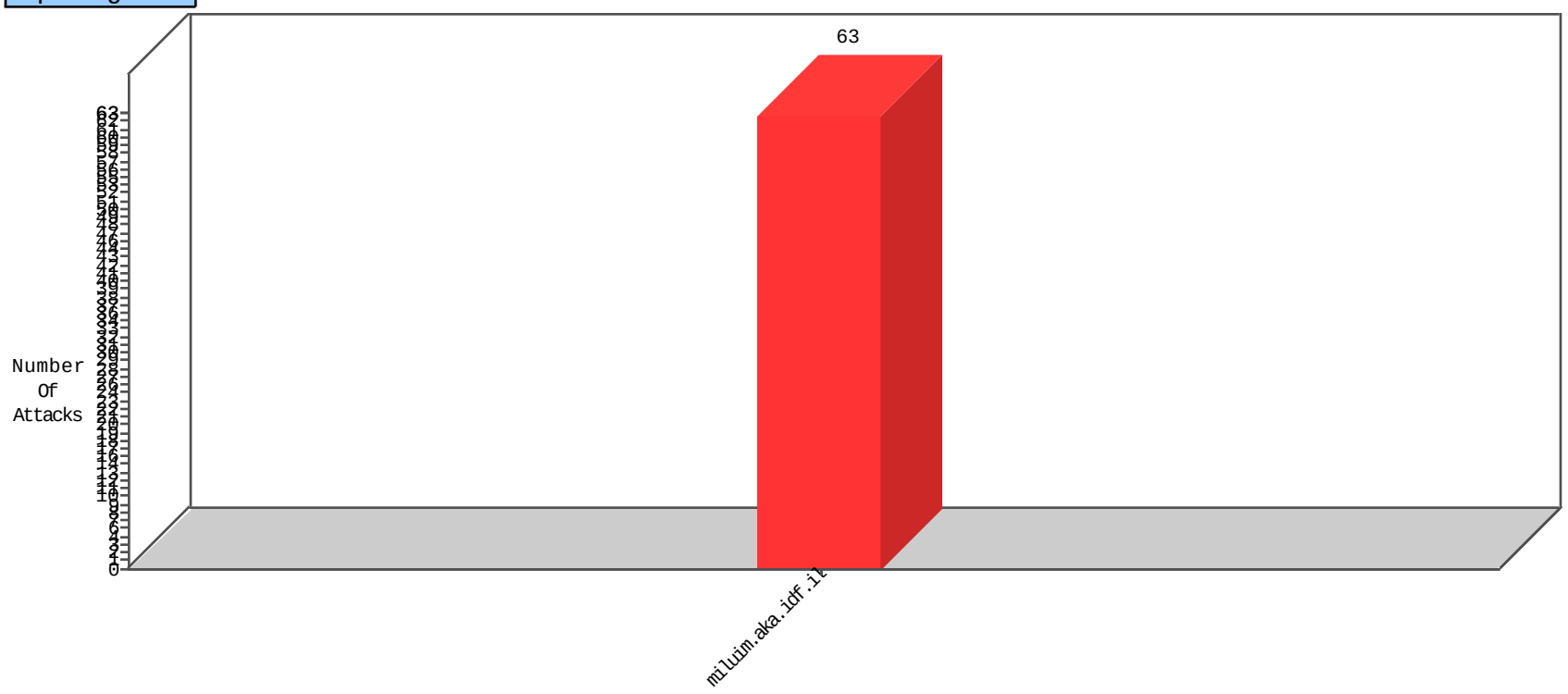
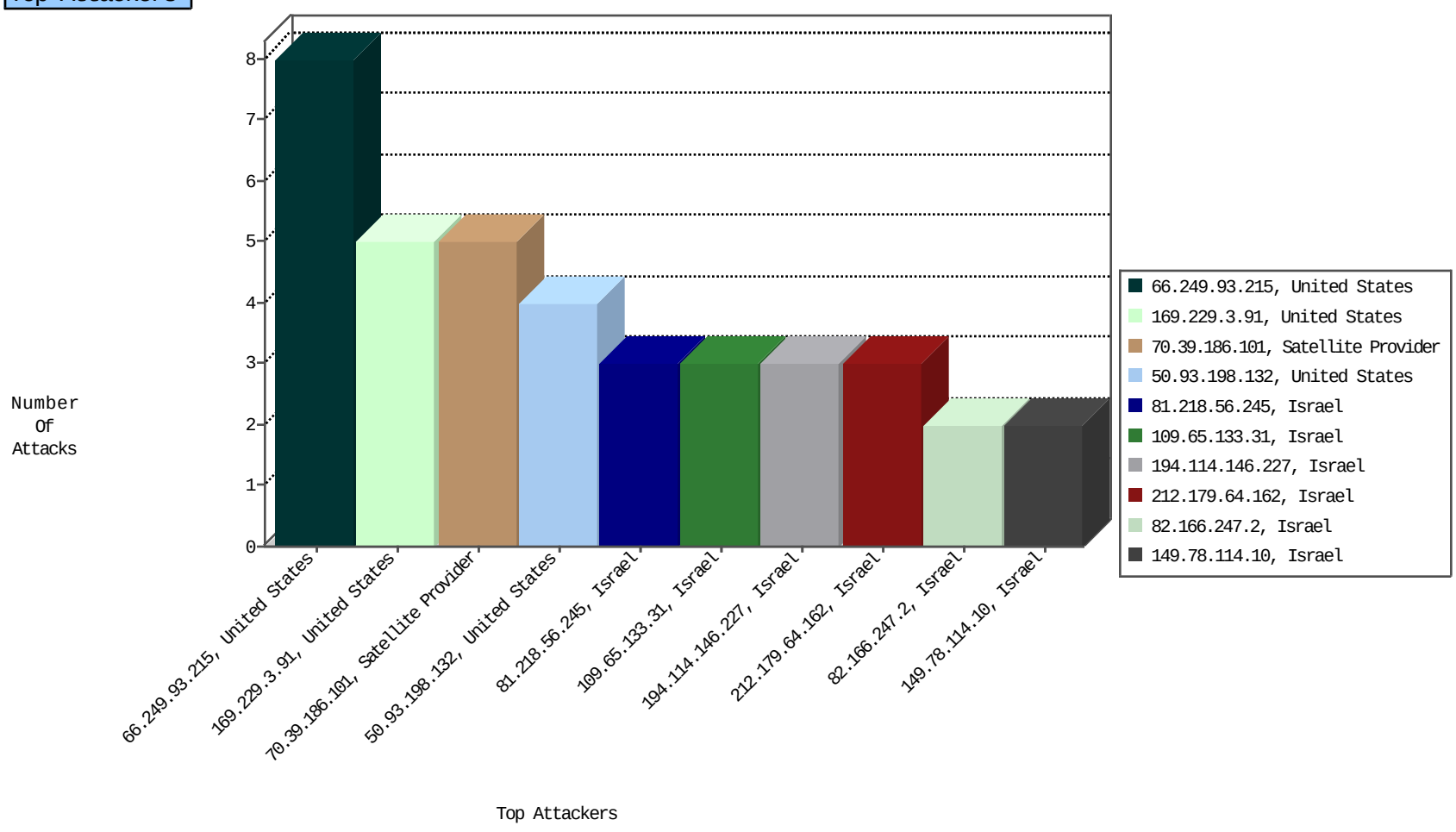
03-14-2016 to 03-15-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



