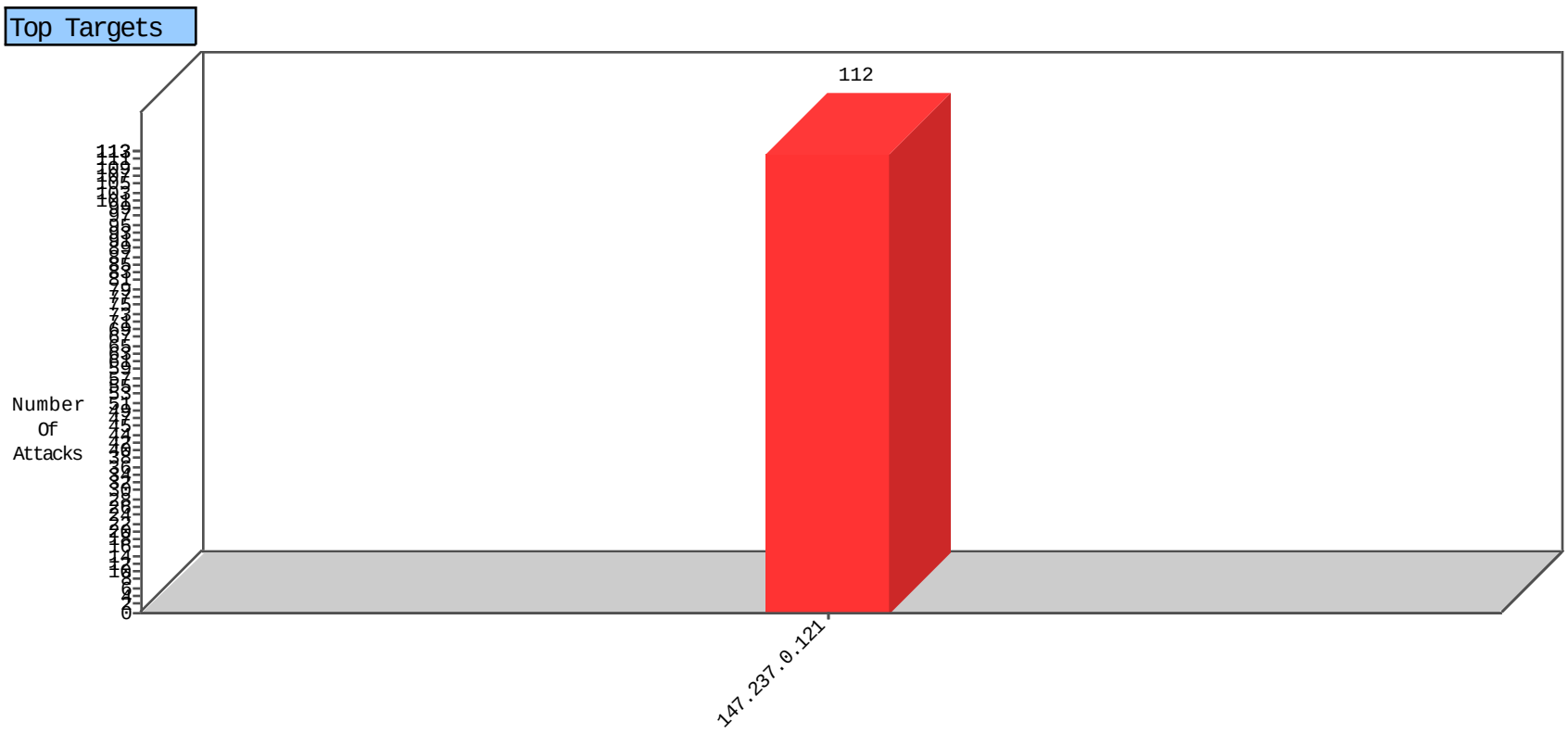
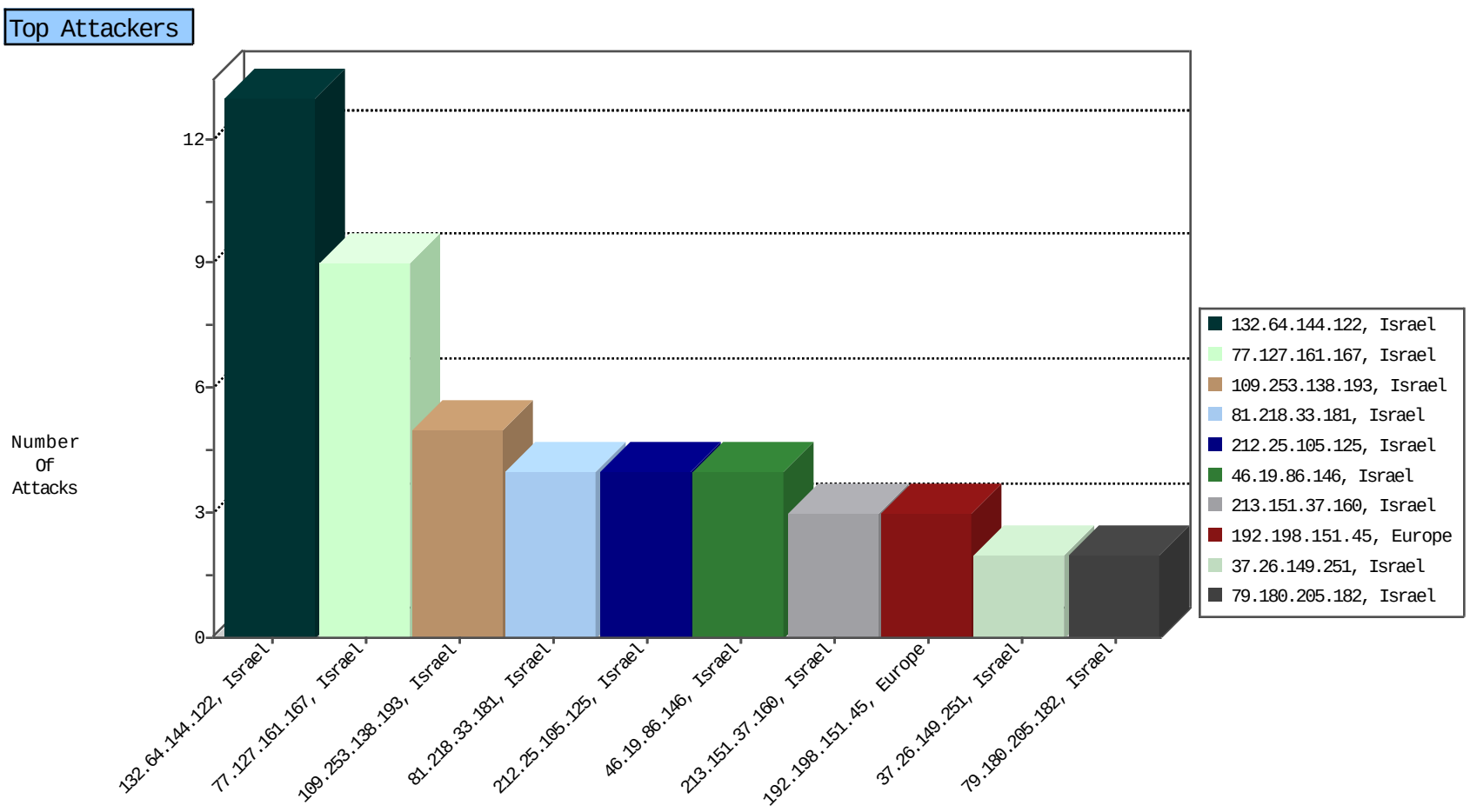
01-13-2016 to 01-14-2016

