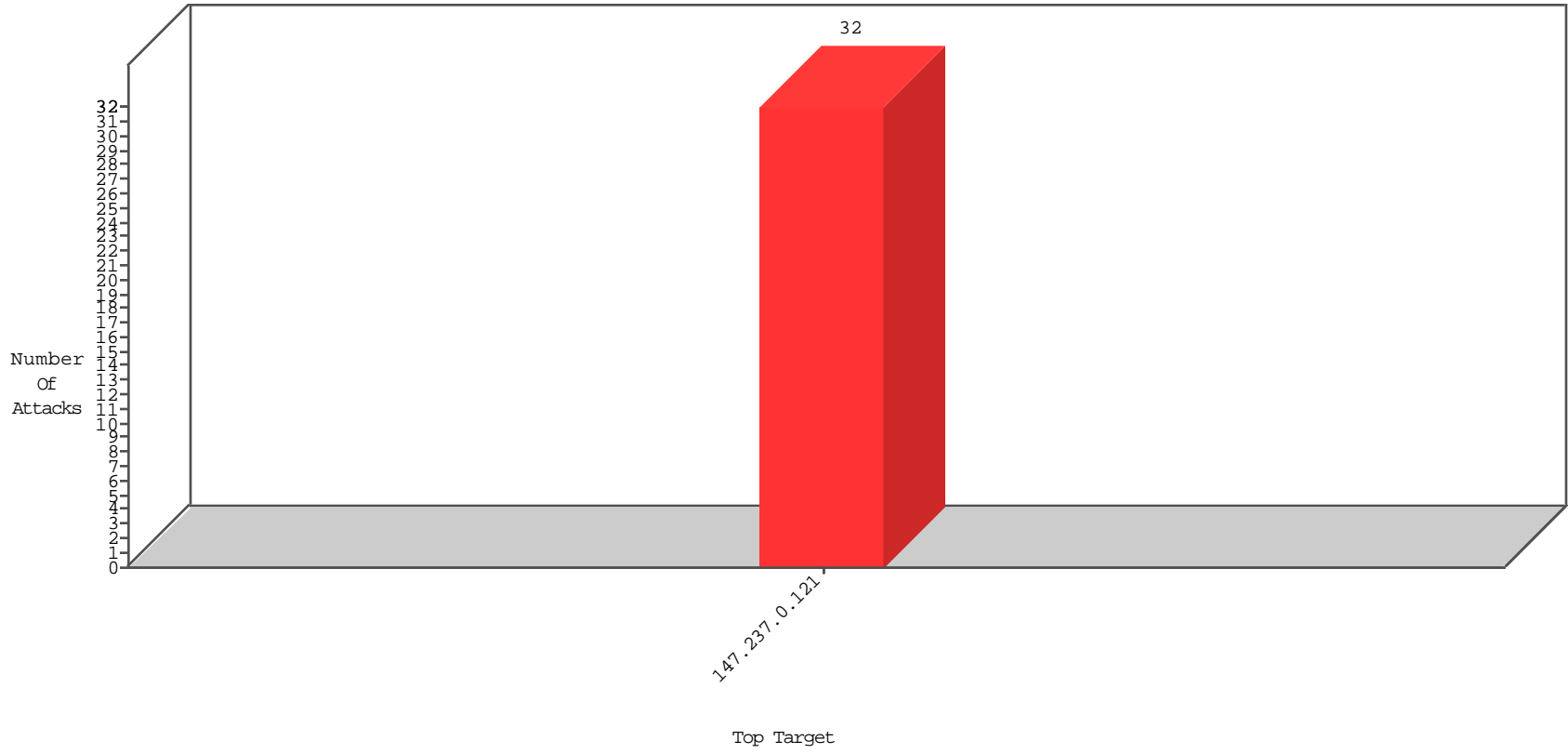


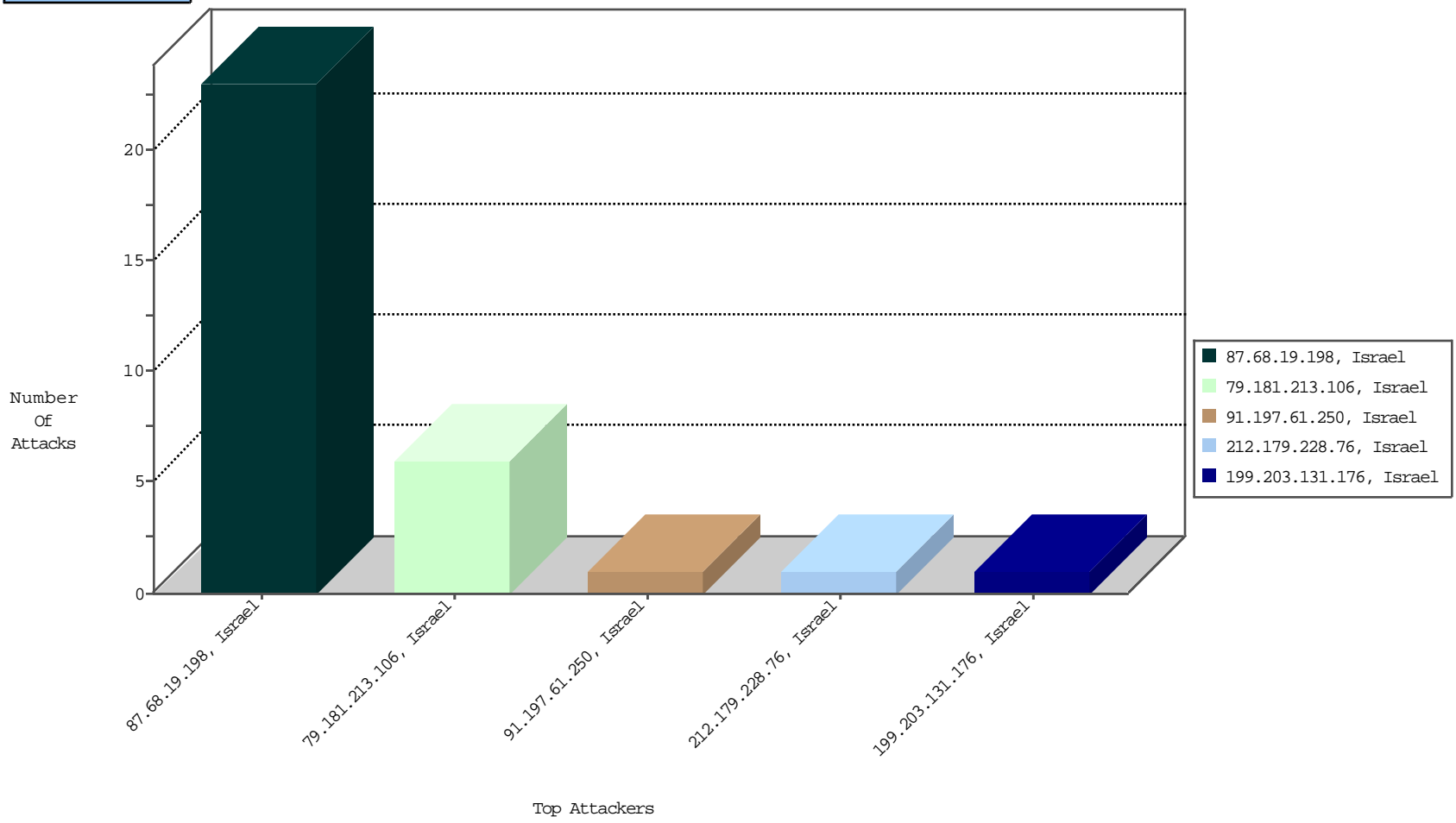
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.228.76	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Isreal	1

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
------------------	--------------	----------------	------	-----------	-------

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
165.225.72.51	Germany	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	504
217.33.23.241	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	402
199.207.253.101	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	274
149.88.229.147	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	245
17.78.81.218	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	230
87.68.19.198	Israel	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	monitor	224
62.221.5.234	Ireland	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	158
49.244.8.175	Nepal	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	144
87.121.106.19	Bulgaria	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	94
130.119.13.66	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	83
46.229.164.100	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	53
149.88.207.5	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	49
2.53.179.15	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
195.110.137.138	Italy	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.88.84.74	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	30
149.88.154.230	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	26
160.62.4.100	Switzerland	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	19
31.168.204.70	Israel	147.237.0.121	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
62.219.183.196	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
194.90.232.2	Israel	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
66.102.9.50	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	12
66.102.9.74	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	10
