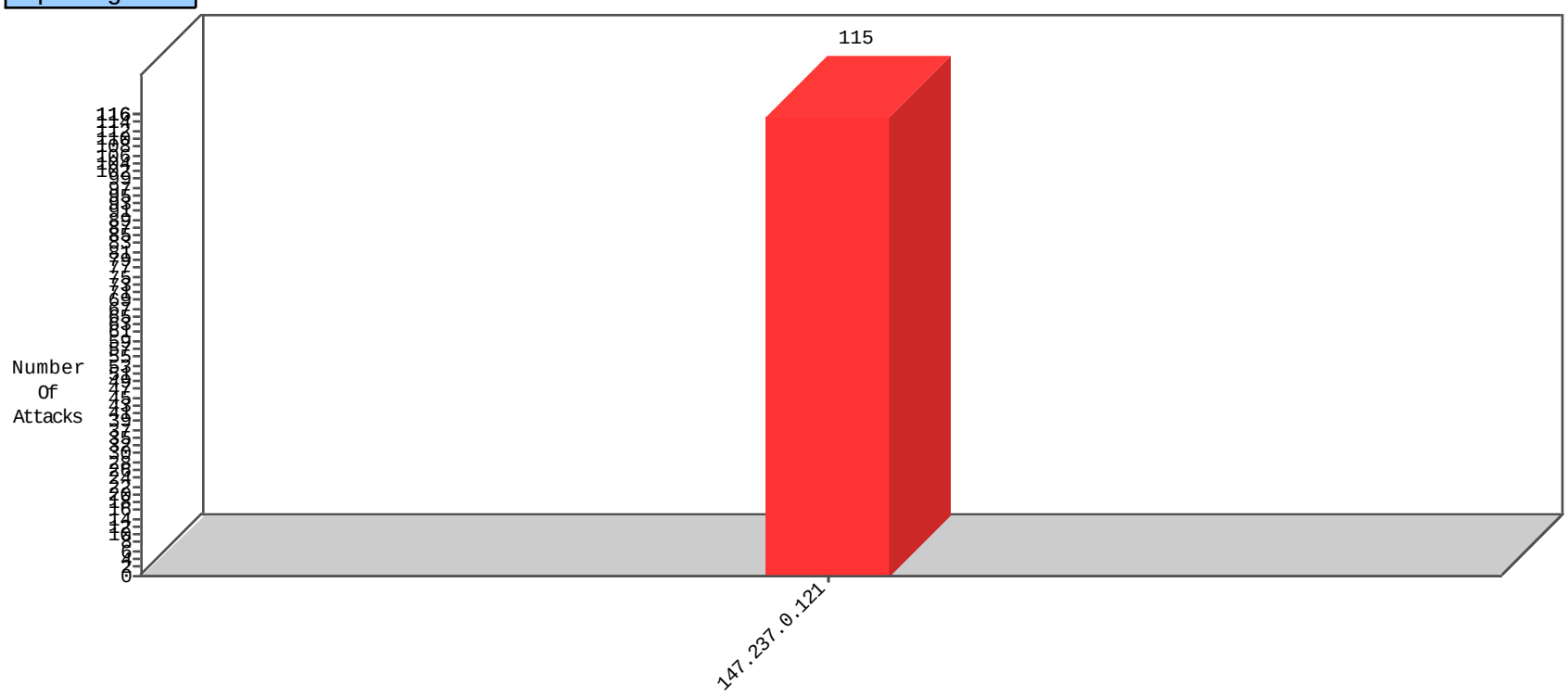
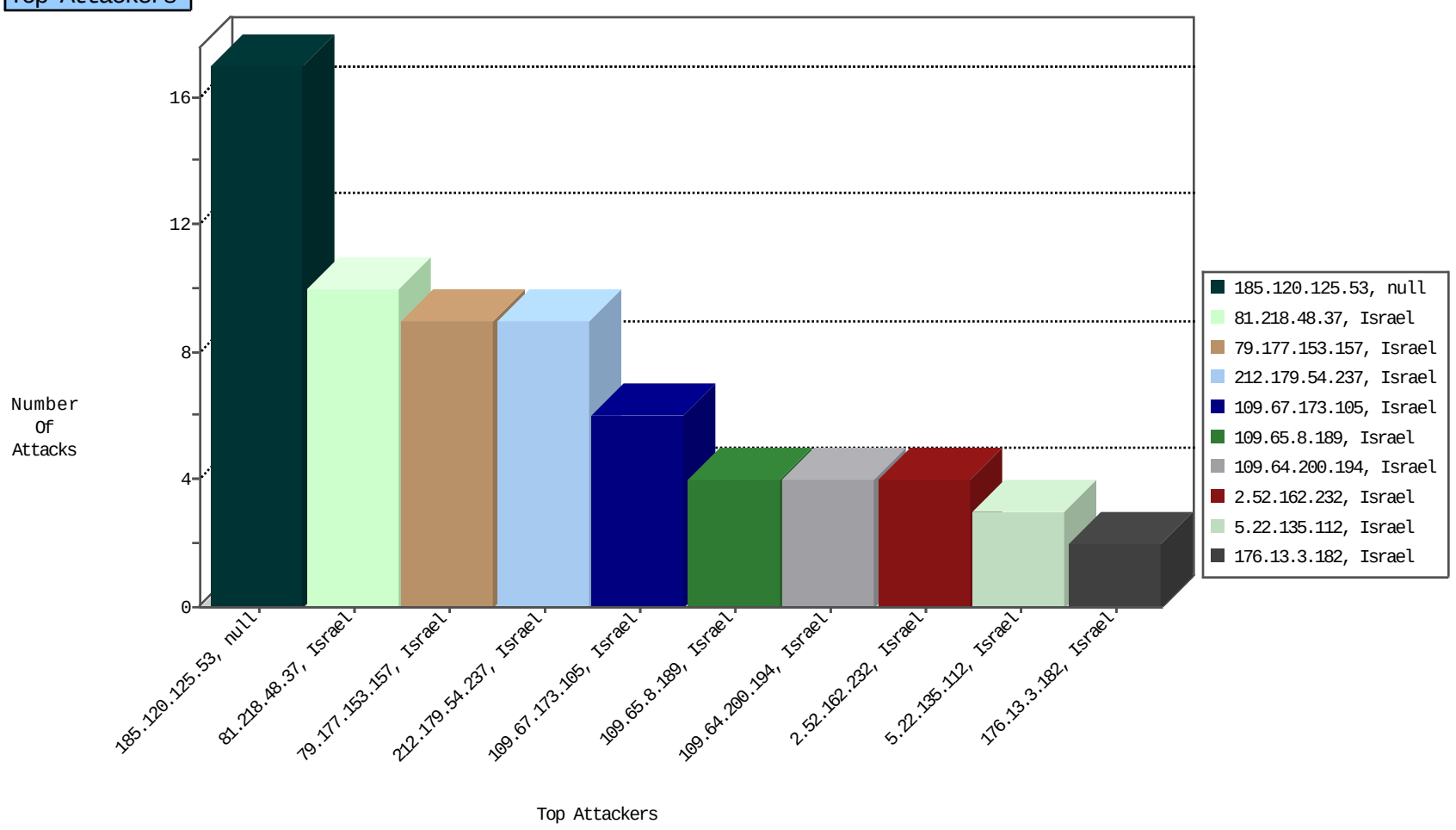
01-21-2016 to 01-22-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-21-2016 to 01-22-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	9
109.67.173.105	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	6
109.64.38.127	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	1

01-21-2016 to 01-22-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-21-2016 to 01-22-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
61.149.161.186	China	147.237.0.121		GPL SCAN nmap TCP	2
146.185.250.2	Russian Federation	147.237.0.121		ET SCAN NMAP -sS window 1024	1

01-21-2016 to 01-22-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1462
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1177
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1005
149.78.169.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	475
155.56.68.218	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	282
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	190
149.88.186.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	180
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	164
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	152
149.78.252.210	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	144
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	114
112.198.90.42	Philippines	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	95
210.61.39.253	Taiwan	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
149.78.146.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
192.114.105.254	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	72
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.78.216.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
40.77.167.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
85.238.99.168	Ukraine	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
207.46.13.108	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
5.29.109.214	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	30
84.108.137.22	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
157.55.39.78	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	23
