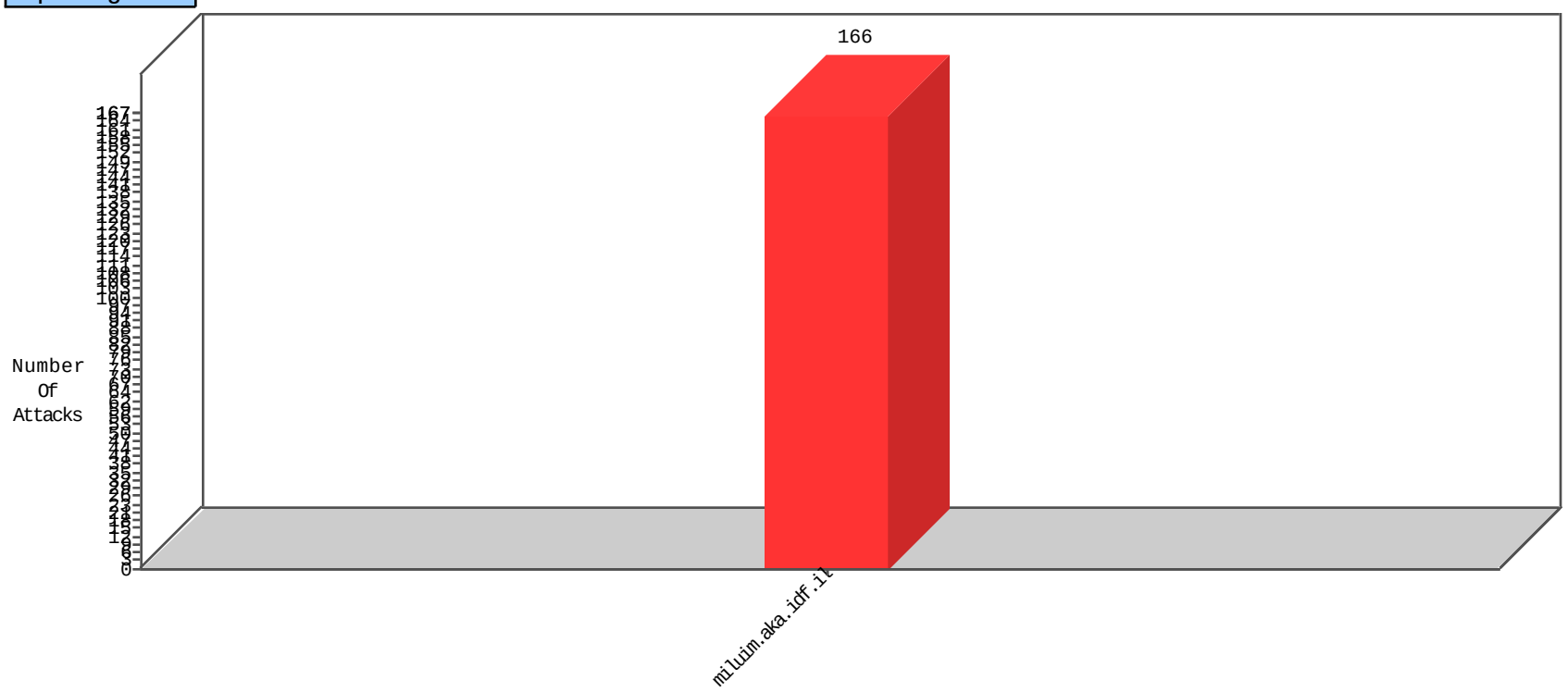
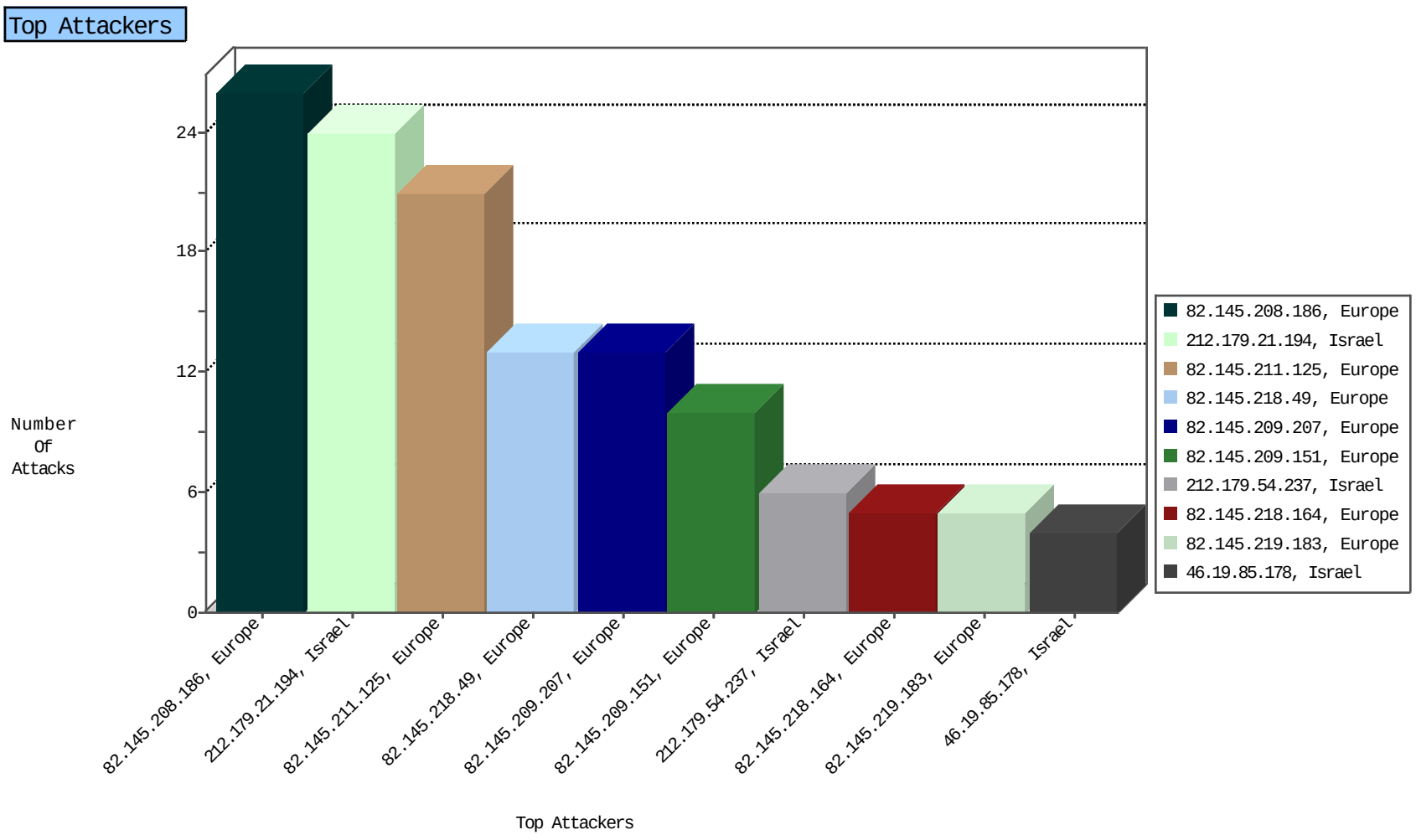
02-25-2016 to 02-26-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-25-2016 to 02-26-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.145.208.186	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	26
82.145.211.125	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	21
82.145.209.207	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	13
82.145.218.49	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	13
82.145.209.151	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
82.145.218.164	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	5
82.145.219.183	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	5
81.218.56.245	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
82.80.217.70	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
31.168.225.146	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
119.41.216.179	China	147.237.0.120	miluim.aka.idf.il	Invalid TCP Flags	drop	NetV-London	2
81.218.56.125	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	1
192.99.63.194	Canada	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
208.100.26.228	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
66.249.81.230	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1

