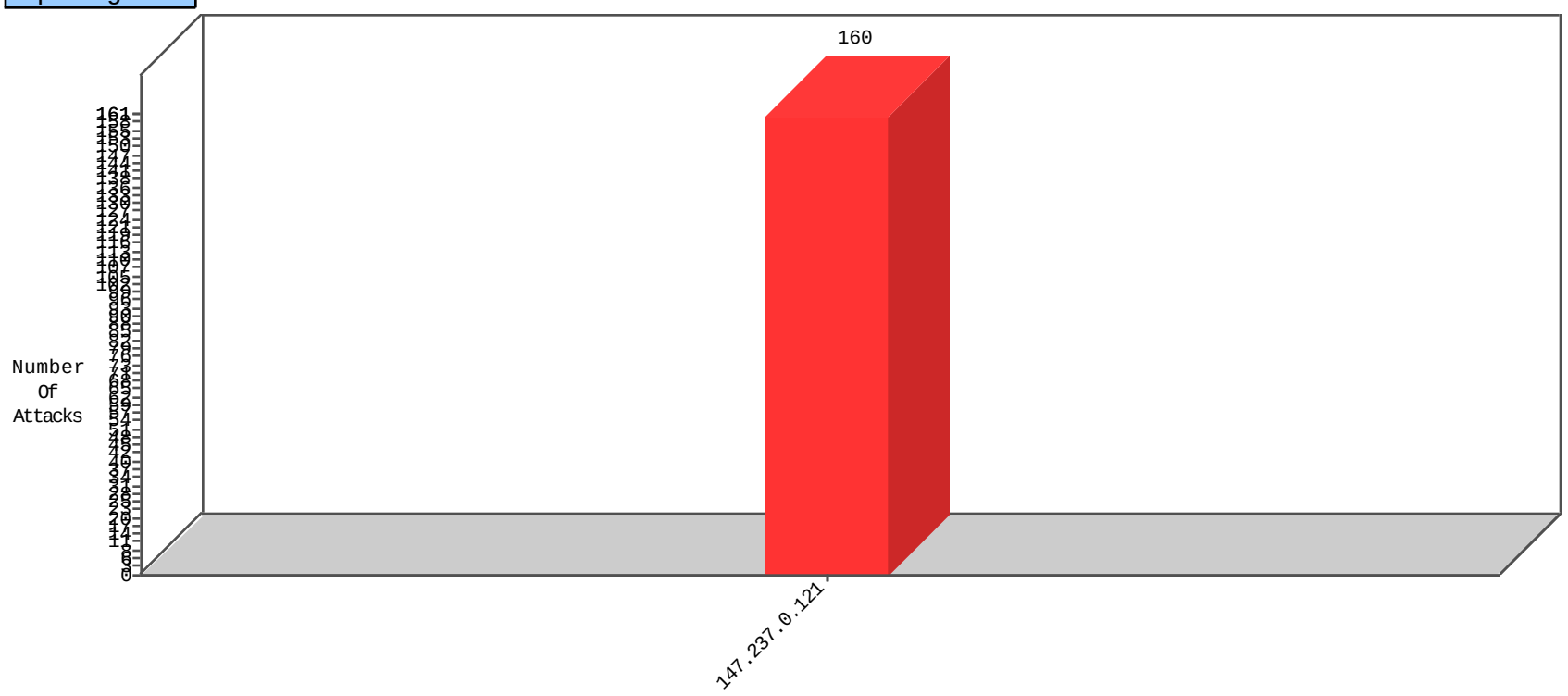
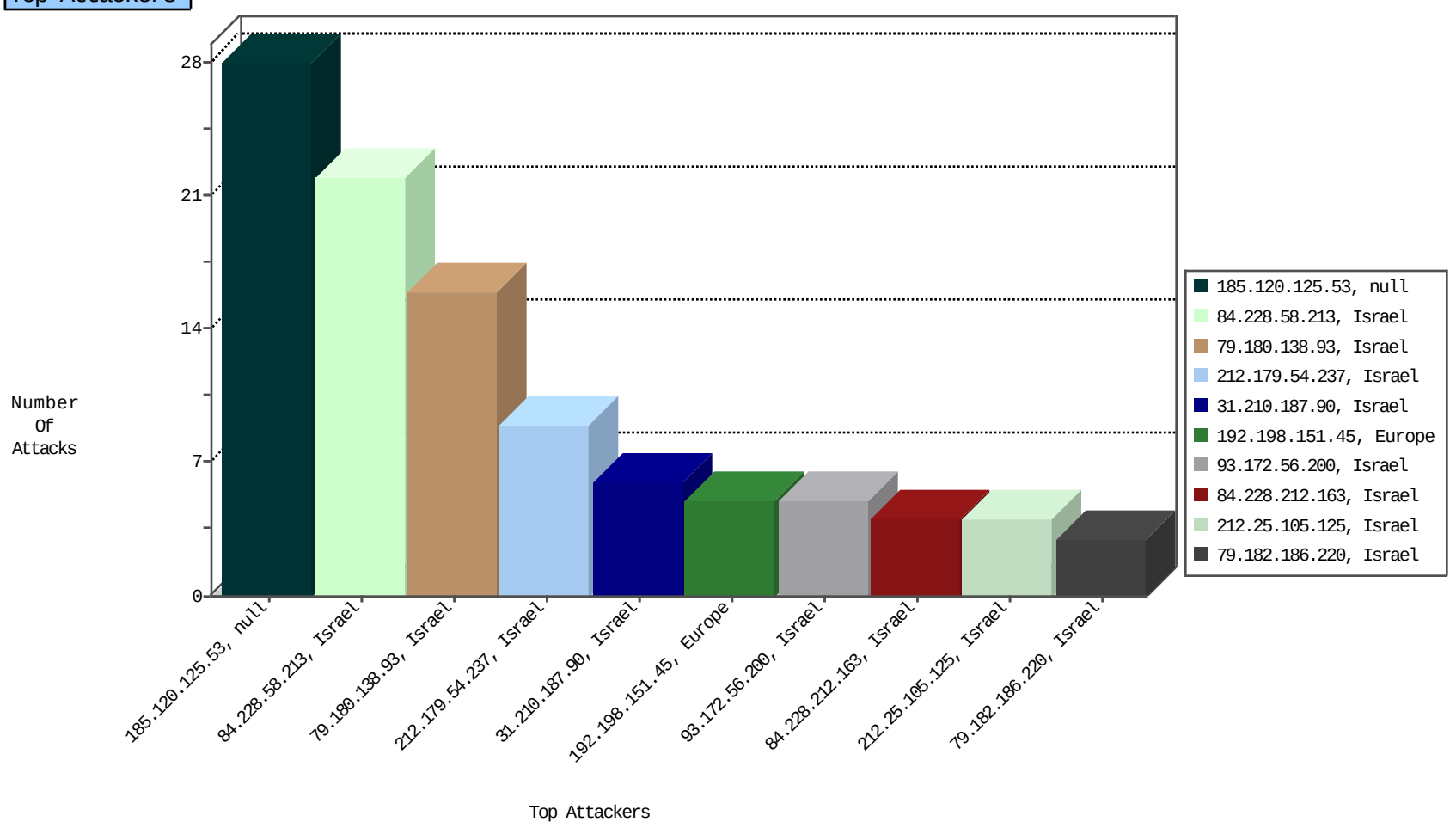
01-20-2016 to 01-21-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-20-2016 to 01-21-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
84.228.58.213	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	22
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	9
79.182.173.196	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
79.182.186.220	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

