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
84.228.130.149	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
93.172.157.99	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
77.125.151.17	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
40.77.167.68	United States	147.237.0.120	miluim.aka.idf.i	drop	SAM rule	drop	12
79.180.14.158	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.30.41	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.30	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
79.183.15.216	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
73.202.246.27	United States	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.109.241.169	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.120.181.192	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.110.108.205	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.44	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.23.192	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
203.124.120.217	Singapore	147.237.0.120	miluim.aka.idf.i	drop	SAM rule	drop	5
46.117.16.175	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.74	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4

02-12-2016 to 02-13-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 87.68.62.196	Block	16
212.76.125.64	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.76.125.64	Block	2
37.46.38.23	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 37.46.38.23	Block	1
212.76.125.64	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1230-he/miluim.aspx&sa=u&ved=0ahukewiq0n65zvhkaxjdpokhvznbgaqfgglmae&usg=afqjcnf7xdcssyxsrnrve8ujuglmfqysg	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cellularTyp in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cell in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
46.19.85.74	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1436-he/miluim.aspx&?â€Ž	Block	1
141.212.122.177	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cellular in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter c in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
37.142.64.36	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter v in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cellu in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
66.249.78.191	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/sitemap/sitemap.aspx	Block	1
149.88.178.145	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cellularT in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter ce in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
37.142.64.36	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter vi in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cellul in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
80.246.133.33	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1435	Block	1
2.54.62.173	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1316-he/miluim.aspx&?â€Ž	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cellularTy in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cel in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
37.142.207.148	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/homepage.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter vir in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
87.68.62.196	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter cellula in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1

02-12-2016 to 02-13-2016