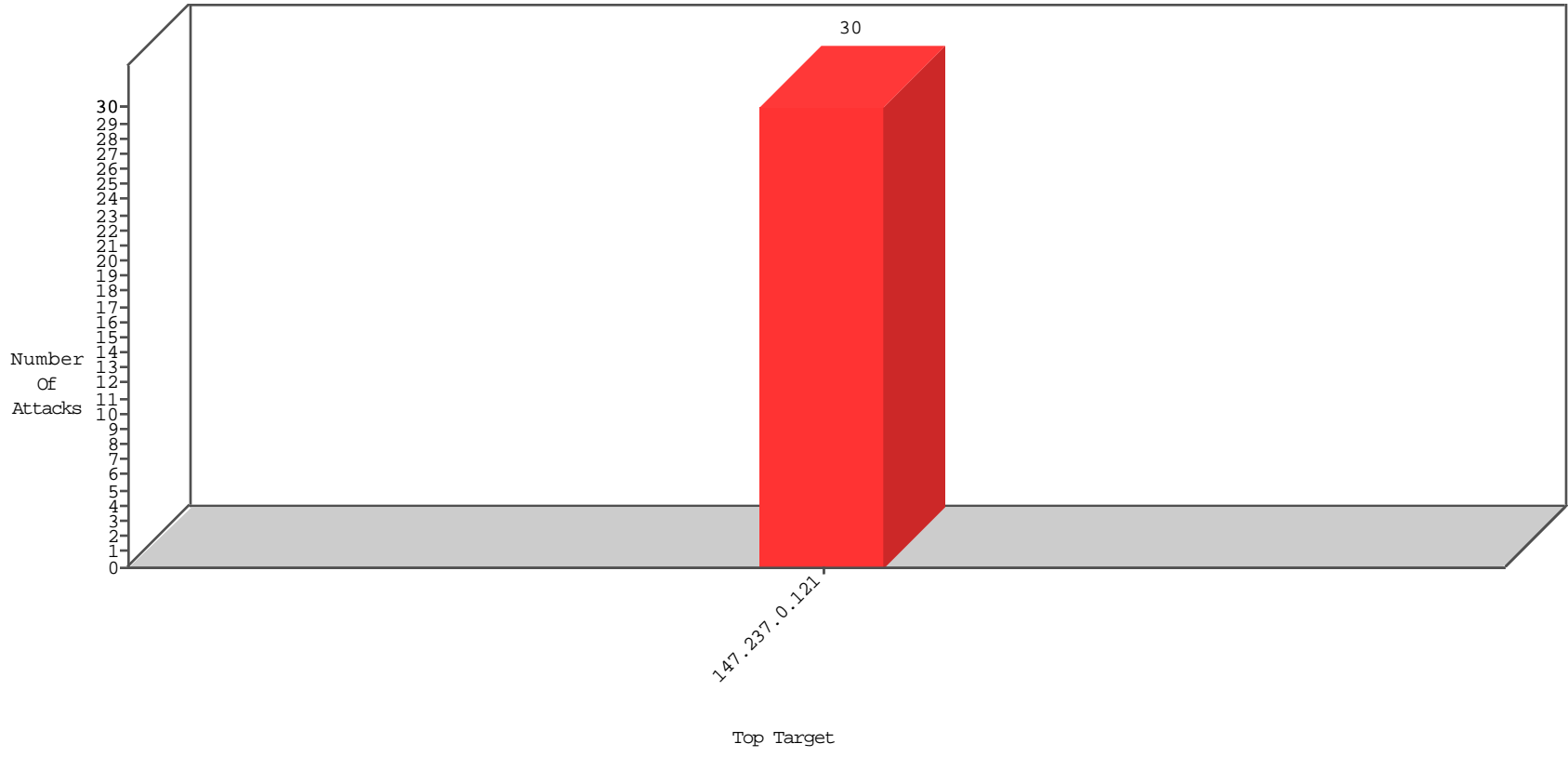


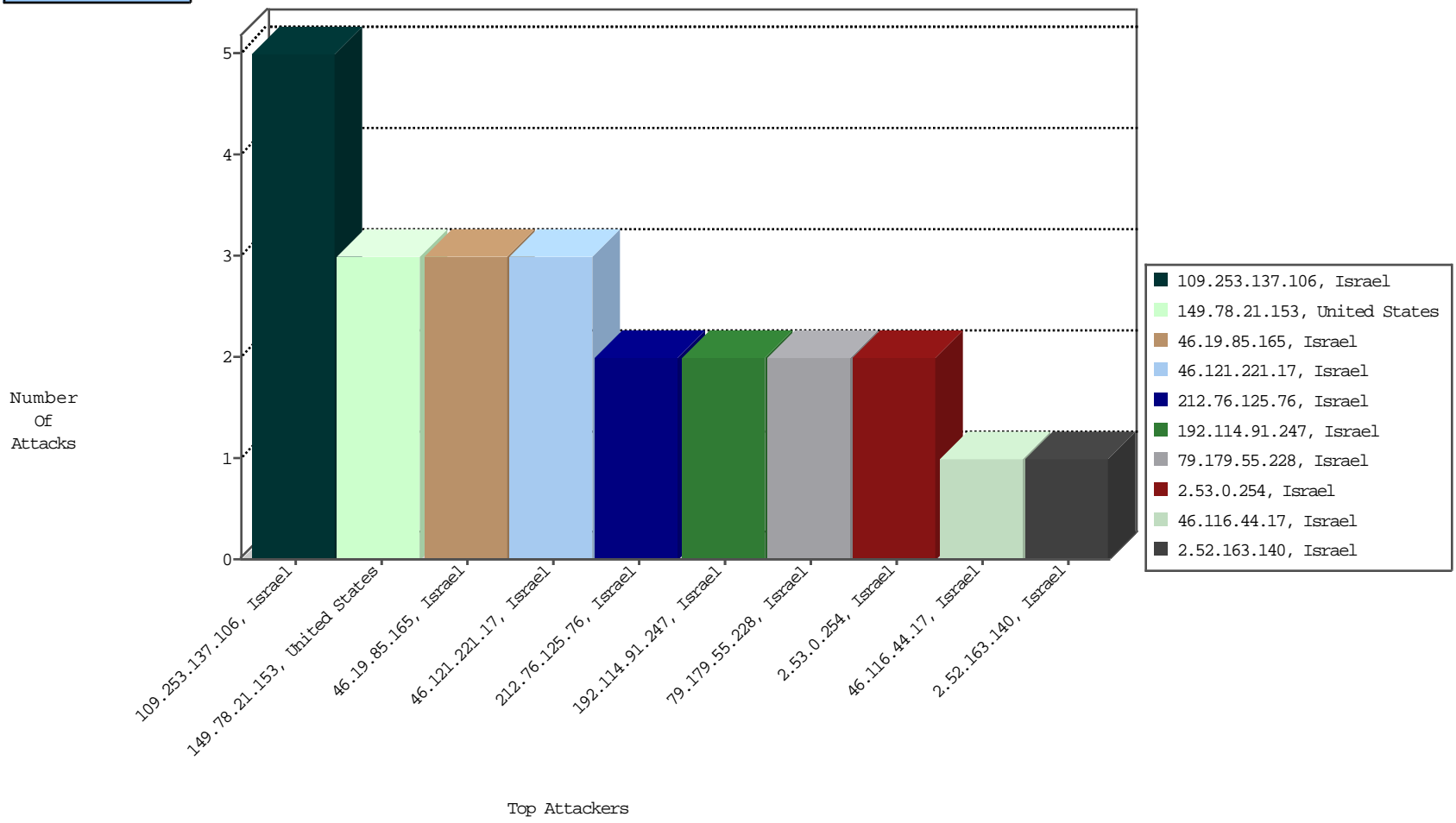
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

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

04-10-2016-11:06:02 to 04-10-2016-12:06:02

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
113.190.13.113	Vietnam	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.125.172.41	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2535
5.22.135.172	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	115
136.237.18.10	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
46.16.142.100	Cyprus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
149.88.135.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
158.116.225.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
17.78.122.217	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
62.219.234.65	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.6.84	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
149.88.62.22	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
178.140.193.71	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
167.220.196.230	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
46.19.85.165	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.144.32	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	9
81.218.241.26	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	9
31.168.96.254	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.1.181	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	4
82.166.53.83	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.121.221.17	Israel	147.237.0.121		drop	SAM rule	drop	4
185.32.179.182	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.71	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
212.179.21.194	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
5.22.131.119	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
149.50.51.117	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
81.218.101.3	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
62.219.195.25	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
199.203.215.1	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
37.26.147.173	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
199.203.215.1	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
