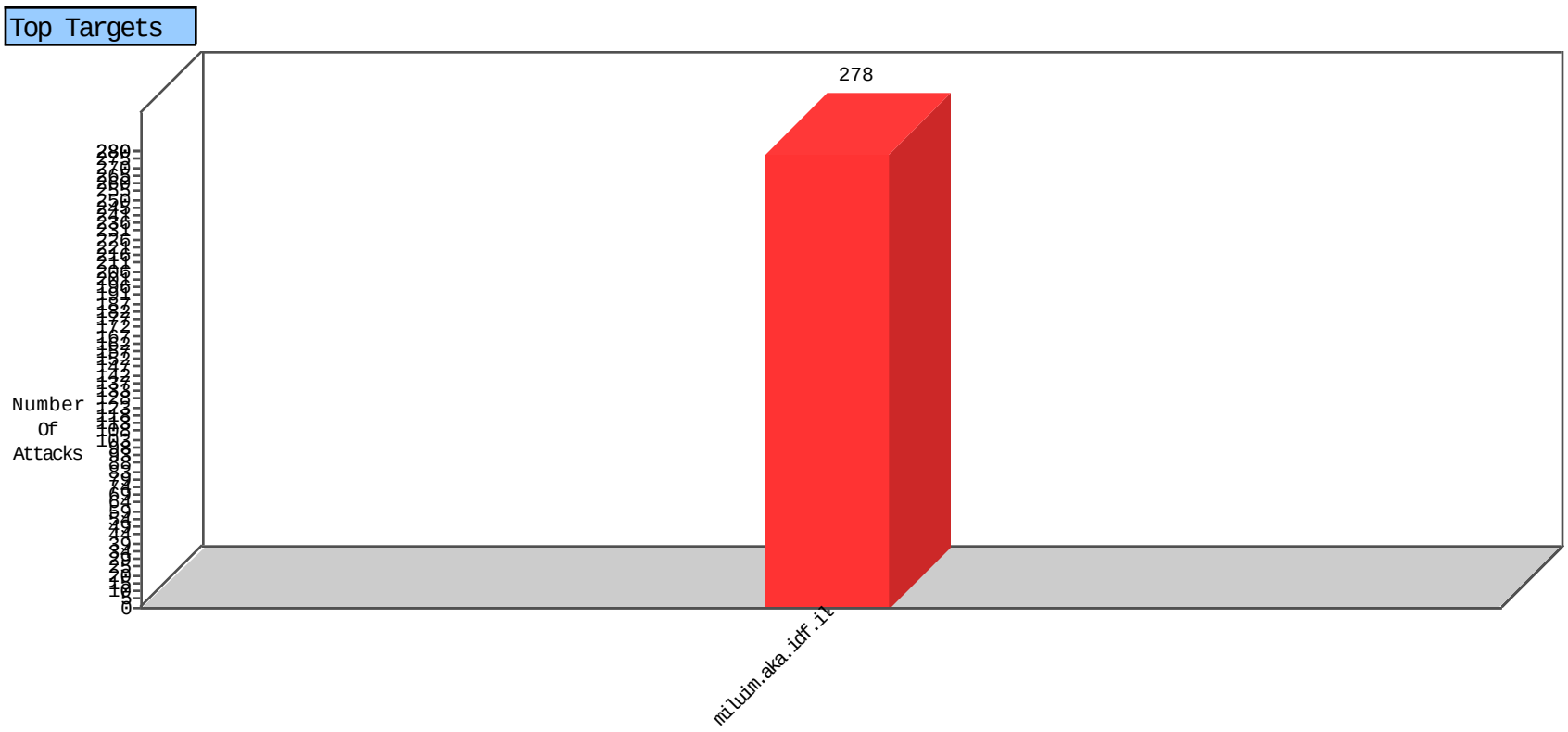
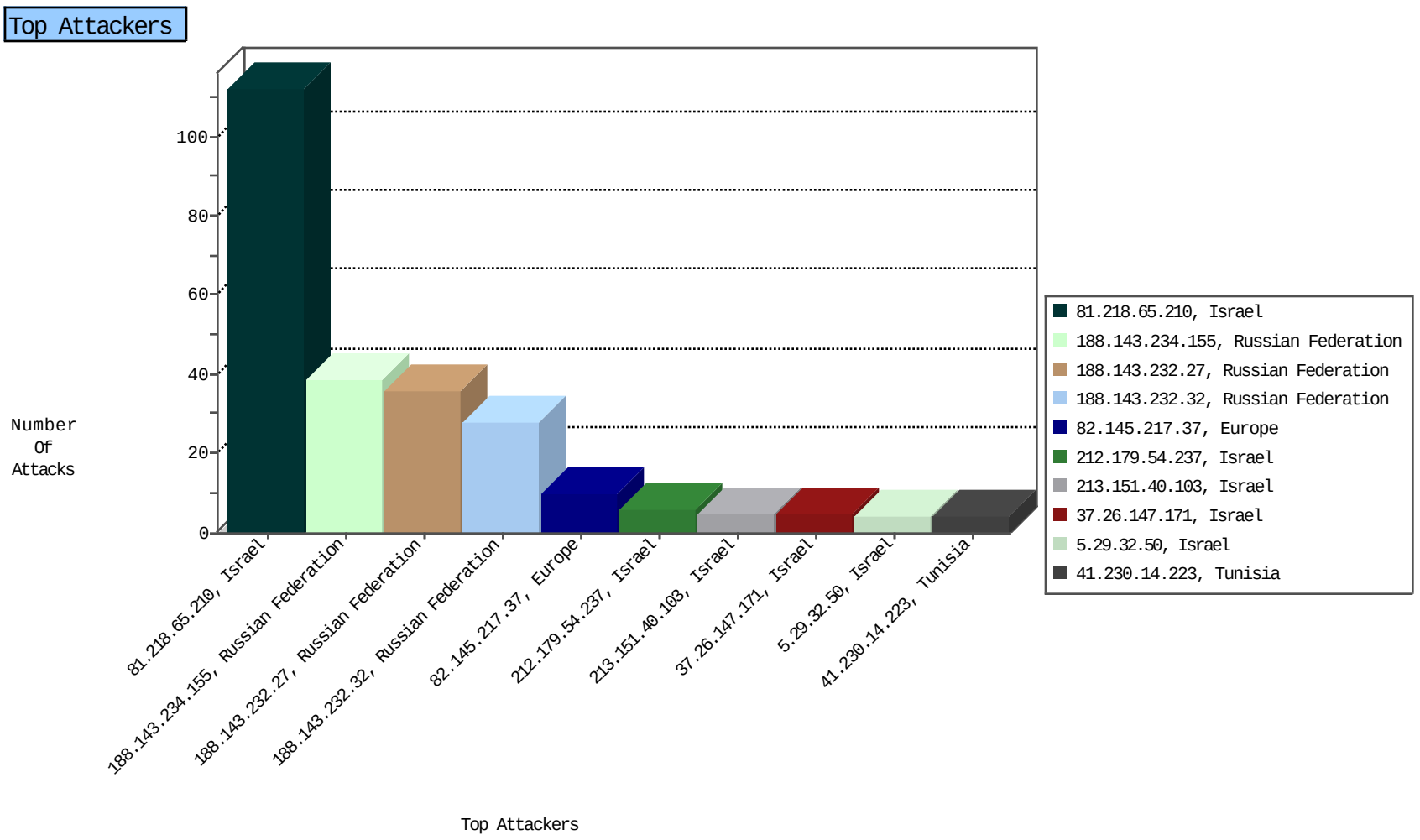
03-05-2016 to 03-06-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



