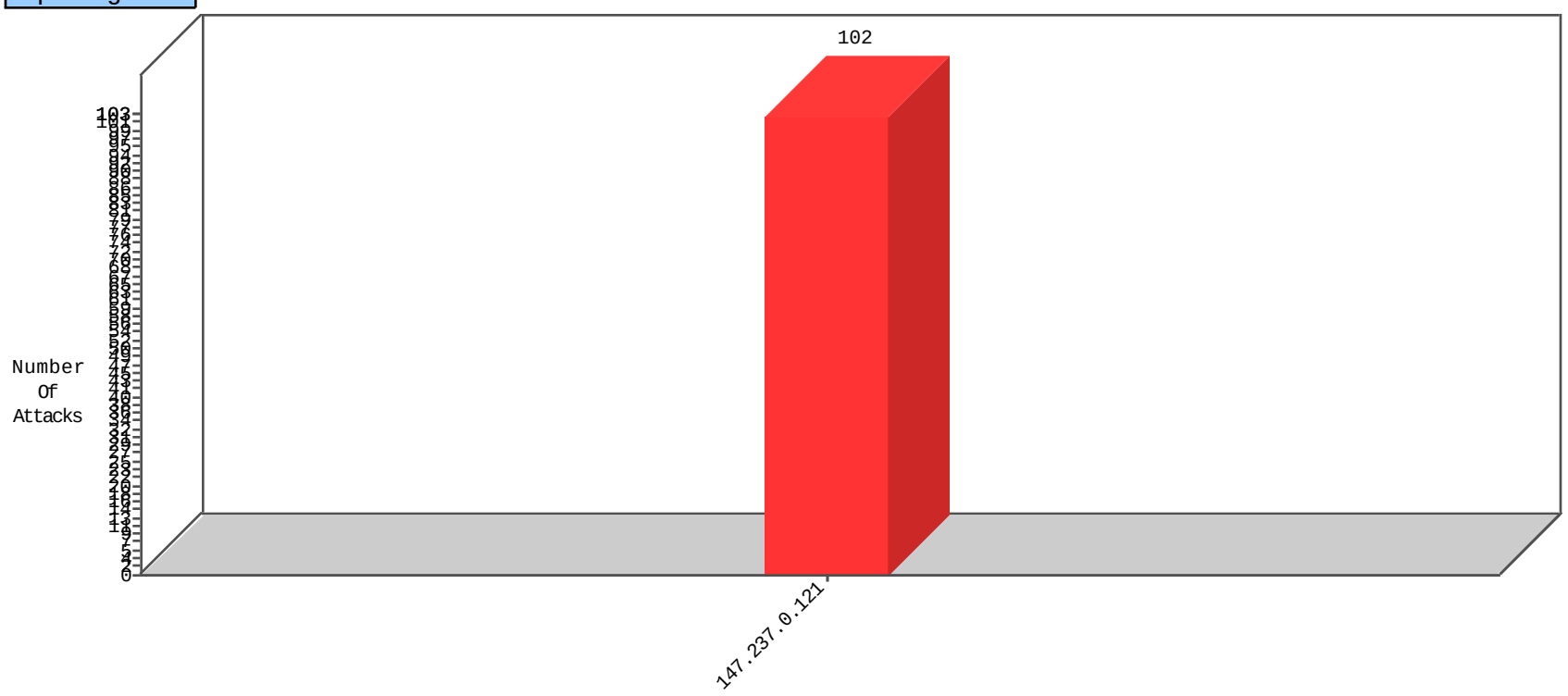
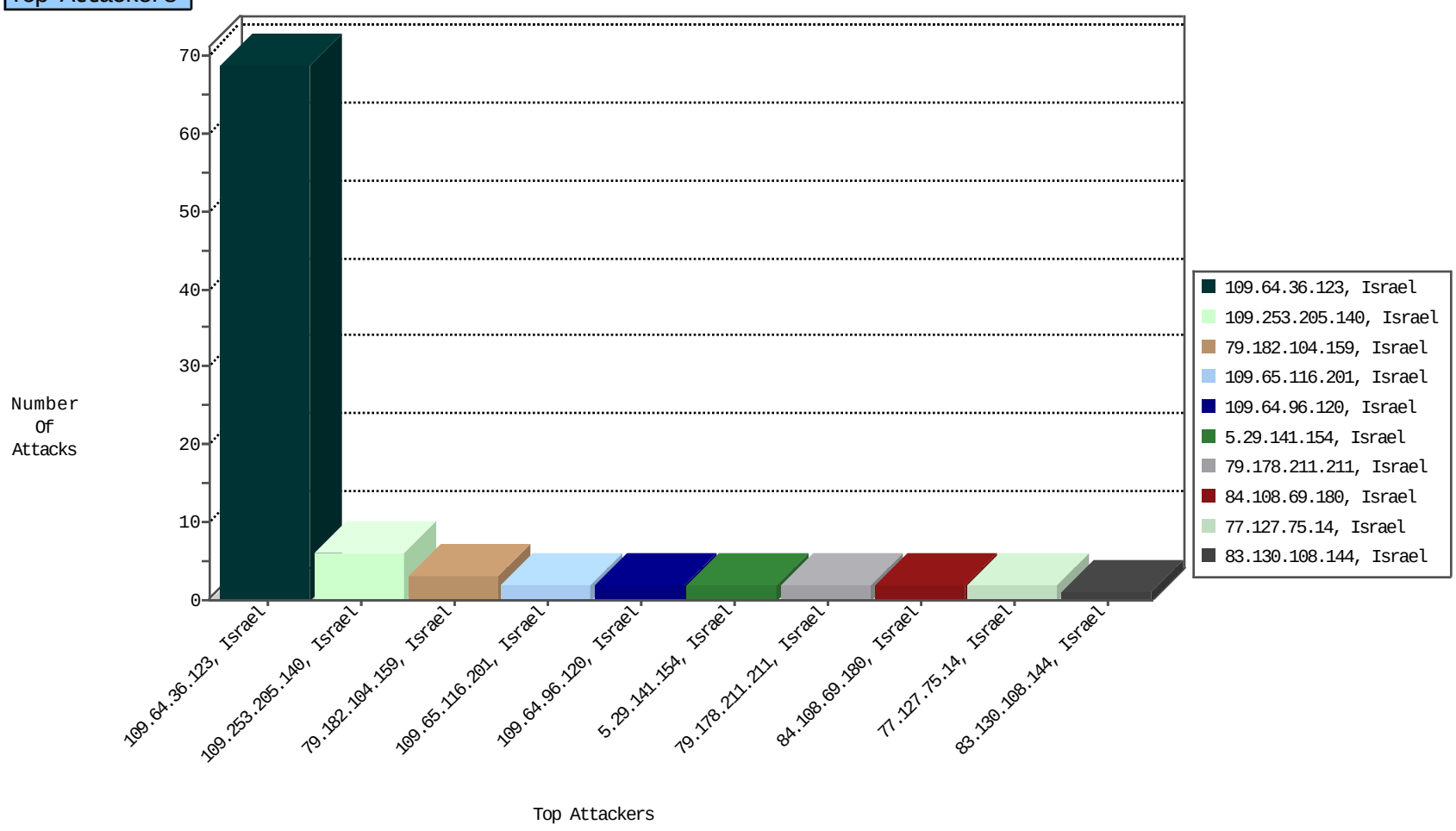
01-15-2016 to 01-16-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-15-2016 to 01-16-2016

Top Attackers In DDoS-Defence

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

01-15-2016 to 01-16-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-15-2016 to 01-16-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
109.64.36.123	Israel	147.237.0.121		SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
89.248.172.98	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1

01-15-2016 to 01-16-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	877
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	752
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	609
149.78.169.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	285
149.78.37.226	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	203
166.70.207.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
149.88.141.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	147
50.7.178.100	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	134
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	132
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	103
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
149.88.242.15	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	91
149.78.148.35	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
149.78.229.33	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
149.78.229.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
149.78.238.35	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
146.0.77.237	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
149.88.142.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
157.55.39.174	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.74.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
66.230.230.230	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.78.87.204	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
64.120.47.67	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
