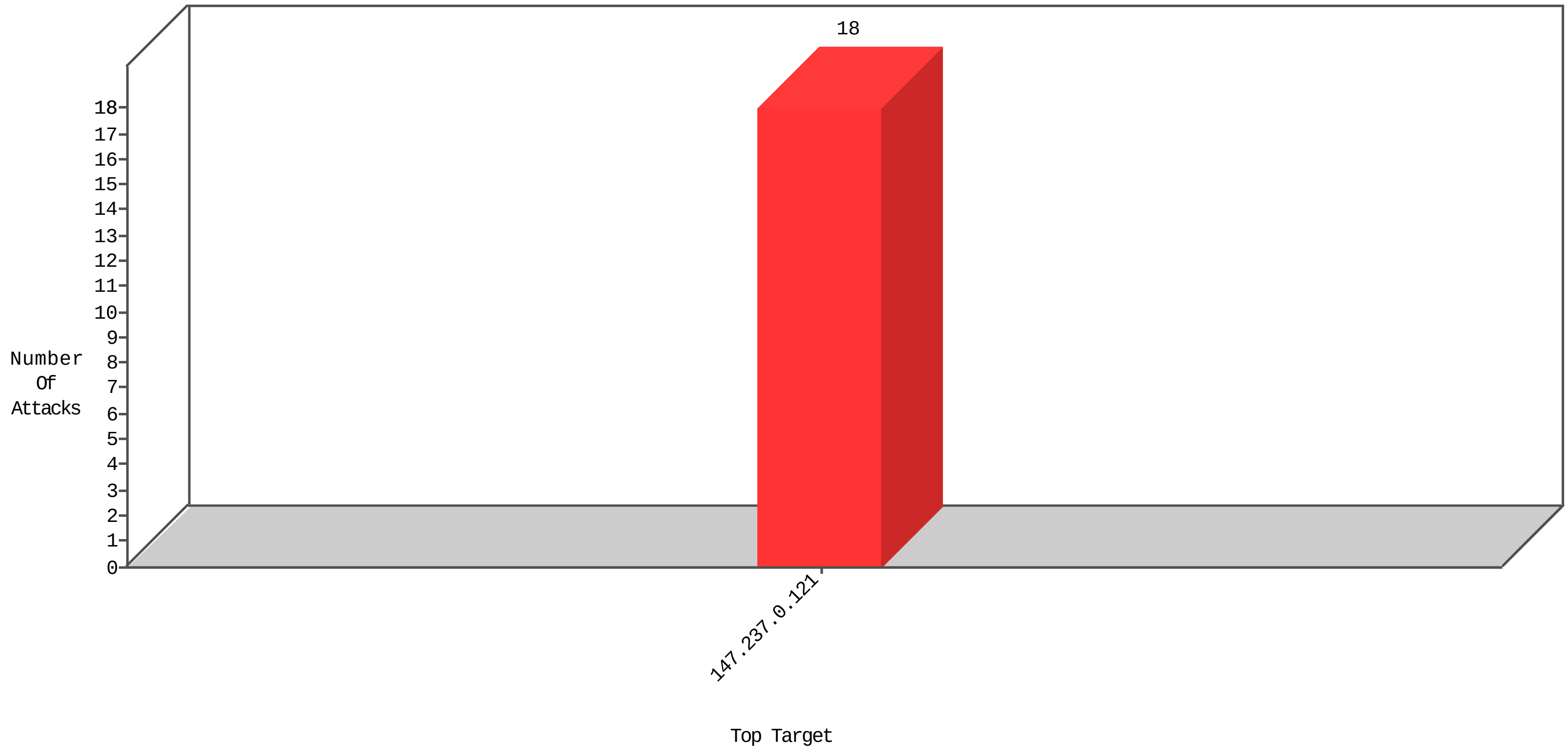
11-28-2015 to 11-29-2015

ממשל זמין gov www.gov.il

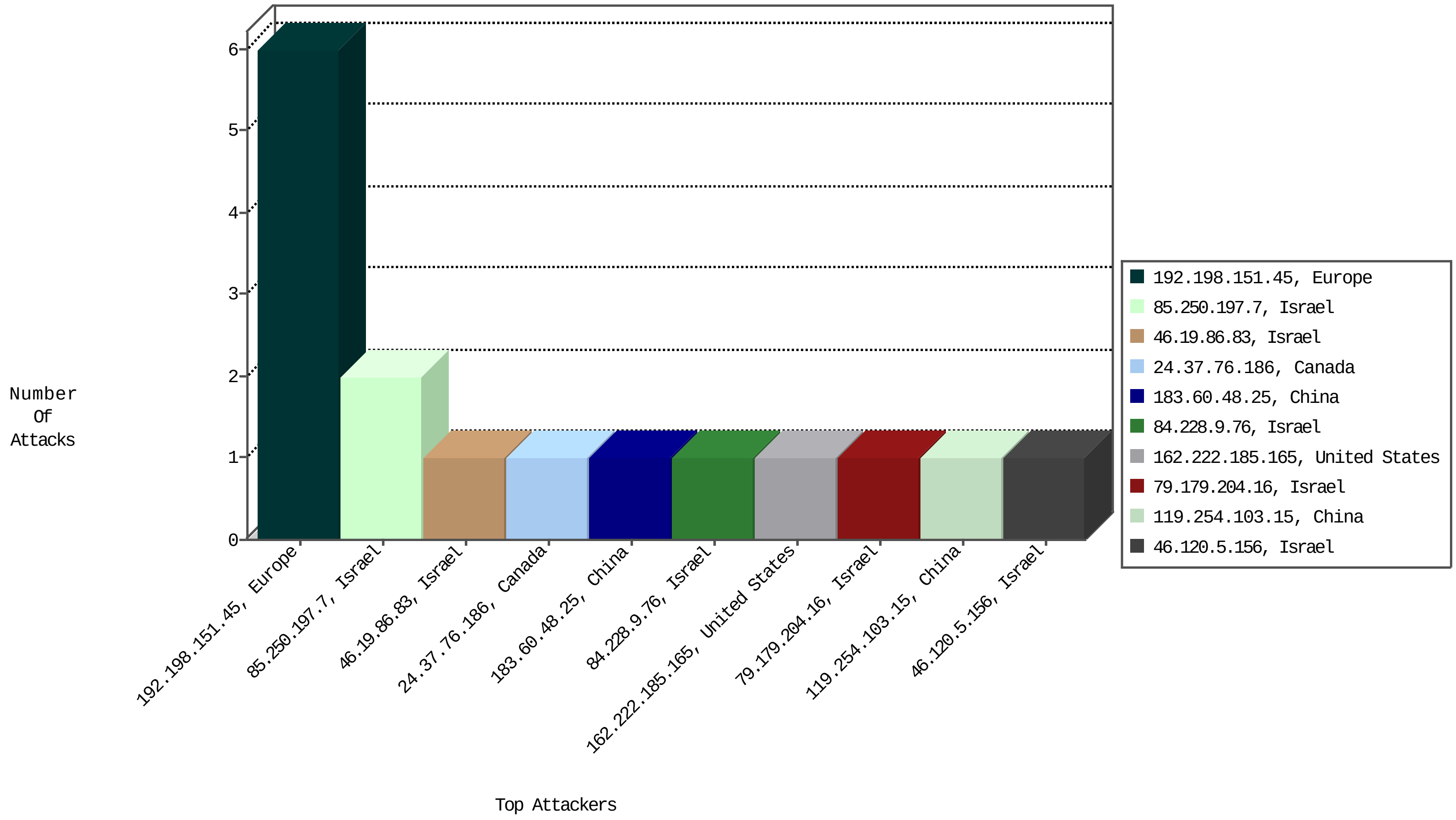
Focused IP Under Attack Daily Report

govsec

Top Targets



Top Attackers



11-28-2015 to 11-29-2015

Top Attackers In DDoS-Defence

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

11-28-2015 to 11-29-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-28-2015 to 11-29-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	6
183.60.48.25	China	147.237.0.121		ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
95.54.216.245	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1
162.222.185.165	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
24.37.76.186	Canada	147.237.0.121		ET SCAN NMAP -sS window 3072	1
119.254.103.15	China	147.237.0.121		ET SCAN Potential SSH Scan	1

11-28-2015 to 11-29-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1867
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1863
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1495
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	228
149.88.13.170	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	216
68.132.202.91	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	202
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	185
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	170
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	168
2.52.54.149	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	111
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
80.246.137.132	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
208.87.233.201	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
66.249.93.223	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
149.78.39.38	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
70.32.40.218	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
149.78.200.202	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
85.255.235.76	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
89.139.38.64	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	37
87.250.241.78	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
66.249.81.129	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.249.75.36	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
149.78.136.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
40.77.167.14	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
66.249.93.247	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
66.249.93.241	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
93.172.147.109	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
46.120.162.70	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	18
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
79.176.143.253	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	17
66.249.81.167	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
213.57.229.26	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
66.249.66.107	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
46.19.85.186	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.54.17.96	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	13
66.249.81.238	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.249.75.36	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
85.250.197.7	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
46.120.5.156	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
212.150.112.56	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.179.204.16	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
84.228.9.76	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
46.19.86.83	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 000797BA2DB1F1119FFE86176D11FC09F8789B4936A5BDB5382E8C2726B92EB057B826E6FDEB7A8084EF50BEE4DEC309DA0C6D96F3040255BADB76C208C2B87F104C172C24C28173D946F3E16E80A65FAA3FA3ADA9A144EF21D3B16E8D93AED522890B90D552FE6A982AE33ADAC422703AED427BCB238C63463824D7AAE1105CA5D8E5544E31CCCB8AF843459ED7E7B6AECB2856A33F826F8631DE0BA9A20FE3	None	1