Focused IP Under Attack Daily Report





01-13-2016 to 01-14-2016

Top Attackers In DDoS-Defence

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

01-13-2016 to 01-14-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-13-2016 to 01-14-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
212.25.105.125	Israel	147.237.0.121		SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
89.248.167.162	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.231		147.237.0.121		ET SCAN Potential SSH Scan	1
5.39.222.253	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
80.82.64.68	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
158.255.6.220	Russian Federation	147.237.0.121		ET SCAN NMAP -sS window 1024	1
31.210.67.78	Turkey	147.237.0.121		ET SCAN Potential SSH Scan	1

01-13-2016 to 01-14-2016

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	2479
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2192
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2019
149.78.25.169	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1469
54.240.197.226	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	589
149.78.227.171	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	569
54.240.197.225	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	556
149.78.234.49	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	325
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	224
54.240.197.227	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	218
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	194
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	190
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	168
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	168
2.54.24.67	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	154
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	143
178.79.177.246	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
149.88.142.117	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	111
149.88.37.76	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
149.78.232.60	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
31.168.14.74	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	72
31.168.14.74	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	72
149.78.50.201	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	72
138.134.102.15	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	65
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
84.228.46.118	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	61
66.102.7.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
54.175.248.228	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
217.69.133.169	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.88.242.243	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
157.55.39.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
46.121.251.150	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
149.88.20.184	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.78.196.124	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
46.19.85.128	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	28
81.218.241.25	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	27
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
37.26.147.194	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
84.109.73.178	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	24
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
77.127.209.153	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	19
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
46.19.85.139	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17

