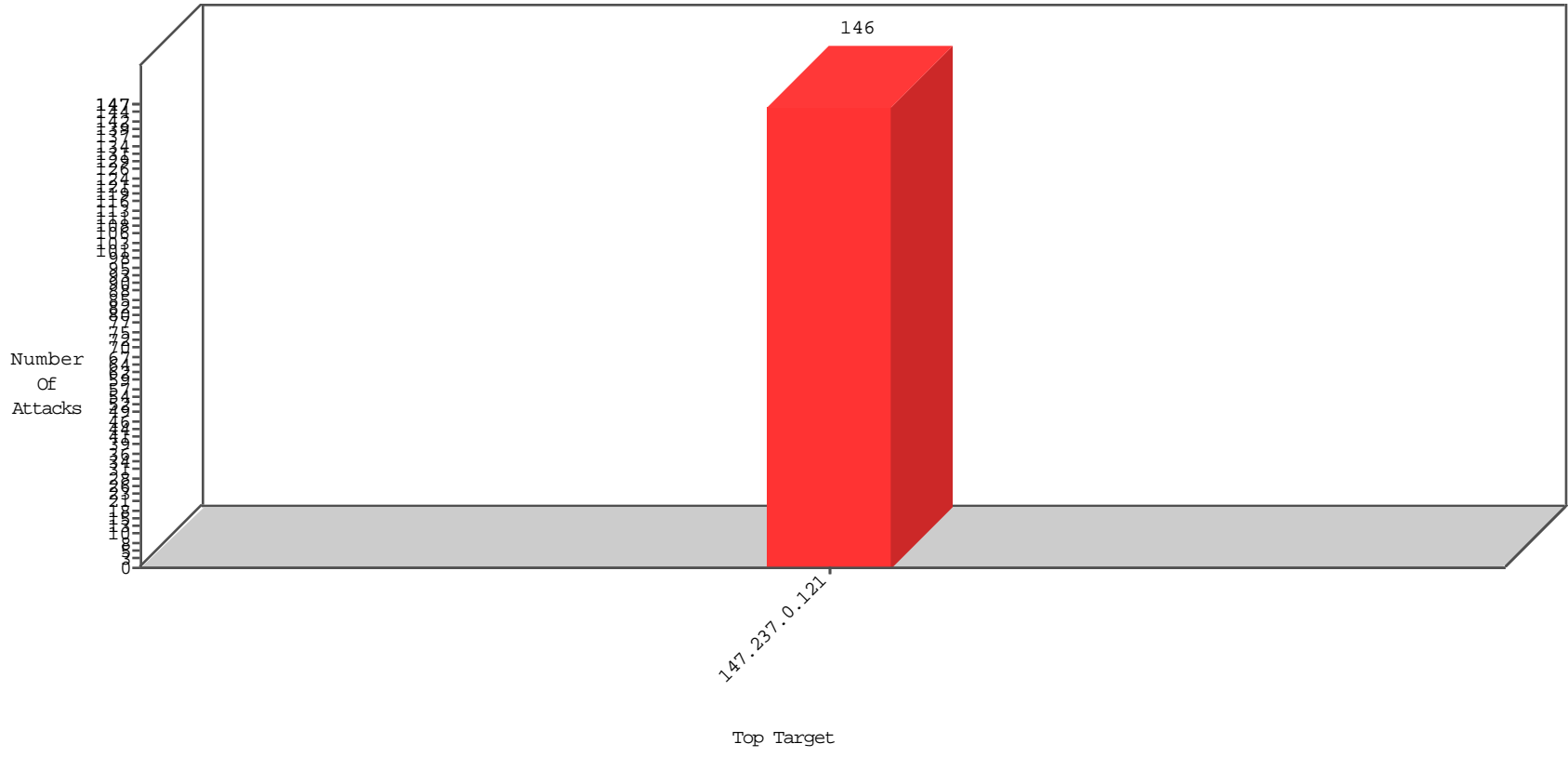


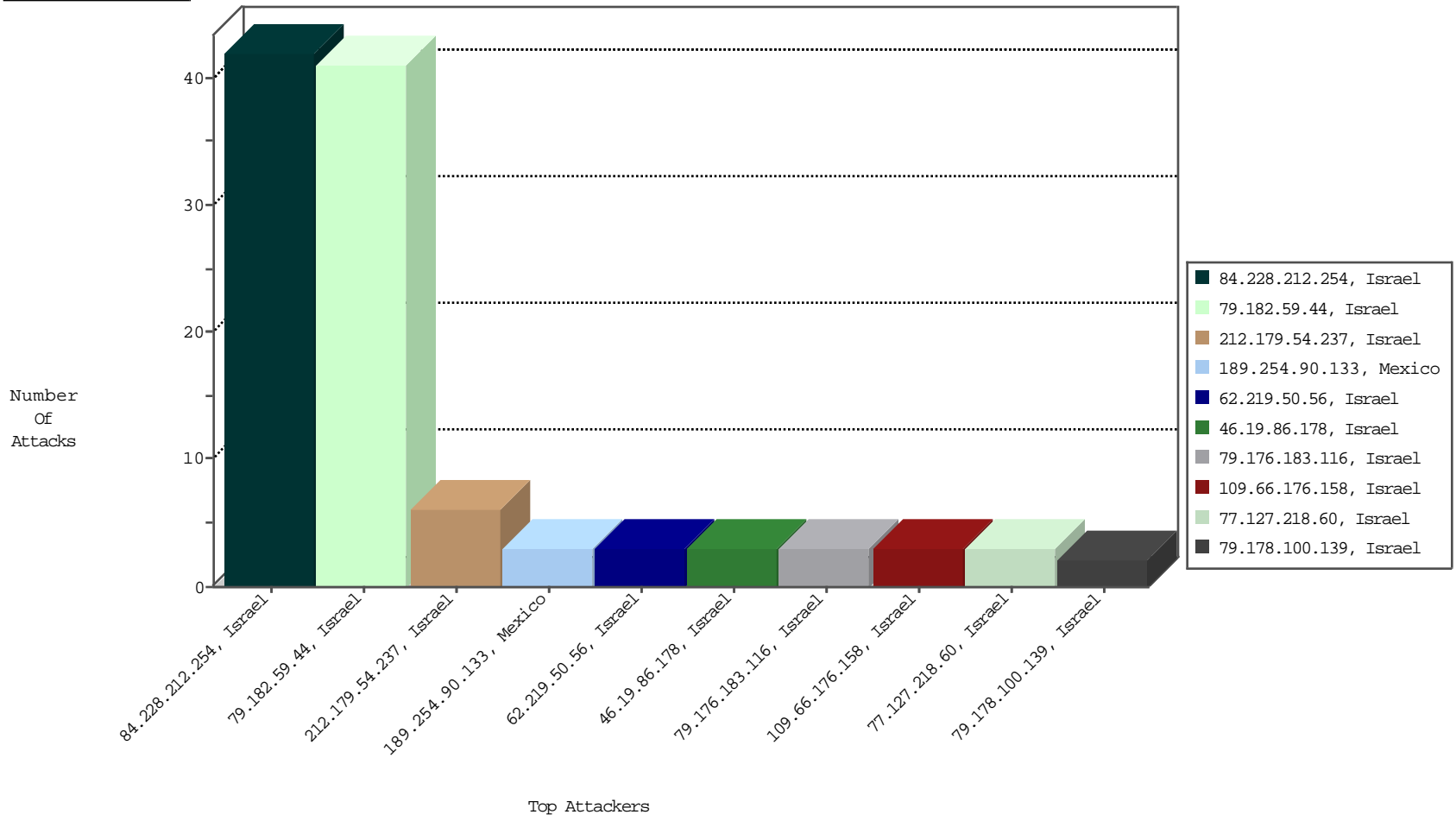
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Isreal	6
79.176.183.116	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Isreal	3
188.120.148.25	Israel	147.237.0.121		network flood IPv4 TCP-RST	drop	DP-Tehila	1

02-12-2016 to 02-13-2016

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
62.215.34.14	Kuwait	147.237.0.121		ET SCAN Potential SSH Scan	2
188.120.132.55	Israel	147.237.0.121		ET SCAN NMAP -sA (2)	2
189.254.90.133	Mexico	147.237.0.121		ET SCAN NMAP -f -sS	1
189.254.90.133	Mexico	147.237.0.121		ET SCAN NMAP -sS window 3072	1
51.254.23.230	United Kingdom	147.237.0.121		ET SCAN Potential SSH Scan	1
189.254.90.133	Mexico	147.237.0.121		ET SCAN NMAP -sS window 2048	1
218.200.188.213	China	147.237.0.121		ET SCAN Potential SSH Scan	1
61.244.111.77	Hong Kong	147.237.0.121		ET SCAN Potential SSH Scan	1
112.168.26.199	Korea, Republic of	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
79.182.59.44	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1215
108.171.135.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	914
139.181.48.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	880
149.78.151.84	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	788
46.254.129.4	Bulgaria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	320
149.78.48.204	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	249
149.88.165.95	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	246
212.82.108.124	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	168
149.78.182.57	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	168
149.88.178.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	157
149.88.71.127	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	153
149.88.237.19	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	151
149.88.21.171	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	149
2.54.38.100	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.34.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
212.82.108.32	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
12.250.207.42	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	124
149.78.93.152	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	109
194.69.102.78	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	106
79.182.59.44	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	101
149.88.101.173	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	97
149.50.71.237	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
