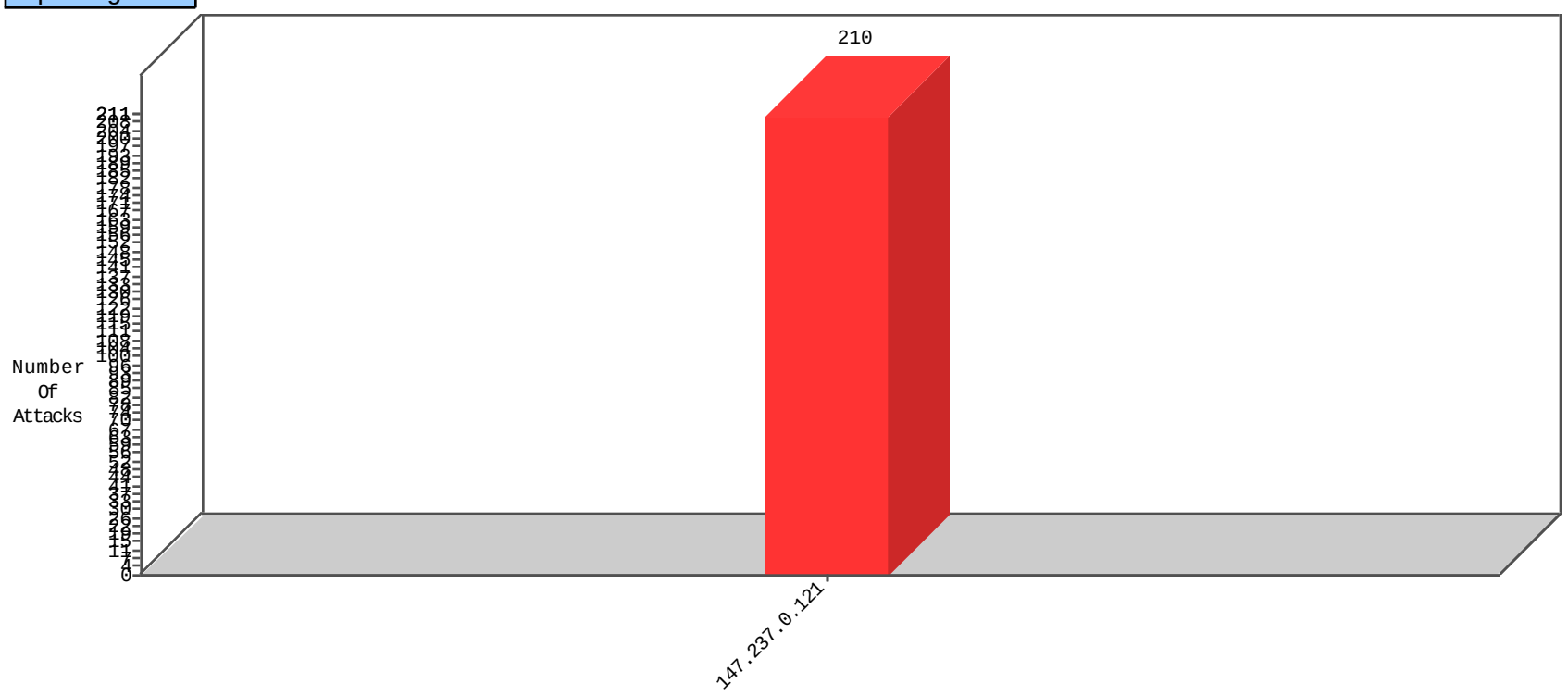
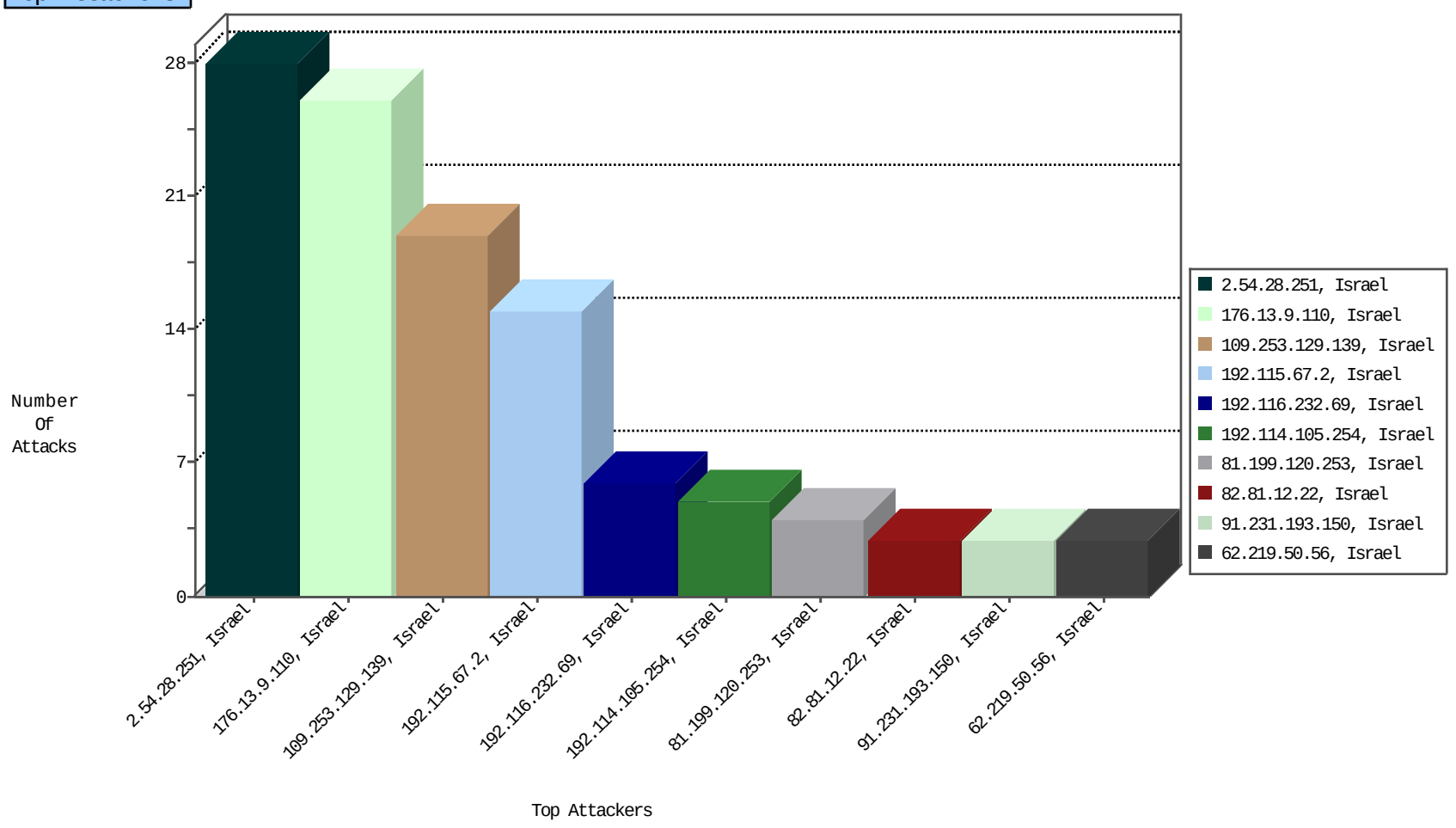
02-14-2016 to 02-15-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-14-2016 to 02-15-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.54.28.251	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	28
176.13.9.110	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	26
109.253.129.139	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	19
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
82.81.12.22	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
212.179.46.189	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