80.179.114.11	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	9
194.90.232.2	Israel	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	alert	9
80.179.114.11	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	alert	6
213.57.237.217	Israel	147.237.0.121	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.102.9.97	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	4
212.179.21.194	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.237.217	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.242.61	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.39.195	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.39.193	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.10.91	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.199.251.227	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	alert	1
185.3.144.34	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	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.181.213.106	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddDocs&FileToActivate in www.miluim-ishi.aka.idf.il/login	Block	3
79.181.213.106	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddDocs&FilesToCheck in www.miluim-ishi.aka.idf.il/login	Block	2
87.68.19.198	Israel	147.237.0.121		Malformed HTTP Header Line 1	Block	1
87.68.19.198	Israel	147.237.0.121		Abnormally Long Header Line request header name	Block	1
87.68.19.198	Israel	147.237.0.121		NULL Character in Header Name at	Block	1
87.68.19.198	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Name from 87.68.19.198	Block	1
87.68.19.198	Israel	147.237.0.121		Illegal Byte Code Character in Method g³ù:d[#5]0`[[#28]][[#15]][[#18]][[#23]]ä>Ä[[#5]]•ä¶Y[[#6]]'š; ,ab;ý-èw<^[[#20]]İ'cæž"ò-ĐÈ }@c-0cú7µ+ã'[[#25]][[#16]]ÄöÜ>#012'•bé>ZçİŠ:P•Öÿæ[[#31]]9ž'	Block	1
79.181.213.106	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesNames in www.miluim-ishi.aka.idf.il/volunteeringbyage	Block	1
