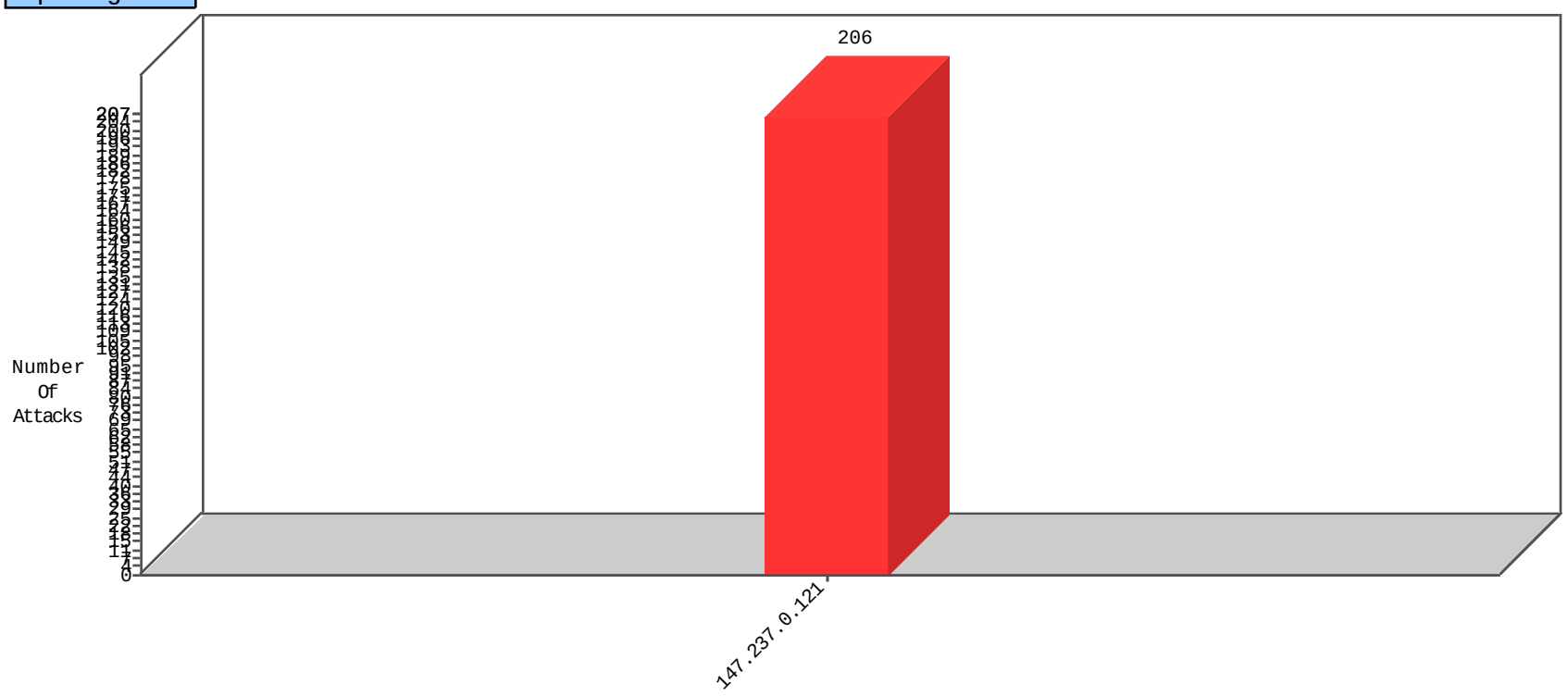
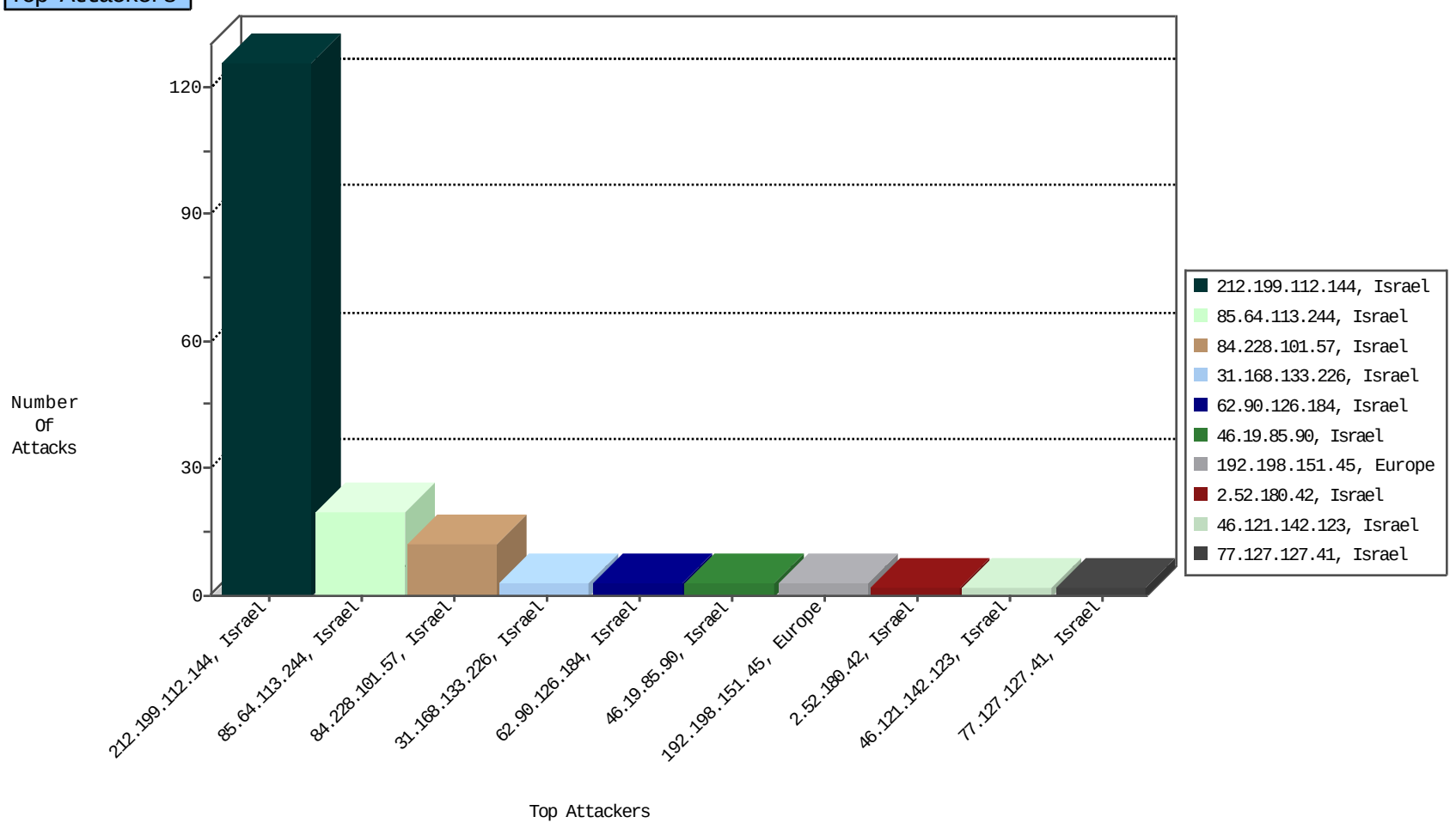
12-20-2015 to 12-21-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-20-2015 to 12-21-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.199.112.144	Israel	147.237.0.121		Anomaly-TLS-renegotiation-Cli	dest-reset	BBL-Israel	126
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

12-20-2015 to 12-21-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-20-2015 to 12-21-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	3
94.102.48.195	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
223.4.174.30	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
192.198.151.43	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
193.105.134.220	Sweden	147.237.0.121		ET SCAN NMAP -sS window 1024	1

12-20-2015 to 12-21-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3720
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3152
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2128
149.88.213.104	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	486
68.180.229.110	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	317
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	284
149.78.229.97	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	264
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	249
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	222
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	197
149.78.41.170	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	180
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	171
149.78.242.197	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
17.78.98.182	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	155
149.88.185.151	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	146
149.78.27.168	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	143
157.55.39.214	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
79.178.170.236	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
79.25.232.148	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.88.231.14	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	102
149.78.148.43	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
192.88.162.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	84
49.224.243.212	New Zealand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	75
68.180.228.168	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
13.21.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
