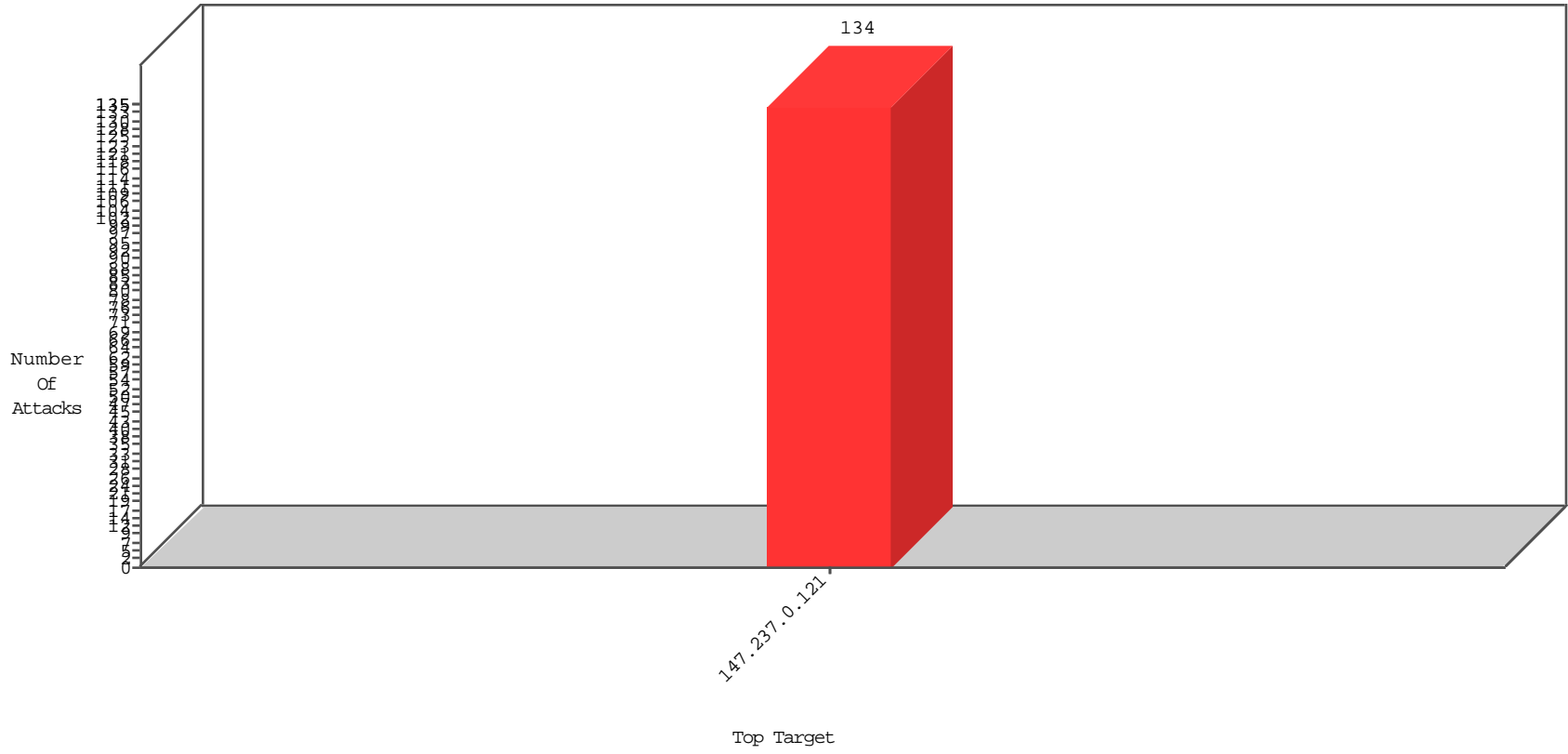


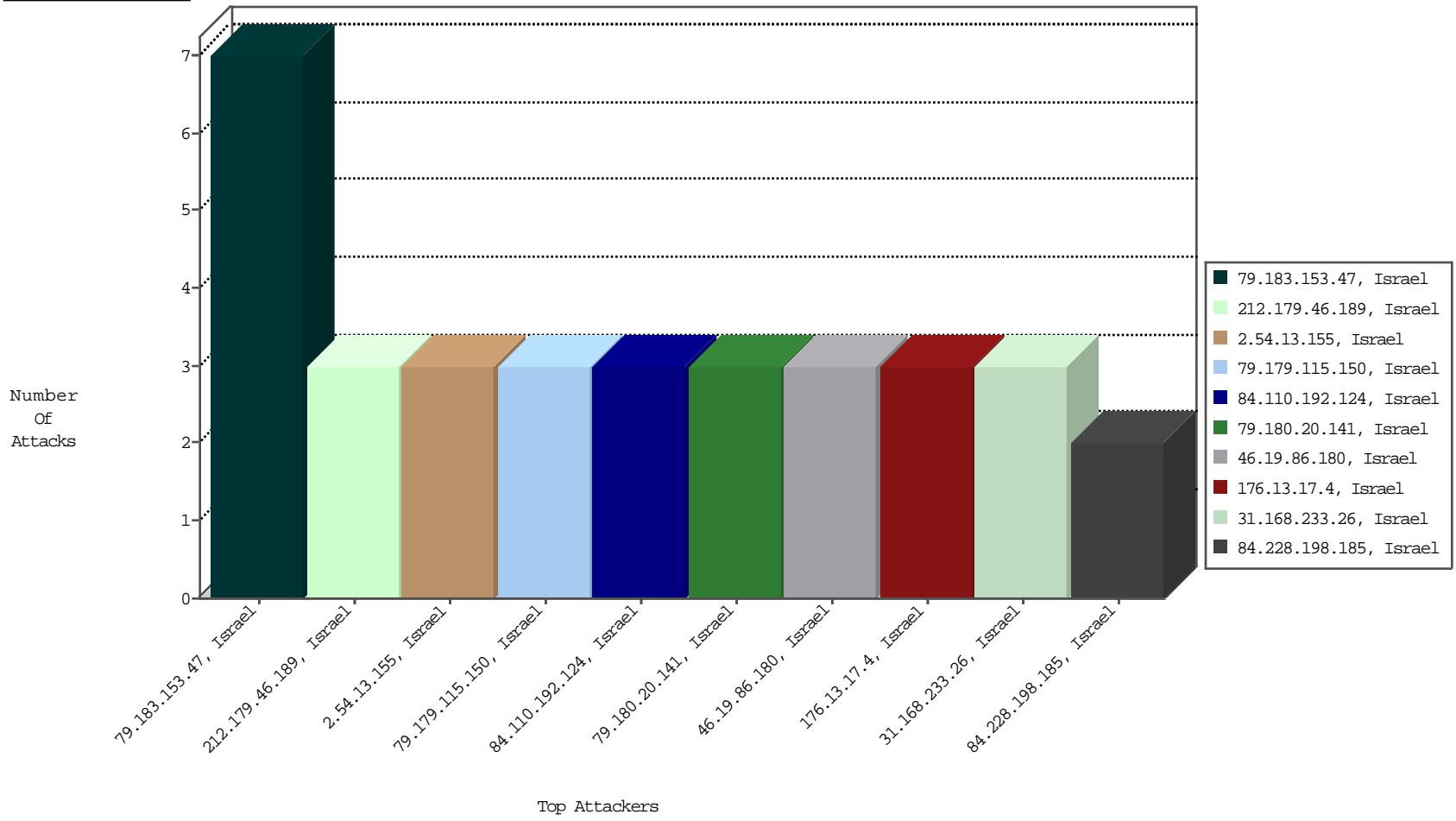
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.183.153.47	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	7
79.180.20.141	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

02-19-2016 to 02-20-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
91.201.236.114	Ukraine	147.237.0.121		ET SCAN NMAP -sS window 1024	1
103.53.84.13		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
146.185.250.105	Russian Federation	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
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	781
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	747
23.27.45.132	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	736
149.78.242.196	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	614
149.78.247.2	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	432
149.88.149.97	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	423
149.78.230.177	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	422
149.78.176.227	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	417
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	331
149.78.165.30	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	261
149.88.141.237	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	240
149.88.120.11	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	204
79.183.153.47	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	171
79.176.235.97	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.86.236	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	109
149.88.5.45	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	105
149.88.201.246	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98
206.74.121.194	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	95
149.78.234.243	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	94
149.50.77.229	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	86
149.88.240.76	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
149.88.20.45	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	82
149.78.79.236	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
66.102.9.107	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
112.198.101.188	Philippines	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
80.246.136.186	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
66.43.120.42	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
125.7.53.205	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.78.231.117	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
217.69.133.249	Russian Federation	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	43
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
149.88.73.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.78.103.243	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
149.88.246.99	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
37.26.149.170	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
199.203.159.137	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
176.13.8.149	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
64.233.173.212	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
149.88.104.17	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
110.77.230.188	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
54.197.117.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
5.29.252.207	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	22
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
212.214.229.27	Sweden	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
149.88.241.98	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
31.210.187.100	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	18