52.90.52.42	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.74.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
37.142.244.96	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.36	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
77.125.159.77	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
46.19.86.36	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
66.249.69.98	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
149.88.100.253	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
66.249.81.129	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
209.126.117.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
94.230.86.193	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	9
2.54.51.243	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	9
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
141.8.184.5	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
141.8.132.85	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9

01-15-2016 to 01-16-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.64.36.123	Israel	147.237.0.121		Multiple Unknown HTTP Request Method from 109.64.36.123	Block	7
109.64.36.123	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Method from 109.64.36.123	Block	6
109.64.36.123	Israel	147.237.0.121		Multiple Abnormally Long Header Line from 109.64.36.123	Block	5
109.64.36.123	Israel	147.237.0.121		Multiple Malformed URL from 109.64.36.123	Block	5
109.64.36.123	Israel	147.237.0.121		Multiple Abnormally Long Request from 109.64.36.123	Block	5
109.64.36.123	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Name from 109.64.36.123	Block	5
109.64.36.123	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Value from 109.64.36.123	Block	4
109.64.36.123	Israel	147.237.0.121		Multiple Malformed HTTP Header Line from 109.64.36.123	Block	4
109.64.36.123	Israel	147.237.0.121		Multiple NULL Character in Header Name from 109.64.36.123	Block	4
109.64.36.123	Israel	147.237.0.121		Multiple Illegal HTTP Version from 109.64.36.123	Block	3