149.78.148.218	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
69.180.5.172	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
66.249.80.33	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.78.242.32	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
207.46.13.138	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
149.88.7.255	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
79.183.114.96	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	43
157.55.39.229	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
17.78.97.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
195.200.205.35	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	29
157.55.39.230	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
149.78.42.40	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.93.234	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
77.126.32.73	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
149.88.226.235	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
66.249.69.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
66.102.9.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
147.235.8.62	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
52.90.122.88	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
147.235.8.62	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.249.69.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
85.64.113.244	Israel	147.237.0.121		Unauthorized HTTP Method	Block	10
85.64.113.244	Israel	147.237.0.121		Multiple Unauthorized URL Access from 85.64.113.244	Block	6
85.64.113.244	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/img/	Block	4
46.19.85.90	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
62.90.126.184	Israel	147.237.0.121		Suspicious Response Code	Block	3
216.75.214.8	Europe	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/s	Block	2
46.121.253.96	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.19.104	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.23.127	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
46.121.142.123	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/medicalcommitteerequest parameter ctl00$ContentPlaceHolder1$txtFilesNames	Block	2
77.127.127.41	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.149.185	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
192.118.36.9	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtTitle	Block	1
84.228.101.57	Israel	147.237.0.121		Illegal HTTP Version Ã‚V+&ÃªGERÃ´Â¶2	Block	1
81.218.55.253	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/changeunit	Block	1
46.121.156.43	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
5.29.6.111	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected D2982C1CBE5D15F0F374B9758E617B56826B82E6B570061A1D6E685CEC97B7A72F78006CC02E7A3710DEAE7E03867DAB8D1B3F7C70623BFB5FE03FD6FBF37F71E89A981FEAC3DF514D9F2BCD573A508C9CF3A78127B39E8E7D7C26AEF5AB77D89EF5D1E3FDB55CD9A38ECC54A7EE7EC53881551615BA7A2ADED95E230FCAD368, Observed 13987C2B91FE3A560CFF4A80DD2DB9D852DC72C5BDC0E2CD7561DB736A36D198ECB1AA74E16E15FC0954610250656463FC42553B5F2415E675BB86067EFE67DCF8585135D887627357FB8D1F63B2EB723B8BF2BD9060955829D20EBFF1777E000A395A	None	1
109.65.123.102	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 574725AD4F742E77B5594A68D9EBAEB68EDB0279A0907DBBD96E48E0CC886B4145326C437837A73B594C76F584DDBC1AB1B3C782EFBA8ABAEED7B32295769E027A89DFA3D022183E8E5FEF8C34F3C57E2A78EDB9183B69B4F0209F2F7FE37C3830E5ECFAAA632F4287D4E98914191A835E31D54EA5937DEF9EC5F5AE6419F456, Observed E32C2D36E8BF2053D222C6CC0E253555FB4A4BC06A827D7E6AE4876BD2A1996E1CA78F4397913E16B804356D7082DF0BD38180C6FE9ADD418CB0C101FE42413A9F945BA25B7313A38C9E9FAAA095FB7FA1E1BD3C468C0958E68742080CA2140130F2A6	None	1
84.228.101.57	Israel	147.237.0.121		NULL Character in Header Name at	Block	1
84.228.101.57	Israel	147.237.0.121		Illegal Byte Code Character in Header Name [[#4]]Â€3Ã¥[v&{BÃ³{Â»Ã?ÂŒ Ã† [[#5]]@>$i@[[#22]]bÂ¯0"`ÂºÃš[[#3]]0Â?_*Â¿Ã®NÂ–Ã«/[[#23]]nÂ¹[[#16]]4Ã¸Ã½Ã• *[[#28]][[#3]]Â¤oÂ›qÃ“[[#18]]5]S3<Ã·Â™Â°Ã³WjoÃ›[[#26]]AÃ?Ã-Â 9[[#2]]Ã?Ã¯Ã“Ã¡hÂ‹ [[#27]]Âº[[#3]]Â'[[#29]]*;ZlÃ©Ã½ÂŠtÂ-v[[#19]]Ãº;[[#12]]Â¿'Â¿L[[#15]]Ã¸ÃŸ Â·j[[#27]][[#7]]Ã Ã?^#ÃƒÂ‰Ã¯#/Ã€B lÃž+YÃŒMÂ‡=FÃ”[[#30]]Ã²Ã¢q`oo> ÂµÃ£[[#25]]Ã«;Â Ã€iÃ¿Ã IÃ™0Â?Â¦Â¬0LÃ‹Â?Ã˜Â¢Â‡Ã»Ã…~Ã¶[[#1]]{ÃŒ Â½[[#30]]Âµ•Â¡OK[[#26]]Ã'[[#3]]Â¿X$[[#18]]Â›Ã°xNÂ…Â€Â–s[[#26]]FÂ´[[#4]]Â·nÃ…BÂ€ $Ã?[[#19]]Â	Block	1
79.176.63.36	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
192.118.36.53	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
2.52.180.42	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.52.180.42 (sigalgs DoS Attack)	None	1
84.228.101.57	Israel	147.237.0.121		Malformed HTTP Header Line 1	Block	1
81.218.56.125	Israel	147.237.0.121		Unknown Parameter zi in www.miluim-ishi.aka.idf.il/login	Block	1
5.29.138.59	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
132.70.66.10	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
