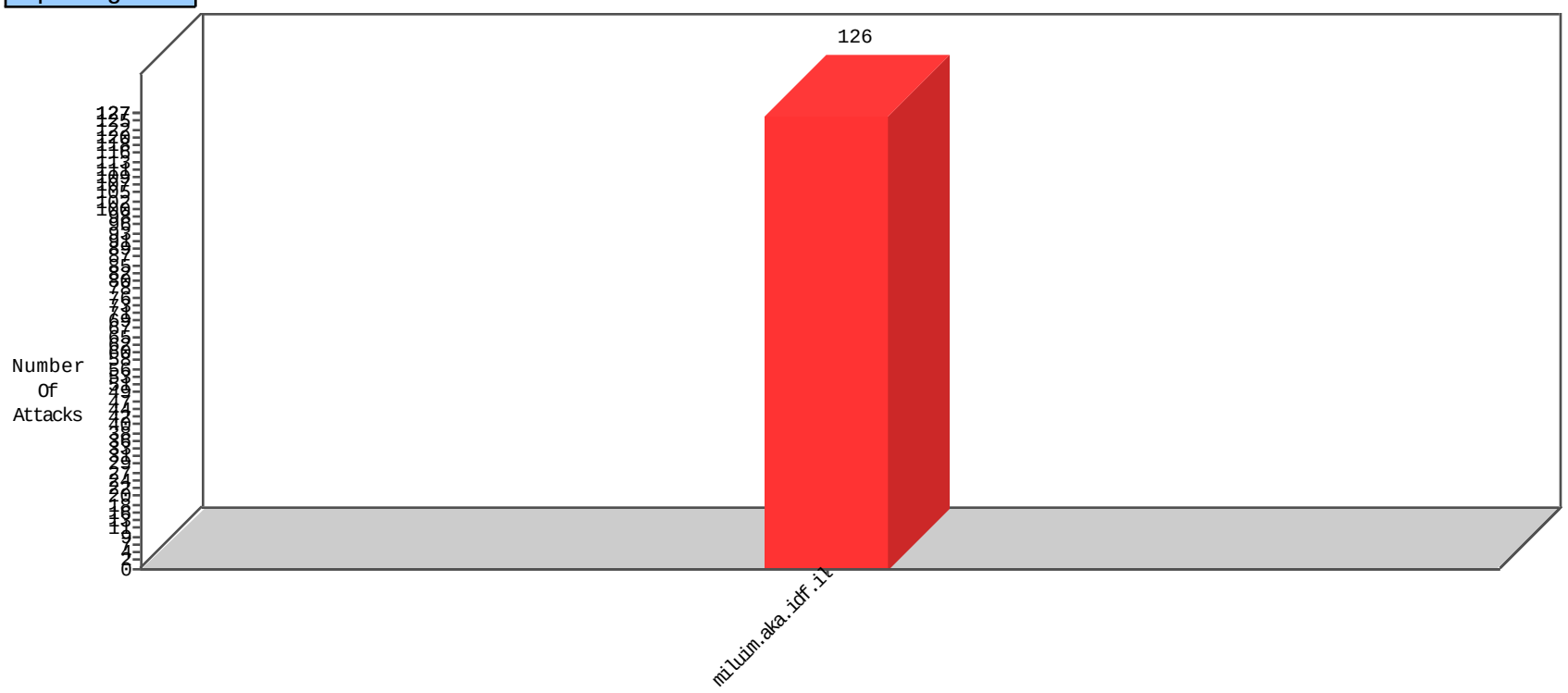
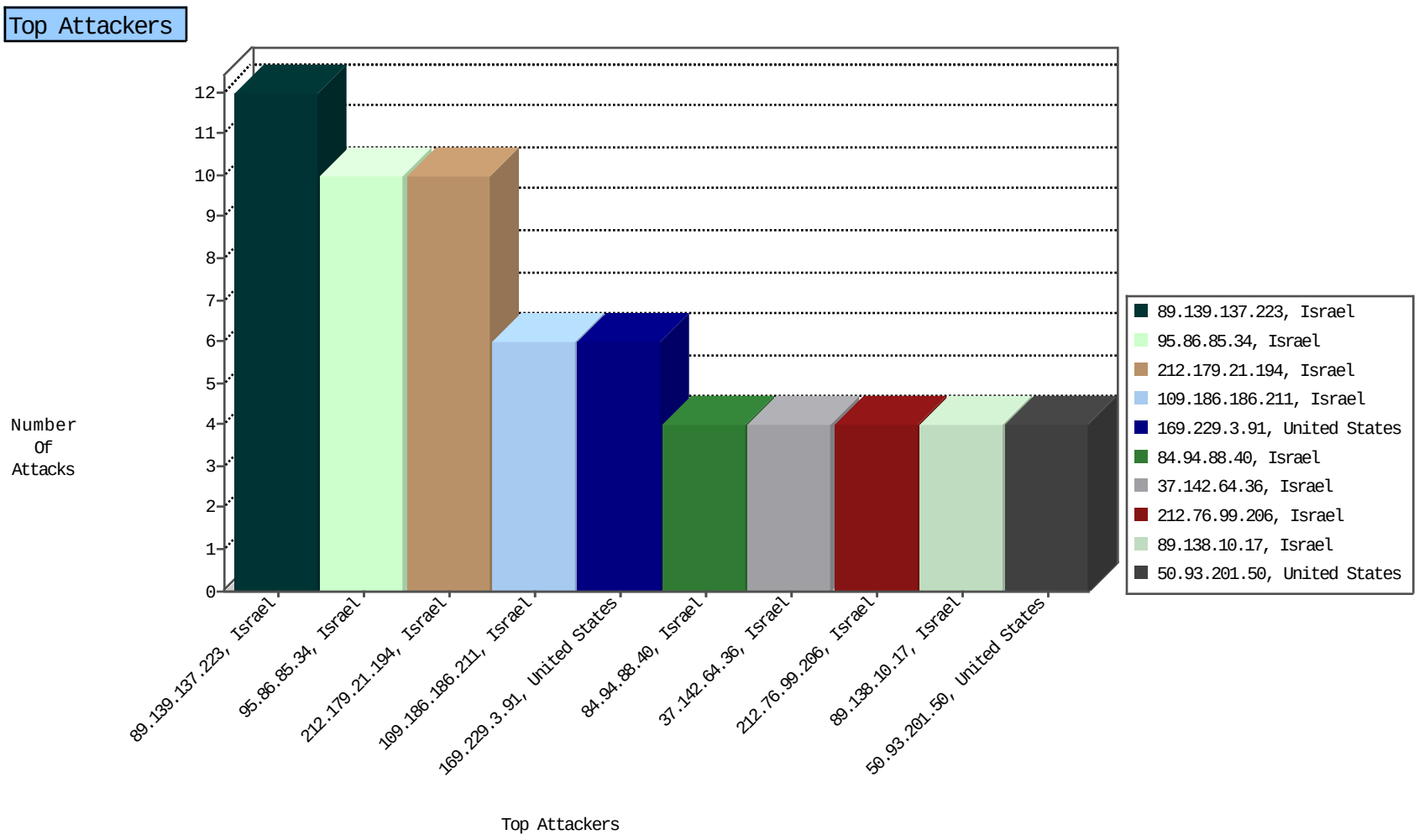
02-21-2016 to 02-22-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-21-2016 to 02-22-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
37.26.148.140	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	2
221.198.170.79	China	147.237.0.120	miluim.aka.idf.il	Invalid TCP Flags	drop	BBL-Frankfurt	2