01-20-2016 to 01-21-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-20-2016 to 01-21-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
216.230.104.182	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
93.158.211.210	Netherlands	147.237.0.121		ET SCAN Potential SSH Scan	1
138.91.190.239	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.0.121		ET SCAN NMAP -sS window 1024	1
212.25.105.125	Israel	147.237.0.121		SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.218.246.103	Russian Federation	147.237.0.121		ET SCAN NMAP -sS window 1024	1
131.109.15.15	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1
185.130.5.234		147.237.0.121		ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.0.121		ET SCAN NMAP -sS window 4096	1

01-20-2016 to 01-21-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.78.187.232	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3487
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1795
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1524
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1383
185.3.147.94	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	738
109.65.20.219	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	486
207.46.13.5	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	454
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	223
149.78.84.19	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	216
149.78.169.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	191
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	191
188.161.82.100	Palestinian Territory, Occupied	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	158
149.78.146.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	146
149.78.252.210	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	143
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	132
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
149.78.62.3	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	93
149.78.36.229	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
149.50.72.92	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	88
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	86
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	85
79.180.138.93	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
2.52.0.34	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
149.50.71.191	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
149.78.42.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
66.249.81.129	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
66.102.6.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
149.78.216.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
79.183.154.179	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
66.102.7.186	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
207.46.13.108	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
82.135.204.89	Lithuania	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
66.102.7.172	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
40.77.167.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
149.88.141.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
2.54.22.14	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
84.228.184.117	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.19.85.179	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
132.64.83.22	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	18
66.249.64.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18