03-05-2016 to 03-06-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
81.218.65.210	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	112
82.145.217.37	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	10
212.179.54.237	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	6
81.218.206.82	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
134.147.203.115	Germany	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	2

03-05-2016 to 03-06-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

03-05-2016 to 03-06-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
203.197.205.118	India	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
23.96.109.87	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.87.205.254	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.101.186.244	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
203.197.205.118	India	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.129.55.113	France	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
23.96.109.87	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
111.118.160.177	Australia	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.244	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1

03-05-2016 to 03-06-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
79.179.138.186	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8796
79.179.197.127	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2313
109.65.171.125	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.182.209.240	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1044
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	864
79.178.57.167	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	504
79.182.108.253	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	360
46.19.85.151	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	196
79.182.180.175	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.65.152.207	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.183.129.98	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
213.57.80.82	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
2.54.39.140	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
79.183.243.182	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
5.28.135.149	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
2.54.149.185	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
2.52.33.198	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
46.19.86.127	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	49
37.142.172.170	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
37.26.149.238	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
109.64.130.227	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.182.110.238	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.179.152.144	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.182.124.131	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
198.204.249.34	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
2.52.130.217	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.85.25	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.86.244	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
37.26.148.218	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.85.26	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
79.182.102.90	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
79.179.164.162	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
212.29.224.138	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
93.172.168.85	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
109.65.179.165	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
109.66.3.81	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
79.179.131.27	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
212.199.218.50	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
109.66.3.81	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.176.207.45	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.52.37.226	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
213.57.91.199	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
185.116.116.108		147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
2.52.134.167	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
213.8.204.46	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
5.22.135.163	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
79.181.168.46	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.191.105	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.176.55.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.81.48.195	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9

03-05-2016 to 03-06-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
188.143.232.27	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter btnSendToFriend	Block	19
188.143.234.155	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/sendtofriend	Block	19
188.143.234.155	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter btnSendToFriend	Block	17
188.143.232.32	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/sendtofriend	Block	16
188.143.232.27	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/sendtofriend	Block	13
188.143.232.32	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter btnSendToFriend	Block	12
37.26.147.171	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Redundant HTTP Headers in header Referer	Block	5
213.151.40.103	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 213.151.40.103	Block	4
188.143.232.27	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	4
5.29.32.50	Israel	147.237.0.120	miluim.aka.idf.i	Redundant HTTP Headers from 5.29.32.50	Block	3
188.143.234.155	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	3
41.230.14.223	Tunisia	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 41.230.14.223	Block	3
185.116.116.108		147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 185.116.116.108	Block	2
66.249.75.204	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method	Block	1
46.19.85.114	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx'	Block	1
185.116.116.108		147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894/he/miluim.aspx	Block	1
66.249.75.204	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/general.aspx	Block	1
213.151.40.103	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjo1aagtqrlahwdajokhbk8bqmqfggimaa&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	NULL Character in Method	Block	1
66.249.64.7	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
84.109.106.57	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1432-he/miluim.aspx'	Block	1
185.112.248.32		147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
66.249.64.15	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/faq/faq.aspx	Block	1
5.29.32.50	Israel	147.237.0.120	miluim.aka.idf.i	Redundant HTTP Headers Referer	Block	1
198.204.249.34	United States	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/../shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
41.230.14.223	Tunisia	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/mobileurl	Block	1

03-05-2016 to 03-06-2016