109.253.205.140	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	3
79.182.104.159	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 47DDA4565553F1C871E82560DF8740D353629AE551AB06B3FC5D98C0567213038938E220BD069F5B9B94CFFECF72DC72E6A9096D187345E0099CD0EBBE5EAC9AE3D8F03893199B89A1D943A8A769187A05CF5E4328F8BB1F7044D97F2CCB2EB50E0CA4E9C5B5692CCD7A2D313C156BA8FFDA6AFAA7D9CD10C4C1CFDCF44DE46D, Observed 064B3DCDABAFFAA8DDABC2AF51ED41E8DE740F8C6B0EE1AB666E4E7633F7C569B196018AA6D9DFE8F03CB72E6B5C1CEBC39B0E118B9CA72E3BDE392586C069D85652A44C1084814E17034978FF9695C079FBFB73105992AF734297493652EC68AC73B3	None	3
109.64.96.120	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
109.65.116.201	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 9EE61CD90F551DB88F6155A6B34BC212CF537E74EBC09AEF6F546901D6AAB9802845B81B36A173F0446EF8CDD053DF5C4B3A931A96E82B6FD0410A46CA71CBCDC134FE26C82F08EEBDE8A4C9E6B87C2398DB1B2ED32E2173B8E09B0C7FC12C9F2EDAED10043DCD3F71946F0D08FAF5F8062F03EC4CD285BD0442424A02D3C5F2, Observed 1BC85FE8B9315BEE6CB5C0976470473EEEA8F2CE295EF879DEFA46AED94DE78138D446C2B746CE868DC7B57E994E7F62A1921728E60457FD8606CB02D1BEFAAD703FEAF3D524C04F2CD3440DE45B591539347646C4BD38F8D32027395BE69FD0CCD014	None	2
77.127.75.14	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
109.253.205.140	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.211.211	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
109.64.36.123	Israel	147.237.0.121		Multiple Illegal Byte Code Character in URL from 109.64.36.123	Block	2
84.108.69.180	Israel	147.237.0.121		Suspicious Response Code	Block	2
109.64.36.123	Israel	147.237.0.121		Illegal Byte Code Character in URL .ÃŸ[[#29]]g<×”×?iÂ¬[[#18]]×Ÿ[[#23]]Ã?	Block	1
109.64.36.123	Israel	147.237.0.121		Abnormally Long Header Line request header name	Block	1
109.253.205.140	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.253.205.140 (sigalgs DoS Attack)	None	1
109.64.36.123	Israel	147.237.0.121		NULL Character in Header Name at [[#28]]Â…Â—Â»+NxÂ´Â¬Ã”ÃžcÃ½Â§>Ã—jzPnÃ¸ =[[#14]]eÂ¸ kkÂƒÃ¾Â¶Ã¡Ã«?Â¡[[#2]]VK<Â½Ã…[[#0]]bÃ?Â¾[[#27]]EcÃ-ÂŸÂ¹ÃŒÃ¢Ã°Â-Ã„[[#15]]ÃŒÂ‹Ã'Ã—[[#2]]Ã½[[#3]]Ã±Ã??Ã‹	Block	1
