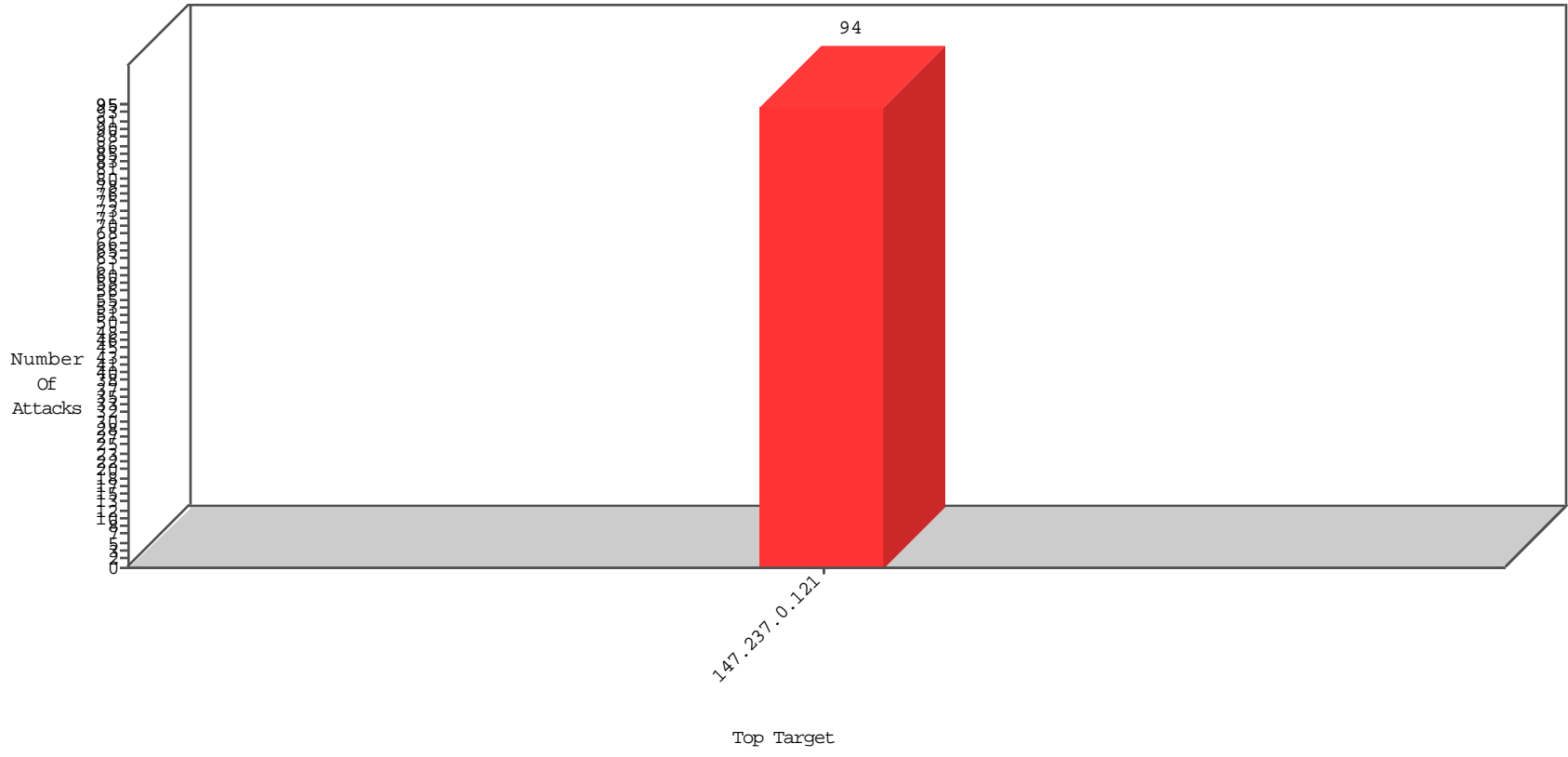


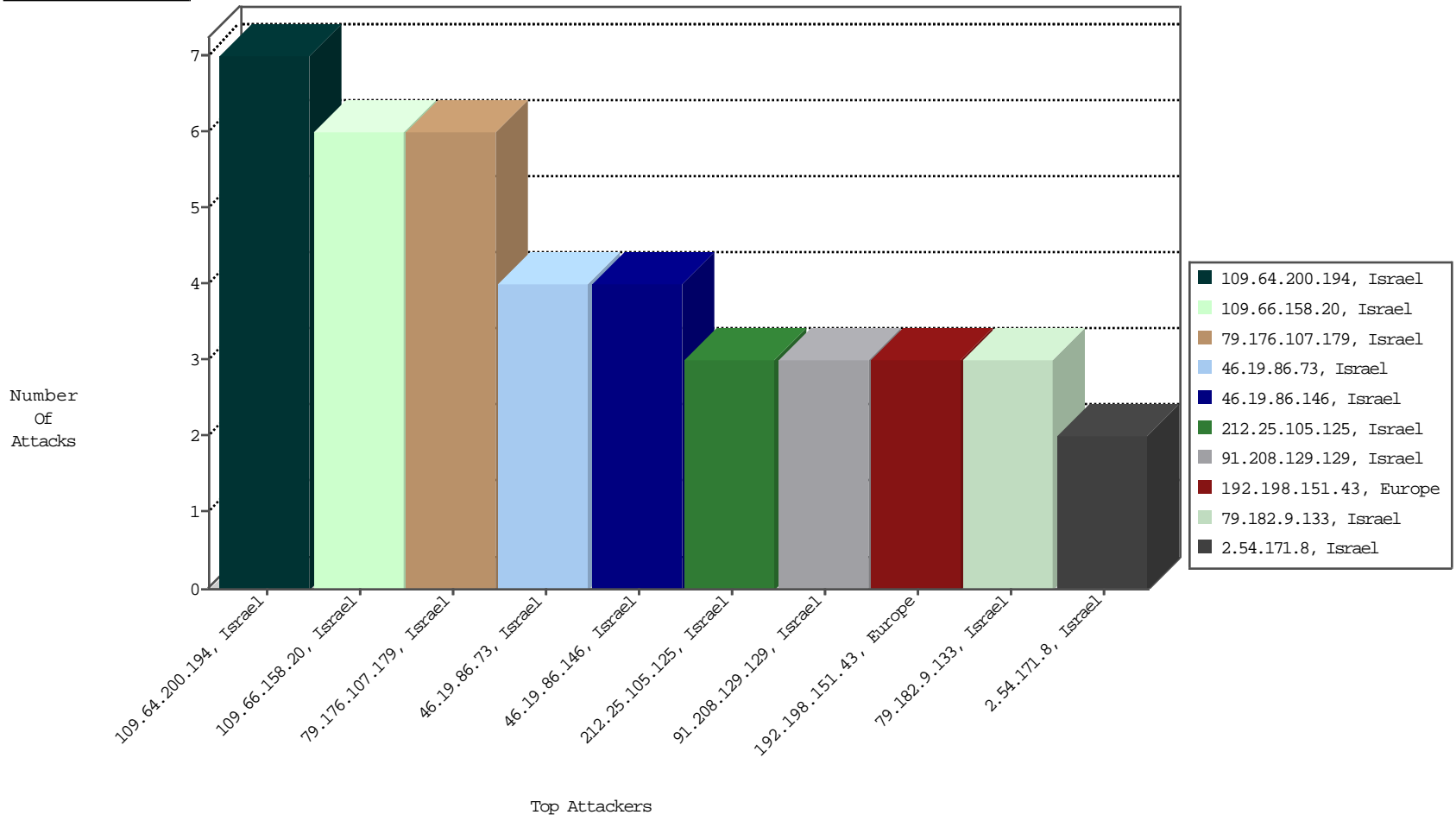
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.176.107.179	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	6
109.66.158.20	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	6
91.208.129.129	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	3
192.118.132.185	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	2

01-14-2016 to 01-15-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.177.25.253	Israel	147.237.0.121		13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.43	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
31.210.67.78	Turkey	147.237.0.121		ET SCAN Potential SSH Scan	1
80.82.64.68	Netherlands	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
223.4.174.30	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
79.122.226.6	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1
222.174.5.27	China	147.237.0.121		ET SCAN Potential SSH Scan	1

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	2323
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2235
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1801
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	530
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	248
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	236
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	216
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	204
182.48.248.66	India	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	199
149.78.169.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	199
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	192
81.180.66.34	Moldova, Republic of	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	171
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	140
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	135
212.25.107.145	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	100
207.232.46.170	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	80
66.249.83.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
207.46.13.10	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	75
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
2.54.148.4	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	54
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
149.88.109.80	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
31.168.14.74	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
212.25.107.145	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
31.168.14.74	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
149.78.84.69	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
212.25.107.145	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	26
66.249.69.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
207.232.46.170	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
157.55.39.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.169	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
116.109.224.120	Vietnam	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
185.3.144.113	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	23
66.102.7.172	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
62.219.34.173	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	21
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
37.46.39.140	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	19
