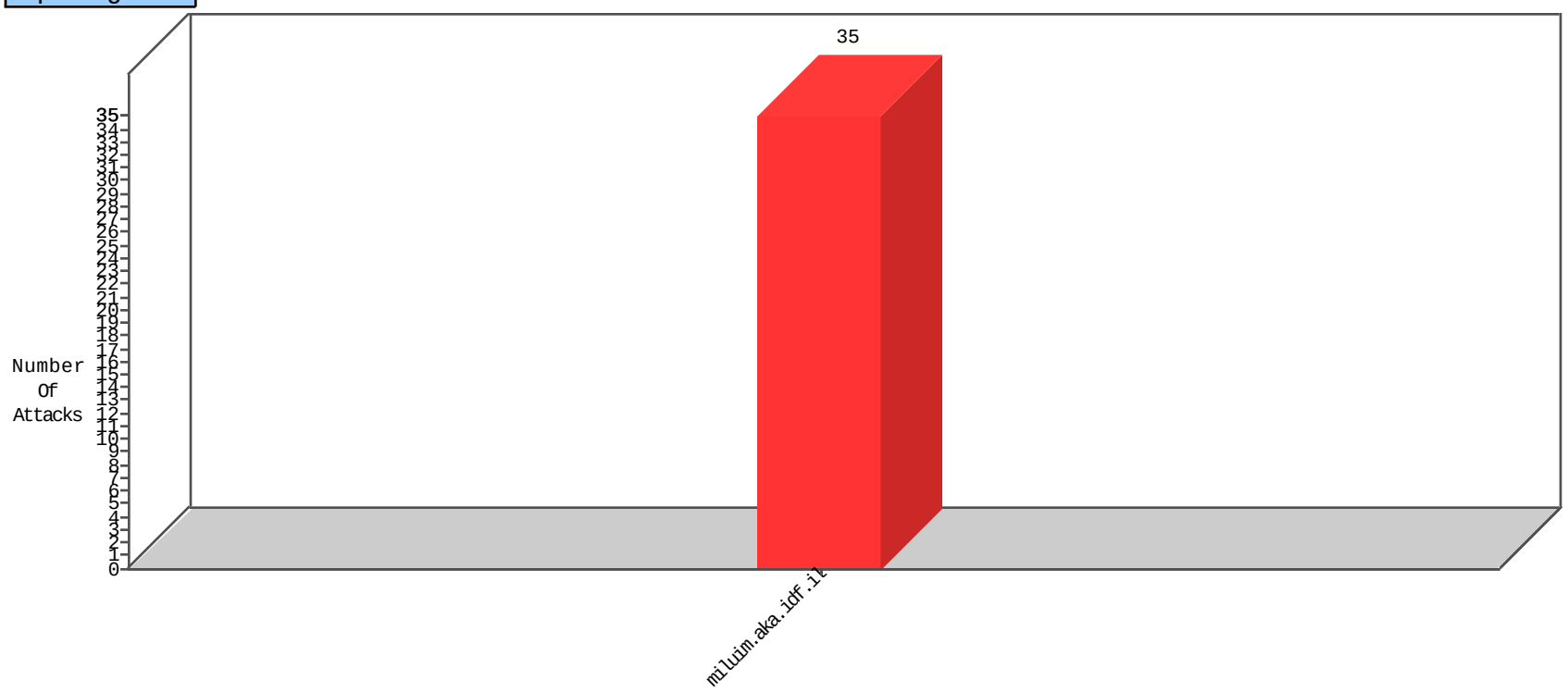
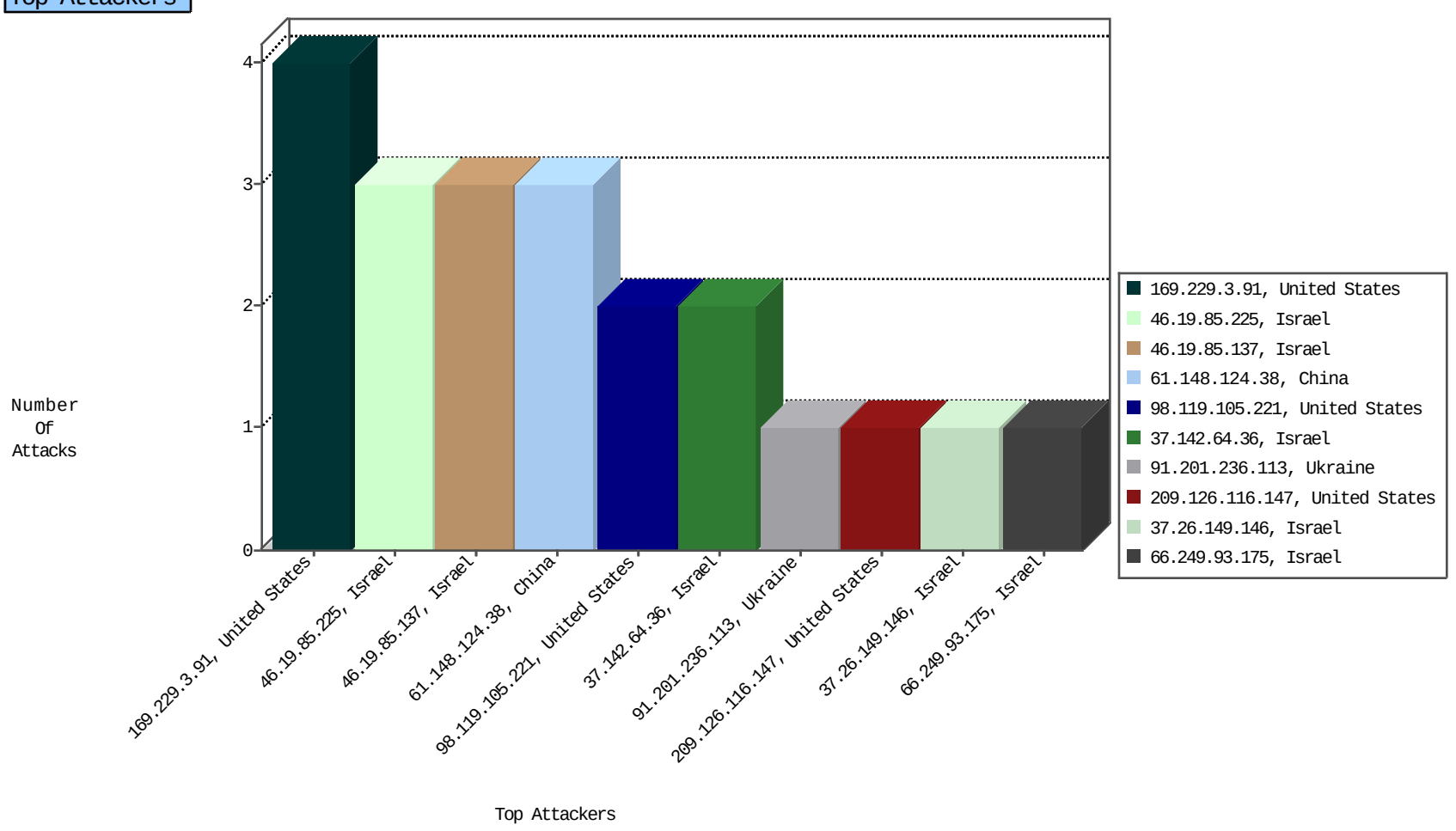
02-05-2016 to 02-06-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-05-2016 to 02-06-2016