79.180.175.209	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C86BCEB49CD02ECB0DE36468F21673A6AE80771126023C7F1C78621D4950D430702A3B4DA5609A7D897A1DD53E83ECACED9E343FA988081306AC75509D28E7ECCFDD89D760A5B3F80744F9A7120E281D3917A5CE140AA27CF4AE4C5E651C352CDBE68E0908D0BC722A78D81AD0585182476D2C019B026264AB12ACA91FB18934, Observed 0062C7BEBAE8B2ED034609493695DCD850CE814E61541EC84F0FE7FF8075DB2D524C482589A13930EC20A5E06C80B31792059EADCA1794B3F6FE63AEDF1A903DB125B7CF5DF6A2C42223DF552128D7DB2693B0114B82F70A89FEC0CAFF4A84CF802AB0	None	1
109.64.36.123	Israel	147.237.0.121		Malformed URL .ÃŸ[[#29]]g<×”×?iÂ¬[[#18]]×Ÿ[[#23]]Ã?	Block	1
109.64.36.123	Israel	147.237.0.121		Illegal Byte Code Character in Method ciÃ¤	Block	1
212.117.140.158	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
84.108.238.214	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.255.253.47	Russian Federation	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.64.36.123	Israel	147.237.0.121		Multiple NULL Character in Method from 109.64.36.123	Block	1
109.64.36.123	Israel	147.237.0.121		Illegal HTTP Version xpÂ”*Ã?&Â•aÂ¨ÃŠÂ¢Â²ZJWÃ'-[[#5]]Â¿ a\ÃŠMÂ…ÃŒ[[#30]]{Ã³[[#5]][[#24]]Â±EÂœYcÃ§Ã§Â¨_+Ã?[[#23]]-Â·Ã˜[[#22]]oÃ©^Ã»Ã‹Ã¬Â½_Ãž7Ã¶Ã?Â¾Â„[[#22]]<Ã½Â?ÃƒÂ©Â“[[#5]]Â´[[#27]]vÂ•Ã·Â¦Â?Â—Â¡Â™[[#30]]UÃ–Â¾XpÂµÂ–kÂ©y[[#1]]MxkOÂ²ÃŠÂŸ)Ã½EÂ”Ã¾Â-SÂ½Ã¿ [[#14]]Â¯Ã€[[#23]]Ã¿,3oÃ?NÂ³[[#30]]Â¾$-[[#28]]6UÂ©Ã†Ã‰h[[#20]]}FÃ«wÂ¾Ã¬	Block	2
109.64.36.123	Israel	147.237.0.121		Abnormally Long Request request version	Block	1
109.64.36.123	Israel	147.237.0.121		NULL Character in Method R[[#24]]Ã³lÂ•Ã,Ã±?Ã»erÃ¡Â‰[[#8]]vÂ½Â³7ÃªÂªEaÂ¢-Ã‰Ã B/Â?:Â–Â“3Â€•Ã¹Â?[[#12]][[#25]]-mTÃ?ÃŠ#2>^[[#2]]Ã–bÂ?Ã¢Â½;<XL[[#8]][[#11]]Ã¹Â¨%ÃšÃˆ'[[#15]]qDÃ¿[;Ã‰[[#11]]6Ã†'ÂŠÃ‹Ã¨[[#0]]Â Âµ[[#30]]Â‡Ã´Ã [[#3]]-+Â—[[#15]]%Ã²lÂ”Ã§Â‘[[#26]][[#2]]Â Â¤Ã?U[[#20]]+Ã?Ã Ã,[[#3]]P[[#14]]b[[#19]]g[[#16]]Â‹Â„AeÃŒÂ¦Ã§\ÂŸÂ§Ã˜V[[#0]]Â¿Ãƒ%Â›;	Block	1
2.54.41.174	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