02-14-2016 to 02-15-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

02-14-2016 to 02-15-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.115.67.2	Israel	147.237.0.121		SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	13
115.236.75.201	China	147.237.0.121		ET SCAN Potential SSH Scan	1
94.102.48.193	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1

02-14-2016 to 02-15-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	2766
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1084
17.78.77.125	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	920
177.21.101.83	Brazil	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	772
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	722
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	679
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	534
139.181.48.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	486
194.9.253.237	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	448
149.78.235.249	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	382
46.16.142.100	Cyprus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	363
212.235.103.211	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	343
109.253.151.104	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
149.50.77.229	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	219
149.78.151.84	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	215
213.71.179.110	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	202
192.146.6.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	191
134.222.104.250	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	187
2.54.28.251	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	184
149.78.11.143	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	182
46.19.86.217	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
149.78.79.115	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	180
37.46.38.224	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	176
149.88.196.104	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
15.65.244.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
109.64.163.90	Israel	147.237.0.121		Bad TCP sequence		monitor	152
2.54.28.251	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	144
2.54.28.251	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	144
2.54.28.251	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	144
2.54.28.251	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	144
149.88.9.102	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
17.78.122.117	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	134
149.78.23.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	130
15.65.252.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
165.225.76.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
165.225.72.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	106
81.180.66.34	Moldova, Republic of	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	97
149.78.25.65	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	93
149.78.30.244	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
167.220.196.213	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
176.13.9.110	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
149.50.87.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
149.88.109.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	81
149.78.34.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	81
132.72.213.91	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	80
149.78.84.19	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	77
66.102.7.172	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
138.134.102.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	74
149.88.246.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
79.178.154.98	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	74