66.249.81.129	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.249.75.29	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.75.47	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
79.183.113.243	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
66.249.75.38	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
212.235.98.139	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
66.102.7.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
79.176.5.107	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	14

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.64.200.194	Israel	147.237.0.121		Suspicious Response Code	Block	7
46.19.86.146	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	4
2.54.171.8	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	2
79.182.9.133	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	2
46.19.86.73	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	2
46.19.86.245	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	2
95.86.115.95	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	2
46.19.86.73	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.80.23.86	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in www.miluum-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
213.8.241.234	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
62.219.134.154	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
46.19.85.127	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
192.198.151.43	Europe	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluum-ishi.aka.idf.il/changepassword/newpassword	Block	1
109.253.129.242	Israel	147.237.0.121		Parameter Type Violation virt in miluum-ishi.aka.idf.il/cellularreference	Block	1
82.102.169.113	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.179.62.20	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100\$txtNewPass1 in www.miluum-ishi.aka.idf.il/personalsettings	Block	1
176.13.6.78	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.26.148.155	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
2.52.45.124	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
93.172.191.94	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNimuk in www.miluum-ishi.aka.idf.il/valtanrequest	Block	1
82.80.144.149	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 82.80.144.149 (sigalgs DoS Attack)	None	1
213.57.239.240	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
79.178.51.16	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	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
109.253.219.143	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
2.54.254.131	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	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
80.178.203.103	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected DF5AA8AF47DDA2DDA9DF515793D220DEC4D77618165CCF9B12CD92CBD8E7534FCB198C9540E5B00B10408BD1AE535F1F91A41428E6751568765DAE3E818C51864D6D27A62789FC2869D420B930C5F0FF5B1DCA4D2C08DCF4EFD5ED0A00D6FAC4743EA22BB461D512744E1E7B1F249C76CF194F329C818948A7E7C5A46AD2E, Observed A1E8ACAF9DD4277AE2A422673AF699E271C88F580D460DF212245E3FDB806E585D9C1BA7F80FE0DB964F9EF113D4ECABC572DA903F6C085034DF6DD3C65C2B89A4C24EFA64FF594C5E2F1497653AA33AD102D914D5A39F62AE8D97133F6510A2C786C9	None	1
212.179.129.6	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