109.64.36.123	Israel	147.237.0.121		Illegal Byte Code Character in Parameter Name &Â®[[#3]]ZÃ›Ö°Ö´[[#6]]3^[[#1]]5g[[#4]]Â?[[#18]]k[[#7]]IÂ°Ëœ[[#28]]5Â ÃŠ×¡×²â,ªG?Â³Â«Â?qO[[#27]]"Â¥@[[#31]]×?[[#2]]Ö» in ÃŠ×›×“eÃ›Âš6Âœ	Block	1
85.65.103.27	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
109.64.36.123	Israel	147.237.0.121		Illegal URL Path Encoding 1â€?Ã¼ÂœaÂ¦[[#14]]2Ã¼Ã?y[[#23]]a×´0×¥Ã¿yÖ¸ ×¢[[#5]]×•lâ€°Â¯Â¶[[#25]]Ö¼i×™Â±[[#8]]×ªÃ›m×¡\[[#26]]×œdg×•Ë†â„¢×ª[[#31]]Â?×™Ö¸Ã¿kgÂ¹z[[#20]][[#12]]^vÖ¸Â»[[#1]]â€ºÂ?â,ª7Ö´Â?[[#15]]kÂµrÂ±Â?â€žÃš~[[#8]]â,ª× ×©Ö¿_[[#25]]8`câ€“×˜×°[[#8]]oÃ¼lâ€?!×£[[#29]]×“o%	Block	1
109.64.36.123	Israel	147.237.0.121		Illegal Byte Code Character in Header Name [[#28]]Â…Â—Â»+NxÂ´Â¬Ã”ÃžcÃ½Â§>Ã—jzPnÃ¸ =[[#14]]eÂ¸ kkÂƒÃ¾Â¶Ã¡Ã«?Â¡[[#2]]VK<Â½Ã…[[#0]]bÃ?Â¾[[#27]]EcÃ-ÂŸÂ¹ÃŒÃ¢Ã°Â-Ã„[[#15]]ÃŒÂ‹Ã'Ã—[[#2]]Ã½[[#3]]Ã±Ã??Ã‹	Block	1
109.64.36.123	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
83.130.108.144	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
5.29.141.154	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 5.29.141.154 (sigalgs DoS Attack)	None	1
109.64.36.123	Israel	147.237.0.121		Illegal Byte Code Character in Query String &Â®[[#3]]ZÃ›Ö°Ö´[[#6]]3^[[#1]]5g[[#4]]Â?[[#18]]k[[#7]]IÂ°Ëœ[[#28]]5Â ÃŠ×¡×²â,ªG?Â³Â«Â?qO[[#27]]"Â¥@[[#31]]×?[[#2]]Ö» on ÃŠ×›×“eÃ›Âš6Âœ	Block	1
109.64.1.144	Israel	147.237.0.121		Double URL Encoding - parameter: ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
109.253.151.35	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
109.64.36.123	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.64.36.123 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.64.36.123	Israel	147.237.0.121		Malformed HTTP Header Line 3	Block	1
109.64.36.123	Israel	147.237.0.121		Illegal Byte Code Character in Header Value	Block	1
176.13.8.71	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1

01-15-2016 to 01-16-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.64.36.123	Israel	147.237.0.121		Unknown HTTP Request Method ciÃ¤ in URL .ÃŸ[[#29]]g<×”×?iÂ¬[[#18]]×Ÿ[[#23]]Ã?	Block	1
5.29.141.154	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1

01-15-2016 to 01-16-2016