147.235.236.1	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.165	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.59.250	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
176.13.1.181	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	1
149.50.51.117	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
188.120.148.188	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
132.73.204.249	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.253.137.106	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected B2B1F6CB93FD2A5A67AAF6207B75659B0085EBD2B86AEB34A6CDC62F979C63872FC913A4526 B5B8DADB08D0F7277F9D2C4236668BCDDA11BAED99818B314F8EOCE72DA1FEB881E3EFA48D 901BF9C42FADC423BE67F4CD4637A93C06C58F4392C6C0996D82BF8FAB3219B46FD36D79A0 A9811C1B9C94C17CCEAB789ABD0A8B1E, Observed C9406C87769819E50E0EAD985632E7F861B1BB6037C988E5668C7994393D08CE32E8B720A276 4F9FC36A946B3A726EB182087CDEEB5833BBEFFCD0AF16B0708C26D9852C885EB215108962A8 D8AEFE305CF6E6CD70FF32F715DB936946957D45B38D4D	None	5
46.121.221.17	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesIDs in www.miluum-ishi.aka.idf.il/valtanrequest	Block	3
149.78.21.153	United States	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	3
2.53.0.254	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
192.114.91.247	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.76.125.76	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
79.179.55.228	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
185.27.105.115	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
46.19.85.165	Israel	147.237.0.121		Suspicious Response Code	Block	1
212.76.125.76	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
79.179.55.228	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
31.168.160.218	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/shamapchange	Block	1
46.116.44.17	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
212.143.110.33	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.19.85.165	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
195.160.242.40	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.52.163.140	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.165	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1