02-25-2016 to 02-26-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

02-25-2016 to 02-26-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
94.102.49.151	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.173		147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.162.178	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.209.141.122	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
45.32.80.167		147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1

02-25-2016 to 02-26-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
2.54.177.4	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4608
2.54.180.29	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4608
185.3.147.236	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
185.3.144.126	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
5.22.130.245	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
109.67.145.173	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	477
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
100.45.61.223	United States	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
79.180.168.205	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
46.19.86.56	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	342
77.127.2.70	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
37.26.147.232	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	169
62.219.238.10	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
77.126.151.124	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
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
37.26.149.184	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	144
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
46.19.85.61	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
64.134.168.1	United States	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
2.52.188.175	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
2.52.17.118	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	77
185.27.105.154	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
85.65.24.106	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	72
2.52.11.217	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	65
46.19.85.10	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	64
212.68.132.218	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
46.19.85.10	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	64
46.121.254.163	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	53
46.19.85.240	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	52
46.19.85.104	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	50
46.19.85.44	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	41
46.19.85.192	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	40
85.65.24.106	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
2.52.130.53	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
79.183.129.98	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
185.3.144.4	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
77.127.29.129	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.179.205.184	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.192	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.214	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
192.116.177.154	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
46.19.85.39	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
109.66.26.225	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	25
46.19.85.39	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
109.66.26.225	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
79.176.167.185	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.120.126.24		147.237.0.120	miluim.aka.idf.i	drop	SAM rule	drop	17
46.19.85.200	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.129	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
212.179.19.65	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16

02-25-2016 to 02-26-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	14
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	8
109.253.204.237	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1449-he/miluim.aspx'	Block	3
37.142.216.160	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1449-he/miluim.aspx'	Block	2
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	2
66.249.78.191	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/s8009654/appdata/local/microsoft/windows/temporary internet files/content.outlook/ac1ertwo/hachvana.mod.gov.il	Block	1
46.19.85.178	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version __atuvc=0%7C4%2C0%7C5%2C0%7C6%2C0%7C7%2C1%7C8; __atuvs=56cec30224dd573b000	Block	1
213.151.36.128	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjo7eurt5hlahvgrxokhq-jdfoqfggimaa&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	1
157.55.39.79	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
46.117.130.44	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1449-he/miluim.aspx'	Block	1
5.39.222.159	Netherlands	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/rom-0	Block	1
85.65.170.93	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 85.65.170.93	Block	1
46.19.85.178	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL asp.net_sessionid=v4rykwr4uqzxtlulzkhiwevc;	Block	1
157.55.39.102	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
66.249.64.7	United States	147.237.0.120	miluim.aka.idf.i	Unknown Parameter fileld in www.miluim.aka.idf.il/console/core/doc_mgr/library/manage/resource/getfilecontent.hh.asp	Block	1
85.65.170.93	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
46.19.85.178	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method 476d5.1452168846.1.1452168846.1452168846.; in URL asp.net_sessionid=v4rykwr4uqzxtlulzkhiwevc	Block	1
185.82.200.91		147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
66.249.78.184	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/s8009654/desktop/בהצ "מועדון דעה"	Block	1
46.19.85.178	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
213.151.36.128	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 213.151.36.128	Block	1
46.19.86.37	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1451-he/miluim.aspx'	Block	1
2.54.173.15	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1449-he/miluim.aspx'	Block	1

02-25-2016 to 02-26-2016