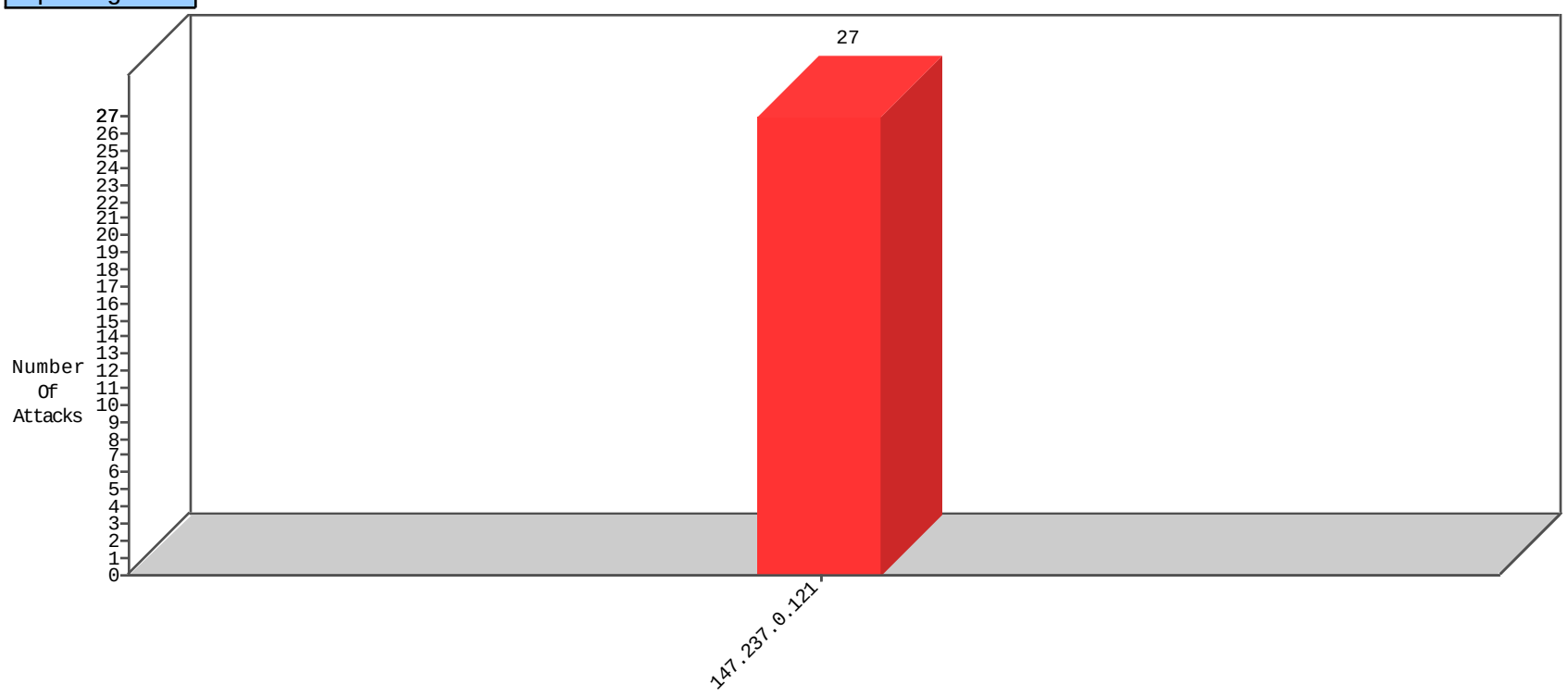
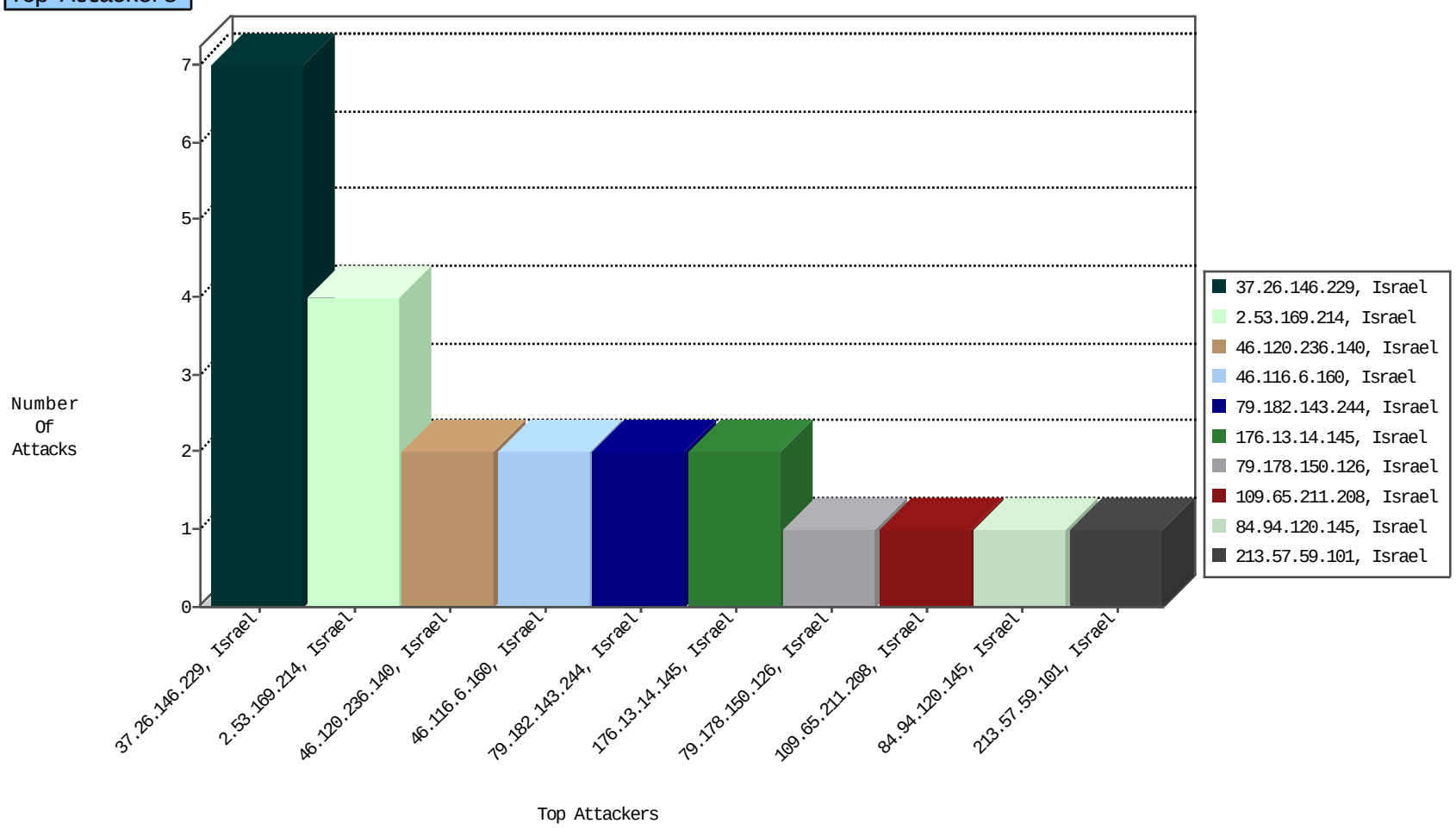
04-19-2016-12:06:00 to 04-19-2016-13:06:00