84.228.101.57	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.228.101.57	Israel	147.237.0.121		Illegal Byte Code Character in Method Â©ÃªÂ´Ã–d_Ã¥Â¢[[#8]]Â“Ã¡&k[[#31]]Ã¥Ã±wÂ?Â°QÂ˜ÂŽÂ–%:wkÃ,uÃ®Â¡[[#16]]Ã–yÃ^;[[#18]]}l-Ã¦5EÃ£[[#11]]Â«R[[#30]]Ãš[[#30]][[#23]]Â¹ÃƒÃ„-Ã¯	Block	1
79.176.229.7	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
193.169.71.243	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/firstlogin	Block	1
46.19.85.193	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 9436A08A002F71647475E0E48B891FEEF9A039E16C0B42AEAA36201F37A0CF41CD47228AD9E86099141CBF6058F1EC978526C4DBC9DB9957C3FAEADB69834A444FF1B6829E0B86E4F97A642DE0F501F2C1FBF5A1390AFC8B4ECE16E5020A2288DC6A26A00AF06672E7BA908354C13E1D47CB137601DEC92DE5AF9390AC2495FD, Observed 4982D7BB71A31AC32ED4EC31C51925DF2E01ED7C072C128B92990152C2CD5065CC9ED99BFC32EC03520DDE76263D6225AE641F053203B68CE0F3DB13558176FEFC1FD73FBF107EF2D49F3E32404EEB141DDBC68BA653124FC048431A8F2D2BC2868077	None	1
2.52.180.42	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Malformed URL Ö±ÃŠÂ°Öµ2oÖµÖ½×ŸÖ´0_Â?Â§Â¡Ã›×œqÂ±Âž<×¡[[#4]]â„¢Â¸kqrvÖ¶×°:Âœ×?â€¦×´Â¬•	Block	1
84.228.101.57	Israel	147.237.0.121		Abnormally Long Header Line request header name	Block	1
37.26.149.130	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Unknown HTTP Request Method Â©ÃªÂ´Ã–d_Ã¥Â¢[[#8]]Â“Ã¡&k[[#31]]Ã¥Ã±wÂ?Â°QÂ˜ÂŽÂ¬%:wkÃ,uÃ®Â¡[[#16]]Ã–yÃ^;[[#18]]}l-Ã¦5EÃ£[[#11]]Â«R[[#30]]Ãš[[#30]][[#23]]Â¹ÃƒÃ„-Ã¯ in URL Ö±ÃŠÂ°Öµ2oÖµÖ½×ŸÖ´0_Â?Â§Â¡Ã›×œqÂ±Âž<×¡[[#4]]â„¢Â¸kqrvÖ¶×°:Âœ×?â€¦×´Â¬•	Block	1
84.228.101.57	Israel	147.237.0.121		Illegal Byte Code Character in URL Ö±ÃŠÂ°Öµ2oÖµÖ½×ŸÖ´0_Â?Â§Â¡Ã›×œqÂ±Âž<×¡[[#4]]â„¢Â¸kqrvÖ¶×°:Âœ×?â€¦×´Â¬•	Block	1
212.117.136.8	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
2.54.44.89	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed FEC82FF5A58BCE4331F1A2E4A4E4491BAC956995C72AA2DAD665C42703FA9EB3BFBD51B30DFD9ADEB1583A857CBBF3D2F804351307D3701338464DEA46317F654B75613637C2098332A07B710C990650DB9C44B94296BE423D746E84E5FB53D32EB3CAF178B3339362301FD8CA85584618E599B2AD9872EF5253C5DB82D4A29C258E92AD642B10BB52DC247E8CD8D281674EC055AC28FC6B607F0E36EEDEEC8B	None	1
91.231.193.150	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
84.228.101.57	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.228.101.57 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
84.228.101.57	Israel	147.237.0.121		Abnormally Long Request request version	Block	1