01-13-2016 to 01-14-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
132.64.144.122	Israel	147.237.0.121		Suspicious Response Code	Block	13
77.127.161.167	Israel	147.237.0.121		Suspicious Response Code	Block	9
213.151.37.160	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	3
46.19.86.146	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	3
109.253.138.193	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	3
81.218.33.181	Israel	147.237.0.121		Unauthorized HTTP Method	Block	2
81.218.61.202	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
109.64.101.94	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
81.218.33.181	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/img/	Block	2
2.52.5.91	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
109.253.138.193	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
87.69.52.27	Israel	147.237.0.121		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 87.69.52.27	Block	2
176.13.19.141	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
37.26.149.251	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
84.109.13.116	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.109.13.116 (Open Mode)	None	1
2.54.131.159	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
192.114.91.244	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
79.178.48.55	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.178.48.55 (Unknown SSL Session)	None	1
109.65.54.150	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.26.146.151	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
84.228.17.90	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
212.25.105.125	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.13.10.46	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.180.205.182	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
37.26.148.244	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.13.116	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
2.54.184.143	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
192.198.151.45	Europe	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
79.178.48.55	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
176.13.3.175	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
109.65.165.88	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
46.19.86.146	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
37.26.147.174	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
84.228.46.118	Israel	147.237.0.121		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 84.228.46.118	Block	1
83.130.116.14	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
212.143.64.69	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
176.13.15.59	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
79.182.150.98	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected A09882E1D9E22AC6CABA3B044449F94301CD75BAE256133FF3CA8E1C6190F89C504AF066BACB1402141856C8FD543029A7C7E6049442C2410751A2344738D0DD60547C190E2E4B0F4C291DCF714C042AB132D905BA0C358E4AC22CDA62F23BFB28098C961932416BF15709DB4518B0EA5CD7BA796017FB9D35F6E7CE0D9AC5FA, Observed 45802E92903233CBADF7FA594AF7390DF337AB2A08366D70517A9FD9B3F1B20A53037947843FF9374C5C522CB5CB654844E1AFD400DAA7123BE937ACD520505F6108E710924DDA0007758DFD52A9CB6EE2A1690FFE7E29BAC53F4BBE2F3F011AEA6A8F	None	1
77.127.245.58	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
109.64.163.78	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
37.26.149.155	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
5.29.246.99	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
84.111.160.128	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
81.218.56.171	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
194.114.146.227	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
176.13.4.100	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
79.178.51.16	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
109.67.147.223	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
46.121.193.145	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
37.26.148.195	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 37.26.148.195 (sigalgs DoS Attack)	None	1
83.130.116.14	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
2.52.173.172	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.241.234	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
80.179.141.237	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.178.29.148	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
132.64.27.216	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.65.54.150	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.65.54.150 (sigalgs DoS Attack)	None	1
31.210.188.117	Israel	147.237.0.121		Suspicious Response Code	Block	1
84.228.17.90	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C5398529A59CB6CDCB8DECB0B703BA2608DE9DDD271A827FA0679F3524F7D2FEE44B10EC70A4D570C88895667B23EB0C2BBA03432D98D4E58BE87C6EC41E78EDD50423BE40E364884B6E3C00A3FC9626EDD9FAE40CAB57F704B8755752FA8B158E5D40A690F67D0FE14AA56172EA8ED9233AAA4B51B74A24E4DE47C818044C85, Observed 1D3DE28FA5939B08EF93831CFDBC5404CFA45FA9F3CF8FC411BFD9BC00E7D15959FB116A09CF77169A6D0DD6CEA75321DC86AFE95955A130572937082CD5F339A38DF0315C1C878A410D87189075D1D1157FECFE5DD9F851B586A059937E9A63585DD4	None	1
81.218.56.171	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
212.25.105.125	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.25.105.125 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
176.13.6.78	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.205.182	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1

01-13-2016 to 01-14-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.121.251.150	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 3413A45A2B9237859C6038BE87D21558634BD5155895D8A293B66F1B9DEC5409FE594254DB08D97EC66751F2AF67E2987DC105F5DD961D3471FE4B93A7CAD587E5C58091E144C469FADD4C7F566FFCFA22D504C28241AEA57692CF74D3A1EB004B620C33F0B9A0CEE534B77828296AF0D4B8BF8D146DC0B9BDEA0A043D70916D, Observed 493DFBCE15A4A69EE15EE36F2AC5CA4466F8D0EE71CC21F076FEE2859458718F4C7945452FCC7C8A8E9992D3C0468549CED7325AD6F2246CF05F67048DC8FA956E6E57D6467535F8F29126B830728421F4FFA2DAA7AC8A0A7970741FC0DDDFA794C4C4	None	1
109.253.130.220	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
93.172.163.9	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
37.26.148.195	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1

01-13-2016 to 01-14-2016