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.21	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
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
81.218.241.26	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	19
109.64.167.148	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	18
217.68.8.59	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.66.107	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
5.22.129.124	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
66.249.64.175	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
82.102.169.113	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
207.46.13.5	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
185.27.105.161	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	13
82.166.53.161	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	13
66.249.93.208	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.249.81.129	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
54.152.228.86	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
79.181.49.193	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	10

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.120.125.53		147.237.0.121		Suspicious Response Code	Block	17
81.218.48.37	Israel	147.237.0.121		Multiple Unauthorized URL Access from 81.218.48.37	Block	5
81.218.48.37	Israel	147.237.0.121		PHP Attempt	Block	5
109.65.8.189	Israel	147.237.0.121		Suspicious Response Code	Block	4
176.13.3.182	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
31.168.247.71	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
17.78.149.178	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
84.109.208.132	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
2.52.162.232	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
2.52.39.103	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
132.72.90.145	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/images/sites16x16.png	Block	2
5.22.135.112	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
79.177.153.157	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.177.153.157 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
79.177.153.157	Israel	147.237.0.121		Abnormally Long Header Line request header name	Block	1
212.179.57.94	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
2.54.163.66	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	1
95.35.64.72	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
79.177.153.157	Israel	147.237.0.121		Illegal Byte Code Character in Method Â§sh[[#25]]Ã¼[[#26]]Â?[[#29]]Â“ Ã¢Â?mÃ¹Â¼Ã±[[#12]][[#24]]Â?QÃ°[[#18]]zÃ `Â¢Ã£EÃ‰U[[#11]]Â¦"sÂ£[[#28]]Ã”Â?Ã±Ã–Â¢cB0Âªm´Ã”Â?Ã‹vÂ‡Ã˜Ã¡^[[#7]]lÃ´K[[#12]].Ã?ÃŒÃŒÂ²A[[#7]]ÃªÂµeÂ?9Â©(ÃŒH)Â¬Âš(Â‡Â“Â¯Ã®ÃŸÂ S*Ã§Â¼Â?KÃ?T[[#4]],Ã•Ã?ÂŽÂ˜[[#23]]ÂŠOÃ§t9vÂ±#Â¾]NÂ©;Â™oÃ€Ã¾Ã¦Ã˜0Â»Ã´Ã¬Ã½ÃªÃ…[[#17]]Â–vÃ„Â?	Block	1
192.114.105.254	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.199	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.255.253.96	Russian Federation	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.126.194	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
84.109.17.181	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
2.52.162.232	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.52.162.232 (sigalgs DoS Attack)	None	1
79.177.153.157	Israel	147.237.0.121		NULL Character in Header Name at Ã™K8Â»Â°Ã½Ã¡Ã£Ã?bÂˆrbÂ£[[#6]]Ã¼t1sRÃ?Ã•TyÂœ[[#6]]5Â™Ã¡[[#30]]YÃ„YRm[[#29]]Ã«[[#7]]Â?Â´Â¦CÃ·[[#15]]Ãƒutkgà´Â¢Ã³Ã¹Â°m[[#18]]Â¸M[Â¡Ã°Â¯Â›Â¡Ã?[[#15]]Ã…Â˜_Â?Ã?Ã’=ÃªÂ¹"${[[#20]]Â¬Â-Ãœ kYr)Ã-kxÃ°Â–ÃŒÂ†mÂ?[[#16]]g-IÂŠ[[#16]]Ã¹PÁ´0ÂŽÃ¼Â•&Ã„•Ãž[[#0]]I[[#15]]Â·Ã…Ã½Zk	Block	1
79.177.153.157	Israel	147.237.0.121		Abnormally Long Request method	Block	1
213.8.63.12	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
185.32.179.156	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
37.46.43.141	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
2.54.180.205	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.64.105.129	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.64.105.129 (Unknown SSL Session)	None	1
79.177.153.157	Israel	147.237.0.121		Malformed HTTP Header Line 5	Block	1
79.177.24.102	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
194.90.25.90	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