01-20-2016 to 01-21-2016

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	16
31.210.187.90	Israel	147.237.0.121		Unknown Parameter __EVENTTARGET in www.miluim-ishi.aka.idf.il/shamapchange	Block	6
84.228.212.163	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	4
192.198.151.45	Europe	147.237.0.121		Unauthorized HTTP Method	Block	4
109.67.57.159	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.248	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.109	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
194.114.146.227	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
79.180.25.24	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
212.179.129.6	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
185.120.126.16		147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 7CC1ED7F8B005F654CD3141C93A3459E0EE5B2DDCEBDD5C63DC2249650654C4A60B9590EA4FB9AF4D233FEF97D7DABF04857A6D6D9110D6DA3EF4C2F4ACE0717976587C215F204D59F215D4F5DB3E273F19EDB87F86B8C0424E5A81B5785A10C224AC237AE2519E5D2DC982BA4E60DD19AF29E2F4121EA61C00C6435A0D08359, Observed 21919397D1957B3132979320355DB907C345C6DA0A36C864D0941AF0C7DE7347A96F9393D8CAA5B5DD968D611719191C148B7C32DC5662EFC0E634B45CC9C329B11F6A3BA5A0CF256FFEA73ACF25DE4FC985FC533E51D539108D84C8C38449F9FACDE5	None	1
46.19.86.27	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
5.255.253.47	Russian Federation	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.56.200	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
213.57.139.12	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
82.166.136.4	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	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
185.32.179.178	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.109	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.109 (sigalgs DoS Attack)	None	1
2.52.158.166	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
94.230.86.211	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
85.65.182.125	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 85.65.182.125 (Open Mode)	None	1
80.246.136.148	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
212.199.57.66	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.19.86.52	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.255.253.96	Russian Federation	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.156.84	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
93.172.56.200	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
83.130.106.49	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.121.99.252	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		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
185.120.125.51		147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
5.29.137.239	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
109.64.14.197	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 23D064C685C1862E7F652BE14A0DFBB33A6DD3860C42B4F86610617E6D996FD53C4EA2CB8107C237D896362381B30891F8B8E61FD05F1D52AE4F2E114F8D1842E15A64024F486954935D5C4A407B9E346C03F9F7B52C204AB3009CCFD5AD0982C9EECDEA620A8A73FAF1CFB65EFECF85FFA22F2BACDB0CA29E7BA56CFD05BE4C, Observed 9A183B2A64F2D56B271A38D63B863D5316441C5E940B6AC9BEEDE670928DAD907BDA3255540E2BEBB1CDE8E31E9C05F09FC69A1E95288ECD28DCA3C4BEF81668A1C39F06FF9EC9C1CC4C0B6056D79C5A60043E2AB5794F12FB109C28605C214C0CCB88	None	1
85.65.182.125	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
213.8.174.4	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
81.218.66.250	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
192.198.151.45	Europe	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/s	Block	1
46.19.86.75	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
132.70.66.9	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
93.172.56.200	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
84.108.249.65	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C98FD15745F639A024D7B11A9C34198754E51ECCBDF141659C7140D49ACA816EFF22F89896E9989250EB1130D86B683A05BC2F6DE736F41F8007FBE8C6217B113D84C63983913013D221A0C13EA75E8589B7D128ABC6B45358E0A1481574B54A42C76CC7DD07B9B9182397B7C7D6AA98FFB16123E8CA8B949D03DB08C243AB17, Observed 2C23ABAB9135DD1BB1F304EF808C16E3F615062C080DACEF4EC271A7B0133FFB871650107C6CC7A0A5919FC0E8BA3CAC0E301114F931AF942DE1DF76CD9B21ADE7C470223C0E54F9F4CE09F3302D7E46FD02074637B40F7FD9C2FDB7E7F63AB73D7C40	None	1
62.90.99.64	Israel	147.237.0.121		Suspicious Response Code	Block	1
212.25.105.125	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.137	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.29.248.182	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
109.65.147.223	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
93.172.56.200	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 52C631450B0E2B10613EB7C55F76E59F78B85665ADD2100768255C681D993156739FBE3EAC196EF14DC8503FCB882AB6E13D08E7941484B04BB40B15D02C23A551FA7F2BF097EBD8AD3B8290E3AD58AC05062F4B38E7B27E879D57C853CB1D16417EF8C895D5B919BE69A432817B232E7D5354A02C0F1102146DE951F9552E90, Observed 26000173AD2073B8A13D449D9889AB297447564482ADE28D786F96B1E38D4661D030B64EEFDA1A687F3D89DE7BEA8B038B8F1431C4AEB8359C7760D8ACB36204ED4796A3C57CE85A0783B1963F91281DD44F8306482C63B08867C948A22F5B013DB9B0	None	1
213.57.83.30	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1

01-20-2016 to 01-21-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.97.45	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected E0F1E016741CA72BC455DF10B8EC7E31DA14AFE95868C2DBBE1D8E7D469CD5DCF22583239A65638069FDB16B85F8C1BFAA337A8D1A3EAAB8395C22531ADFF726B647C384D7084B14C327B280CC01CEB74F4AE8F0A55F5E58D2C6870DE88D1B63F7748136DDF5DCFBFF84E85CB3BA710469ADDA13340788579EB34F5E1FCF6593, Observed 6CDCE153D7C05D9588C4F57FA37F1674A07E5317C0ADDEDAF755D2189D442D68467BD4602F4C09B2998F07CAD284C2C8BDB87465FAB6EAA8EC07B7F7A7A4A5916B5A0D6B07260AE8D3912FB81AEC5B98D0DDF73F985810FBDA6F14C9D575EE4682B283	None	1
46.19.86.122	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
185.24.207.16	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
37.26.149.136	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
93.172.56.200	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1

01-20-2016 to 01-21-2016