02-21-2016 to 02-22-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

02-21-2016 to 02-22-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
88.249.106.23	Turkey	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.234.38.249	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
119.81.107.18	Singapore	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	1
109.186.186.211	Israel	147.237.0.120	miluim.aka.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
110.34.192.186	Thailand	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.118	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1

02-21-2016 to 02-22-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
2.54.17.49	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2313
82.81.7.59	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.176.176.51	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.180.37.66	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
109.67.166.179	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	378
79.180.160.132	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
79.181.112.201	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
2.54.29.99	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
2.54.157.217	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
109.64.98.166	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
46.19.85.186	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	168
46.19.85.186	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	168
2.52.62.107	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
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
2.52.151.74	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.176.61.135	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
77.127.2.70	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.177.29	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
5.28.171.204	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.125.24		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.60.83	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
79.178.31.102	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.85.232	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
84.94.200.157	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	64
46.19.85.46	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
2.52.24.47	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.221	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.120.104.51	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.86.180	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.221	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
192.114.23.18	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
188.120.148.97	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	30
37.46.39.172	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
2.52.180.196	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
89.139.247.17	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
109.66.201.74	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.182.58.192	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.181	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.117.224.187	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.85.47	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
87.69.163.137	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
2.54.150.21	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
212.235.72.236	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.85.47	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
87.69.163.137	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
79.181.104.130	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.85.181	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
77.127.162.108	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16