87.68.19.198	Israel	147.237.0.121		Unknown HTTP Request Method g³ù:d[#5]0`[[#28]][[#15]][[#18]][[#23]]ä>Ä[[#5]]•ä¶Y[[#6]]'š; ,ab;ý-èw<^[[#20]]İ'cæž"ò-ĐÈ }@c-0cú7µ+ã'[[#25]][[#16]]ÄöÜ>#012'•bé>ZçİŠ:P•Öÿæ[[#31]]9ž' in URL	Block	1
87.68.19.198	Israel	147.237.0.121		Multiple Malformed URL from 87.68.19.198	Block	1
87.68.19.198	Israel	147.237.0.121		Malformed URL	Block	1
87.68.19.198	Israel	147.237.0.121		Abnormally Long Request method	Block	1
87.68.19.198	Israel	147.237.0.121		NULL Character in URL o aũ4j> " 3,1ç"f]]32#[[+']]22#[[@]]3#[["1Ü{ü}]41#[[;]]41#[[@n ç"s[[#28]] ²-G-i)hw>æ ¥ [[0#]] 5"° ' ; g [[03#]]e	Block	1
87.68.19.198	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Value from 87.68.19.198	Block	1
87.68.19.198	Israel	147.237.0.121		Illegal Byte Code Character in URL o aũ4j> " 3f]]32#[[+']]22#[[@]]3#[["1Ü{ü}]41#[[;]]41#[[@n "çl,ç"s[[#28]] ²-G-i)hw>æ ¥ [[0#]] 5"° ' ; g [[03#]]e	Block	1
91.197.61.250	Israel	147.237.0.121		Double URL Encoding - parameter: ct100\$ContentPlaceHolder1\$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
87.68.19.198	Israel	147.237.0.121		Multiple NULL Character in Header Name from 87.68.19.198	Block	1
87.68.19.198	Israel	147.237.0.121		Multiple Abnormally Long Header Line from 87.68.19.198	Block	1
87.68.19.198	Israel	147.237.0.121		Illegal Byte Code Character in Header Name '[[#24]]-[[#21]]0*8fİ?È	Block	1
87.68.19.198	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
87.68.19.198	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Method from 87.68.19.198	Block	1
87.68.19.198	Israel	147.237.0.121		Illegal HTTP Version	Block	1
199.203.131.176	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
87.68.19.198	Israel	147.237.0.121		Multiple Unknown HTTP Request Method from 87.68.19.198	Block	1
87.68.19.198	Israel	147.237.0.121		Multiple Abnormally Long Request from 87.68.19.198	Block	1
87.68.19.198	Israel	147.237.0.121		Illegal Byte Code Character in Header Value	Block	1
87.68.19.198	Israel	147.237.0.121		Too Many Headers per Request - 61 Headers	Block	1
87.68.19.198	Israel	147.237.0.121		Multiple Malformed HTTP Header Line from 87.68.19.198	Block	1