Top Attackers In DDoS-Defence

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

02-05-2016 to 02-06-2016

Top Attackers In IPS

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

02-05-2016 to 02-06-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
61.148.124.38	China	147.237.0.120	miluim.aka.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
91.201.236.113	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
193.105.134.220	Sweden	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.148.124.38	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Tomcat Web Application Manager scanning	1
61.240.144.64	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
188.126.77.138	Sweden	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

02-05-2016 to 02-06-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
5.28.166.7	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4616
2.54.140.144	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.179.164.251	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2025
87.68.153.107	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	720
79.179.28.185	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	468
84.228.202.188	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
87.68.23.97	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
77.125.79.219	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
2.54.254.131	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
2.54.151.235	Israel	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
149.88.31.179	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
37.26.147.252	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	106
79.180.165.100	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	81
93.172.135.101	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
46.19.85.240	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
46.19.85.145	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	52
46.19.85.240	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	49
185.120.126.40		147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.85.240	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	49
109.66.51.68	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
2.52.16.202	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.85.226	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.156	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
212.179.150.17	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack		reject	36
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	36
46.19.85.226	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	34
212.179.150.17	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	34
79.179.233.219	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
84.111.24.80	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
213.8.204.48	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.85.205	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
77.126.61.99	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.86.170	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
212.179.150.17	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	25
46.19.85.156	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
119.188.4.3	China	147.237.0.120	miluim.aka.idf.i	drop	SAM rule	drop	20
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	18
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.122	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
2.54.13.95	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.250.105.81	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.85.122	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	17
46.19.85.152	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.86.32	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
77.125.158.33	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16

02-05-2016 to 02-06-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.19.85.225	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1431-he/miluim.aspxâ€?â€Ž	Block	3
79.179.193.24	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1431-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.137	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method xajzzxvvvrbe3nue in URL	Block	1
157.55.39.96	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.198	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/news/news.in.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
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method [[#2]]Ã¢ÃªÃ-Ã-`[[#28]]iiÂ¤ÃªÃ«Ã½[[#29]][[#21]][[#18]]Ã—_&Â¨[[#20]]ÂŽ [[#12]]oÂ?\Ã²Ã¦Ã®7T#Ã„Ã•Ã›[[#5]]ÂŸÂ©{wpÃ™G6Yy[[#1]]Â¥Ã— in URL	Block	1
80.246.133.49	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1431-he/miluim.aspxâ€?â€Ž	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request request version	Block	1
66.249.81.230	Israel	147.237.0.120	miluim.aka.idf.i	Distributed URL is Above Root Directory	Block	1
46.19.85.137	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
176.13.8.143	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1431-	Block	1
81.218.241.25	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/	Block	1
54.251.144.191	Singapore	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /	Block	1
37.26.149.146	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1431-he/miluim.aspxâ€?â€Ž	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method [[#2]]Ã¢ÃªÃ-Ã-`[[#28]]iiÂ¤ÃªÃ«Ã½[[#29]][[#21]][[#18]]Ã—_&Â¨[[#20]]ÂŽ [[#12]]oÂ?\Ã²Ã¦Ã®7T#Ã„Ã•Ã›[[#5]]ÂŸÂ©{wpÃ™G6Yy[[#1]]Â¥Ã—	Block	1
66.249.93.175	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
46.19.85.137	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL	Block	1
185.25.151.159	Poland	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
87.68.62.104	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1431-he/miluim.aspxâ€?â€Ž	Block	1
61.148.124.38	China	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/manager/html	Block	1
37.142.64.36	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Malformed URL "	Block	1

02-05-2016 to 02-06-2016