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.19.86.180	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
84.110.192.124	Israel	147.237.0.121		Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	3
176.13.17.4	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
31.168.233.26	Israel	147.237.0.121		Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtEName in www.miluum-ishi.aka.idf.il/valtanrequest	Block	3
2.54.12.176	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
95.35.79.168	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
77.127.219.200	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
185.120.125.13		147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
2.54.13.59	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.67.252.247	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
212.150.254.182	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
185.3.144.121	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.176.49.162	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
2.52.40.165	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.66.6.12	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
46.19.86.50	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.253.145.46	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
62.128.48.50	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
84.228.198.185	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.179.115.150	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
5.22.129.228	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
2.54.8.116	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
94.159.148.194	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
46.19.86.62	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
84.108.69.180	Israel	147.237.0.121		Suspicious Response Code	Block	2
2.54.13.155	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
87.70.7.26	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
80.246.136.253	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
5.22.134.230	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.67.249.162	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.176.129.14	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.142.68.88	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
80.178.201.104	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.102.206.129	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
188.120.134.6	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
2.54.49.23	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.178.108.117	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
2.52.40.138	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.65.148.207	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 52E626FF384BA45DCAE0F5A9A46120EF14561EB8194EF93CA843D49E9B9525ACAF1D9D9BC 9059A8AF1577ED4786CB9557D19F7F0A1C078CEA772FA8EDEBA36942CB065174012148D0 52ACE08332132223A3CDC40EEA4879017385693AF485E7DD206E682E059ED6234E8C9EBC 4406E85AF6F065F74C0E9EDA52B78347C55C3E7E67E43A8839D8EA673D9725EB22DCE9D08 313F50E3C522CB67961208C10D221	None	1
87.70.7.217	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.86.1	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.26.146.195	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.246.137.222	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.180.14.91	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.28.171.204	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.176.234.51	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.86.222	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
2.52.7.234	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
95.86.93.1	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 05C65A60B62A25E2EF3C70E9D60F5535EC4C7D1DD1DBA531D8BA86C6619C6150CCC736F 7670876C14DF4BDFD0396282F714BACA606210230BD9D042812B27F22B5BF0CD9E49FB4B3 DC1769A0D68813567BFB6843FD1FA3CD5BE71A346E2D4D638ADAB3E290D493C56CC7752 1DBBAF66AA984186CEE046BD5E2BEED64FA0254B1, Observed F1D6B3BAE3A522E4594BBB24C75F64F6A1EF1FE81E856F0FDA97A3177355DF26E1B57E1167E DEF6518C3EE15CBA113003B4D66EFE2B6C11A55E2BDCE58E0231BCCF69E09EAECABC2A76D D62A9A42CEFA30F08474C376F51EC303A2890209F5EFBD6070	None	1
84.228.132.94	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.4	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.4 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
80.246.136.186	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.255.253.97	Russian Federation	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
2.54.135.88	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.179.115.150	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
87.71.22.65	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.26.147.190	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
81.218.146.181	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.178.134.248	Israel	147.237.0.121		SSL Untraceable Connection - Heartbleed Attack	None	1
5.29.59.111	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
185.120.126.8		147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
2.54.13.155	Israel	147.237.0.121		Parameter Type Violation ctl00\$ContentPlaceHolder1\$ctl00 in www.miluum-ishi.aka.idf.il/form3010	Block	1
79.178.36.14	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
2.52.34.163	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed DECE8648BDF88E5C092461DF862272D3A1904255F6C12114BD2D424D486883389F768FFCF D6DBAD2C60DD28D87D38A6B85B3A25627FDB0845D051F03C158CFAA598E06A2033D5BCF 0697495AC8E8D6007ED7EB2D058AEE367F2C02436223375425B64FEA77A4F87BF995D1B836 69376C518A3C147640B0868079363ECC483A58C4D11176360148C5B7BA63255FB5F8151F 0146BC577631982D418D9F57B87D6E	None	1
95.86.93.1	Israel	147.237.0.121		Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
46.19.85.4	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
31.154.5.242	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
213.8.204.25	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
80.246.136.229	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.3.147.50	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.67.186.161	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1

02-19-2016 to 02-20-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.176.96.152	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.26.147.215	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.178.134.248	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.102.200.114	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.120.126.8		147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
176.13.8.149	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.178.108.117	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.178.108.117 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
62.219.135.250	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
2.52.34.163	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
109.64.26.80	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.80	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.179.137.74	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
185.3.147.125	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1

02-19-2016 to 02-20-2016