02-14-2016 to 02-15-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.116.232.69	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/$$$&?&?$$$	Block	6
62.219.50.56	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	3
81.199.120.253	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	3
109.67.174.53	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/shamapchange	Block	3
46.117.18.218	Israel	147.237.0.121		Suspicious Response Code	Block	3
192.114.105.254	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	3
81.218.68.234	Israel	147.237.0.121		Unauthorized HTTP Method	Block	3
77.127.17.152	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
46.117.25.99	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.68.78.199	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
79.179.137.74	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
109.253.129.90	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.253.129.90 (sigalgs DoS Attack)	None	2
109.67.158.60	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
46.116.11.4	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
5.29.205.159	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
192.114.105.254	Israel	147.237.0.121		Suspicious Response Code	Block	2
79.178.100.139	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
93.172.187.220	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
89.138.86.139	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
192.116.210.2	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
2.54.179.192	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.3.248	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
213.57.156.127	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	2
185.27.106.39	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.213.18	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected D1D34DEE6F12A4C2571508C576B085ADB9DD13792CE653702901B3A15645815963F2284BFA4C376D61F67B51633620D495973CF695D6B33305F76B7D11CDA840CF648F4C9D11A174EEF555DB90D4405ABAC9E89D8C7C114CBE23AF6D89540975486B19F3F0DCE711F32265D98B76ECEC38EE6B0C5D3C00EFE55CDD55E07193E7, Observed 5890D0C079EC1BFEC2F8781072E335B6D5B8F844D36513F40E90CE50ED6909D074119D5168F86AE209BEF2124CC5A858C95E78CAA205599475DF3A7921F9E093876E33CDBE5AFC2C056A010550F811ED8728895D8F8C81B8037D76DFCEFEA4C14B7BD8	None	1
95.86.123.9	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/&sa=u&ved=0ahukewic0ihr_pbkahxpypokhztuatyqfggkmae&usg=afqjcngdz6y3tfrrk_nryfjxifray36-vw	Block	1
91.231.193.150	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.85.102	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.102 (sigalgs DoS Attack)	None	1
193.47.165.251	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
5.28.161.236	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
192.115.67.2	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 192.115.67.2 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
82.80.68.218	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.68.161	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
62.219.44.242	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.116.11.4	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value BF315DE0CCF8836EEFAAAB23EB27CC8A68C8111AF5538A5C4F594310B0931AEBD8214392AFE1B53BFBC99817F6913ED58F6BF39EEF7412EE7BBFF0F911757116202CB5C421E64F684556D7DBD12624521C3EFD26092E5A11BB37C05A15DAA9551557555712D03C67363D76BD9AF9B5639D8F48DD2F0CEBADBCE50EC04C4CB95E3D2DF0B9AE5A563578A44B7D10C66369395318966489F54A944620A4C2AE6828	None	1
91.231.192.149	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
84.108.104.201	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.108.104.201 (sigalgs DoS Attack)	None	1
5.29.154.22	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.118.117.100	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
185.32.179.46	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 47B78372F00A649042D3B0B247C8C2CFCCCC3F97CAED697E60BE659A5B42C6CDC1106AD390FB7800F343B01A31F93BDE8E8AC550A8C3A6D6329C4274839F07A990916CC4FF9F27AC947CAA45534E836B62B8B97E1865884F965230C48370FDA47C0FA0C878C61FD3091DCAB9AA1EA2E9C3FC880F03D772D23177EAE37398FECF, Observed 4A5B73E3BDFEDE8254129FD64B81685AD44E75734DC3AC66ADF16FCAE5C0A987AC9B9D51EDC7AD22E00A5C020F7B08A352A0E6E6B6DFFF90D6C9F96A325D5357303C4A8C090751DCA5FE5137158723B4196DCFEB92EA8617DE2F404A25E9CE04B94DA6	None	1
81.199.120.253	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
79.178.48.212	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
91.231.193.150	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.68.210	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
194.90.239.2	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
87.69.85.67	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.85.102	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.28.165.248	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
192.115.67.2	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
82.81.16.61	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.180.166.247	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
109.253.129.90	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
95.86.68.161	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
91.231.192.149	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
84.108.104.201	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
193.34.57.101	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 193.34.57.101 (sigalgs DoS Attack)	None	1
2.54.9.250	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.234.254	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.85.200	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.150.255.134	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
82.166.148.154	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 82.166.148.154 (Open Mode)	None	1

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
5.28.191.163	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 4A87CE8D02BED39BE9B5BE046C63282EB32D658C46D0029F3853232226E2B1EC977036BCC170254C521F52D7119B07755FA3FC33D742374C2C3F96A0333D3A3F29F520B2D16FDDFC29C420249572A55DE270331698DB921ED26A42BDE157923BF64EC86422553C2F3E16B4A806C50186FA1639888A1D01502E6BFA7E9A99A6D1244C7F15240AAD121FA29B46DE401FF66CA95C2FCA406D8A61B4DBE1F56F6D10	None	1
79.183.145.1	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
147.236.172.2	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
95.86.68.161	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
77.125.141.104	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
91.231.193.150	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 91.231.193.150 (Unknown SSL Session)	None	1
85.64.202.249	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
37.26.147.153	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
193.34.57.101	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.160.134.35	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
93.173.234.153	Israel	147.237.0.121		Double URL Encoding - parameter: ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
62.90.58.17	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
46.19.86.164	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
91.231.192.149	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 91.231.192.149 (Unknown SSL Session)	None	1
82.166.148.154	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
5.29.62.207	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1