02-21-2016 to 02-22-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
95.86.85.34	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 95.86.85.34	Block	8
89.139.137.223	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 89.139.137.223	Block	6
89.139.137.223	Israel	147.237.0.120	miluim.aka.idf.i	Distributed PHP Attempt	Block	4
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter in www.miluim.aka.idf.il/1443-he/miluim.aspx	Block	4
109.186.186.211	Israel	147.237.0.120	miluim.aka.idf.i	Multiple _vti_ from 109.186.186.211	Block	2
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
84.94.88.40	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	2
141.212.122.129	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /x	Block	2
50.93.201.50	United States	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	2
212.76.99.206	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.76.99.206	Block	2
79.177.34.105	Israel	147.237.0.120	miluim.aka.idf.i	Distributed PHP Attempt	Block	2
84.95.4.122	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/14	Block	2
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	2
95.86.85.34	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjusln3tonlahxn_nikhxxnafiqfggimaa&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	2
89.138.10.17	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	2
212.76.99.206	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjo2salvynlahvh7a4khbkybqcqfggimaa&sig2=vgadfbfscf1iyf_clbtgza&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	2
79.177.34.105	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	2
89.139.137.223	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	2
37.142.64.36	Israel	147.237.0.120	miluim.aka.idf.i	Distributed PHP Attempt	Block	2
109.186.186.211	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 109.186.186.211	Block	2
54.193.38.9	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	2
84.94.88.40	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 84.94.88.40	Block	2
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Distributed PHP Attempt	Block	2
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	2
80.178.144.84	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 80.178.144.84	Block	2
194.90.25.122	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter in www.miluim.aka.idf.il/1441-he/miluim.aspx	Block	2
77.127.187.96	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/14	Block	2
66.249.75.188	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 66.249.75.188	Block	1
46.116.27.140	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1446-he/miluim.aspxâ€?â€Ž	Block	1
4.79.123.3	United States	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter &y	Block	1
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/images/1.he/bullet7.gif	Block	1
79.179.196.238	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1443-he/miluim.aspx'	Block	1
66.249.75.188	United States	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 66.249.75.188	Block	1
40.77.167.62	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
212.199.34.34	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
89.138.10.17	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 89.138.10.17	Block	1
80.178.144.84	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1446-he/miluim.aspxâ€?â€Ž	Block	1
2.54.28.96	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1443-he/miluim.aspx'	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Malformed HTTP Header Line 1	Block	1
66.249.75.188	Israel	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
109.186.186.211	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/_vti_bin/owssvr.dll	Block	1
46.116.27.140	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1446-he/miluim.aspx'	Block	1
31.44.143.182	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewivy9smwijlahveqbqkhyakcpqqfggimaa&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	1
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	1
79.179.196.238	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1446-he/miluim.aspxâ€?â€Ž	Block	1
66.249.75.188	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
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
50.93.201.50	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
46.116.27.140	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1443-he/miluim.aspxâ€?â€Ž	Block	1
80.178.144.84	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1446-he/miluim.aspx'	Block	1
4.79.123.0	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/mailto:moked_miluim@mail.idf.il	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Malformed URL	Block	1
66.249.75.188	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.253.208.132	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1446-he/miluim.aspxâ€?â€Ž	Block	1
46.116.224.123	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
85.64.36.73	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1446-he/miluim.aspxâ€?â€Ž	Block	1
79.179.196.238	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1446-he/miluim.aspx'	Block	1
194.90.25.122	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1441-he/miluim.aspx=	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Header Name	Block	1

02-21-2016 to 02-22-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
66.249.75.188	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
46.116.27.140	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1443-he/miluim.aspx'	Block	1
89.138.10.17	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1
4.79.123.2	United States	147.237.0.120	miluim.aka.idf.i	Unknown Parameter q in www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method Â‡nÂ…$tÃ¢[[#25]]/Ã€Â„Â¥	Block	1
79.179.196.238	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1443-he/miluim.aspxâ€?â€Ž	Block	1
66.249.75.188	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter userid in www.miluim.aka.idf.il/console/core/doc_mgr/library/manage/resource/getfilecontent.hh.asp	Block	1
109.253.208.132	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1446-he/miluim.aspx'	Block	1
89.163.251.200	Germany	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /myadmin/scripts/setup.php	Block	1
50.93.201.50	United States	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 50.93.201.50	Block	1
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter in www.miluim.aka.idf.il/404.aspx	Block	1
85.64.36.73	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1446-he/miluim.aspx'	Block	1
2.54.28.96	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1443-he/miluim.aspxâ€?â€Ž	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method Â‡nÂ…$tÃ¢[[#25]]/Ã€Â„Â¥	Block	1

02-21-2016 to 02-22-2016