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



04-19-2016-12:06:00 to 04-19-2016-13:06:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
37.26.146.229	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	NetV-London	7

04-19-2016-12:06:00 to 04-19-2016-13:06:00

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

04-19-2016-12:06:00 to 04-19-2016-13:06:00

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
109.65.211.208	Israel	147.237.0.121		ET SCAN NMAP -sA (2)	1

04-19-2016-12:06:00 to 04-19-2016-13:06:00

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
72.37.140.42	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1436
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	281
110.174.141.142	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	278
149.88.145.147	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	244
50.118.145.136	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	222
193.186.163.3	Greece	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
46.16.142.100	Cyprus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
134.191.232.68	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
149.88.61.218	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
149.88.86.222	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.102.9.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
37.9.88.68	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
37.9.88.73	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
40.77.167.42	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	5
2.53.169.210	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.109.24.43	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	4
84.109.24.43	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.229	Israel	147.237.0.121		Bad TCP sequence		monitor	4
149.78.52.233	United States	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	4
5.102.242.217	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	3
149.78.52.233	United States	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	2
199.207.253.101	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.116.6.160	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.146.229	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
2.53.140.166	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.244.23.42	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
37.46.39.159	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
212.235.56.185	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
192.118.27.253	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
37.26.146.229	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
212.235.65.236	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	1
37.26.146.229	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	alert	1
2.55.24.46	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.199.251.235	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
195.244.23.42	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
37.26.146.230	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.235.56.185	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.53.169.214	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	4
46.120.236.140	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/shamapchange	Block	2
176.13.14.145	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	2
46.116.6.160	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	2
82.80.139.30	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.19.86.87	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
213.57.59.101	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	1
79.178.150.126	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	1
84.94.120.145	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.19.86.156	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	1
79.182.143.244	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
79.182.143.244	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
192.198.151.43	Europe	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 887F26D61C656FF4325532B2109EC64B8BAE39667AD19489E38A89EE5735C06DBA8C1942CC9F18647D615980EBA9446294C72D69554712B49D651B19D03B3B717C8D47596908EF7C2C999EA4F9B1D78352E33BAC5C91A37A79BD8F9F92E56F724A1CD79CB001A467289A6866E75763126F492CC90954EE89E2FB93D499404DDA, Observed D1FCC870C7559F07F3EB64C03FF0A6F9DFA01528F39A6F5D18472C86874438776415F19E1BB2F0F13539FA6CD0621C341852A8C16C81D5D64BA97B4E1568EEDBC76D2C7B197C6FE18D84FB719628B570B72BEC20209381113ACE3D8311C6FFA0B4123F	None	1