149.78.123.78	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
90.154.240.147	Bulgaria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
109.67.56.140	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
5.29.183.191	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	72
149.88.219.206	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	72
149.88.146.176	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
181.141.14.135	Colombia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
190.65.221.61	Colombia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
40.114.210.53	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
149.88.127.48	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
193.240.172.173	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.78.43.80	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	58
87.237.218.161	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.78.246.2	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
149.78.192.193	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
79.182.59.44	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	49
212.82.108.125	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
212.82.108.33	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.78.34.148	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
149.88.82.213	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
68.99.184.92	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.78.60.229	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
37.46.38.23	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	34
62.128.7.44	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.88.215.28	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30

Top Attackers In WAF

Table with 7 columns: Attacker Address, Attacker Geo, Target Address, Site, Signature, Device Action, Count. Contains 55 rows of attack logs from various IP addresses, primarily from Israel, targeting various endpoints on miluim-ishi.aka.idf.il.

02-12-2016 to 02-13-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
188.120.128.25	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceholder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
79.183.110.92	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
84.228.212.254	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.29.83.198	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.212.254	Israel	147.237.0.121		Illegal Byte Code Character in Header Name ?Ã%G^Â±`"hYaÃ,,Ã?ÃpÃ%OEÂ·m[[#17]]b[[#31]]2aÂ™ Â±Â?Â± R#[[#14]]ÂŠcÃ-[[#24]][[#11]](Ã¶Â"Â?Â±ÃcPd8	Block	1

02-12-2016 to 02-13-2016