03-14-2016 to 03-15-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
81.218.56.245	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
109.65.133.31	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
212.179.64.162	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
70.39.186.101	Satellite Provider	147.237.0.120	miluim.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	NetV-London	3
70.39.186.101	Satellite Provider	147.237.0.120	miluim.aka.idf.il	JLM_Under_Attack_Con_Http	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

03-14-2016 to 03-15-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
82.193.127.15	Ukraine	147.237.0.120	miluim.aka.idf.il	C1000074: HTTP: majestic bot	Block	2

03-14-2016 to 03-15-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	8
94.102.48.194	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
184.80.10.136	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
184.80.10.136	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.116.37.210	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1

03-14-2016 to 03-15-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
70.39.186.101	Satellite Provider	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3725
70.39.186.101	Satellite Provider	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3725
46.19.86.148	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2313
109.65.190.142	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
31.168.83.233	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.179.193.60	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
46.19.86.215	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	1855
195.200.205.34	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1764
87.71.13.59	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1512
79.178.57.167	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	468
79.183.206.78	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	378
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	349
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	349
2.52.157.117	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
2.54.61.64	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
185.24.206.56	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	250
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	238
2.52.14.85	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	236
46.19.86.153	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
46.19.86.86	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
46.19.86.254	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	198
93.94.40.14	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	196
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	163
2.54.4.252	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
79.180.163.168	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
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
5.28.167.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.190.119	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
37.26.146.188	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	144
79.182.25.35	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.55.17.78	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.65.15.224	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
94.159.150.139	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.64.187.116	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
62.219.209.92	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	144
2.54.18.214	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
46.19.86.58	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
46.19.86.180	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
2.52.14.85	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	112
2.52.14.85	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	112
2.52.14.85	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	112
37.26.149.172	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	100
37.26.147.204	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
2.52.44.32	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	94
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	94
212.29.210.131	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	91
2.52.157.87	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
62.219.115.209	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	2
82.166.247.2	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	2
50.93.198.132	United States	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	2
149.78.114.10	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
84.108.145.78	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/resource/userfollowresource/create/	Block	1
50.93.198.132	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspx/xmlrpc.php	Block	1
194.114.146.227	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/1935.gif	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request request version	Block	1
94.230.95.82	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/../../images/shared/hp/nav_bg.png	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method [[#6]] in URL ‡[[#25]]אשא[[#18]][[#14]]3[[#12]]§z"[[#30]][[¡#14[[]#12¹o]]:7lzDŽ˛	Block	1
149.78.114.10	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
87.69.158.111	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
66.249.73.219	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method [[#6]]	Block	1
94.230.95.82	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
94.230.95.82	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
81.218.241.26	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/	Block	1
50.93.198.132	United States	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 50.93.198.132	Block	1
185.89.217.234		147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/../images/shared/hp/hp_icon.png	Block	1
157.55.39.117	United States	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 157.55.39.117	Block	1
87.69.158.111	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
66.249.73.235	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/general.aspx	Block	1
199.16.156.125	United States	147.237.0.120	miluim.aka.idf.i	Unknown Parameter platform in www.miluim.aka.idf.il/894-he/miluim.aspx	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in URL ‡[[#25]]אשא[[ר#18[[]#14]]3[[#12]]03#[["z§]]¡[[#14]][[#12]]o¹:zl7˛ŽD	Block	1
141.212.122.64	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /x	Block	1
188.120.148.122	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/resource/userfollowresource/create/	Block	1
157.55.39.117	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/headerupper/	Block	1
94.185.83.100	Sweden	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
66.249.73.235	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/homepage.aspx	Block	1
204.12.251.37	United States	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/../shared/usercontrols/footer/1230-he/miluim.aspx	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Malformed URL ‡[[#25]]אשא[[ר#18[[]#14]]3[[#12]]03#[["z§]]¡[[41#]][[21#]]o¹:zl7˛ŽD	Block	1