37.26.149.146	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
176.13.6.78	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.49.8	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
82.80.144.149	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
217.132.136.223	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
79.181.175.145	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected FE728FF0BC516CAECF326F8C2B923389B2BECCFBB6E94627AFD40A1CE771A61E23CEA9859A30EE98FEA8F41E9138D01A4702FDDFE41621CB964B4AC31542AA8E48A2B45B93A844D7DADE9D05B3F41BAB1B91E65FC7C3E542FCEB33C01EDD585B2FBE95F43239DFF79B6E2602F25DDB480D95DADE68EBE9FFBEB09E2A353B1C, Observed 0BA519868388B41CC95583C87998CC90E4984CEA7D0011494BF584376B263D1DA9585464F28233F0A53170E40C3CA081BC22CFCE9174016577F42233FA547078247EAA4CB3D1FDA097C4C2B6B79FF992D4D552806C76850F3047EE00C9F5403821380B	None	1
212.25.105.125	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
132.73.206.11	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
5.28.137.148	Israel	147.237.0.121		Parameter Type Violation virt in www.miluum-ishi.aka.idf.il/cellularreference	Block	1
84.228.108.71	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
80.246.137.195	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.199.123.251	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
46.117.141.221	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
37.26.149.218	Israel	147.237.0.121		Parameter Type Violation virt in miluum-ishi.aka.idf.il/cellularreference	Block	1
176.13.11.134	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
2.54.148.4	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
82.81.47.19	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/changepassword/newpassword parameter ct100\$ContentPlaceHolder1\$txtNewPass1	Block	1
217.194.198.125	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected DCE4ECEB8DE042D16587FB6534A2ABC538C63EC4F90F4B459DCE8DF82D7BE0405C97A4958B467FF97C909582A19C437EDB56559682F8E02D9E34EE4B4746AA5815CFFA99F5C093B426D57ECB9A9688A37BF3E1C230A4C78118E1661E5332DC35F34CB9A85DBC823314B4242F29689AD4CBD848581A0C98A491F4E7D67FE4511, Observed 34595AE16CCE2BA725F97B9F0D138546E8AC0D54B36E1A8AFA13FB8B06F8001BAC2245B132E4F6C8BC45C5A42236DC9E768CF6944C31B104868AD9DD90FA8F8B2BC1F10AB1FC5D8E8B14CA0EE1AB40EECB592B187B1711D831F786C11EF422C8DA21CA	None	1
79.182.9.133	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
46.19.86.104	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
212.143.56.92	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	1
176.13.5.113	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/cellularreference parameter virt	Block	1
31.154.10.42	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100\$txtNewPass1 in www.miluum-ishi.aka.idf.il/personalsettings	Block	1
93.157.82.130	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 88641ABAFDB52350389ED4D377306A1A00AD805D88EC01A31E914F16F172F9DF6C7236837892A5872C1A04E1DA8A9E45841399BBD2F93CE4FACC34715FA2290FCC7DD3830A5275F2AA6998BC2CEFC0A0A83E82E00EA4C344574203FBBCD5AB799F9BC27BAAF6FDC44F8841A33939DE96E942678AB1F14236D87FFC13142549B38, Observed E3591E630E71246404A394CEC7726473CAE0507F811093323D09E234BC469CCA42951E988A9BF2B8FA43BEF3D739ACF0A5D05368C194E9F71B44B64F37893D895116D9AE2532AA567646E2670A89602D08B5B3D5F2ABCC616DF357EF974EC1705E8A91	None	1