132.64.90.46	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.178.51.16	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.177.153.157	Israel	147.237.0.121		Illegal Byte Code Character in Header Name Ã•pÃ ?Ã¼Â–Â tÃ€qtÂ‡Â¤Â,Âž<Ã¡Ã†[[#5]]Â²Ã?_Â”Â†[[#14]]Â-Ã©,[[#12]]>ÃªBe[[#7]]Â©[[#8]]Ã™vaZÂ¸CÂ½Â›Â¦Â²Ã¼tÂ?Ã§[[#23]][[#12]]Ã¦Â‰Â”T[[#3]]2q6ÂƒÃŸÃ™[HGÂ’gÃª[[#18]]Â¿\;S<5Ã–ÂŸÂ¢BÂ Ã¡Ã¾+Ã¯sÂ³Ã¶_*CEÂˆÂ?wÂ»[[#20]]ÃˆÃšFÃžEÂ·[[#5]]Â¤7[[#2]]OÃ½[[#3]]Âž Â¥[[#12]]AÃ¯Ã¥Ã?[[#14]]Â¾Ã©S<)Â¶,qÂŽÂ¾Â°kÂ€Ã–Â‡w*lÂ¥ÂŸ[[#5]]BÂŠ[[#26]]P8L$+Âœ Â?WÂ…[[[#31]]Â”Â°XkÃ¤Â¹[[#0]]Â¡Ã?FÂ»[[#11]]Ã–Â£,•>Z$MÃ¯Â”Ã•HÃ?Â¯Ã°Ã£[[#27]]Â?Ã?[[#30]]Ãµ1[[#21]]Ã“PÃ•)[[#26]]Ã˜Ã½[[#1]]nA&Ã¯ÂŠÂ?Â?Â·Â–Ã?Â€[[#8]]Ã¯3Ãµ!Ã-	Block	1
213.8.90.181	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
37.142.131.36	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
5.22.135.112	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
109.64.105.129	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
82.80.153.251	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtNewPass1 in www.miluim-ishi.aka.idf.il/personalsettings	Block	1
79.177.153.157	Israel	147.237.0.121		Malformed URL Â´Â?â€šhiÂ«	Block	1
79.177.43.212	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
212.179.21.194	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected A316F97D0AA0651BE53CCA3F43CCAD2CAFC3641F4FD1C95B430F518F8689A47571F06BF552BFD39F6FD31A0B885FA5EC73E9D9C17454C6671868B3B712C02020A29B5BD0187C47ADEC3E111C5768467B55AC16012594A4CCB29460CF9131DFA5DCC68DCA9C221442C249FC115C6AA6DDD675972561474B0E211728F96B03E6BD, Observed B52347BED7702BAE566BCDD036FD4949A6170CA8F39E07682B4E5CA3749BAC5A3423676D287321EF392769CA053A2806C269F81265B8C94134EA97493BCA6A7411B5B19D457DA8527840E75C92CD2B43763A3840771040967411C9D3B2F0A072E72FD2	None	1
31.168.13.78	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
87.68.77.150	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
2.52.162.232	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.24.179	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.177.153.157	Israel	147.237.0.121		Illegal Byte Code Character in Header Value	Block	1
213.57.93.57	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
192.114.91.234	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
46.19.86.27	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
82.81.66.116	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
2.52.131.242	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1