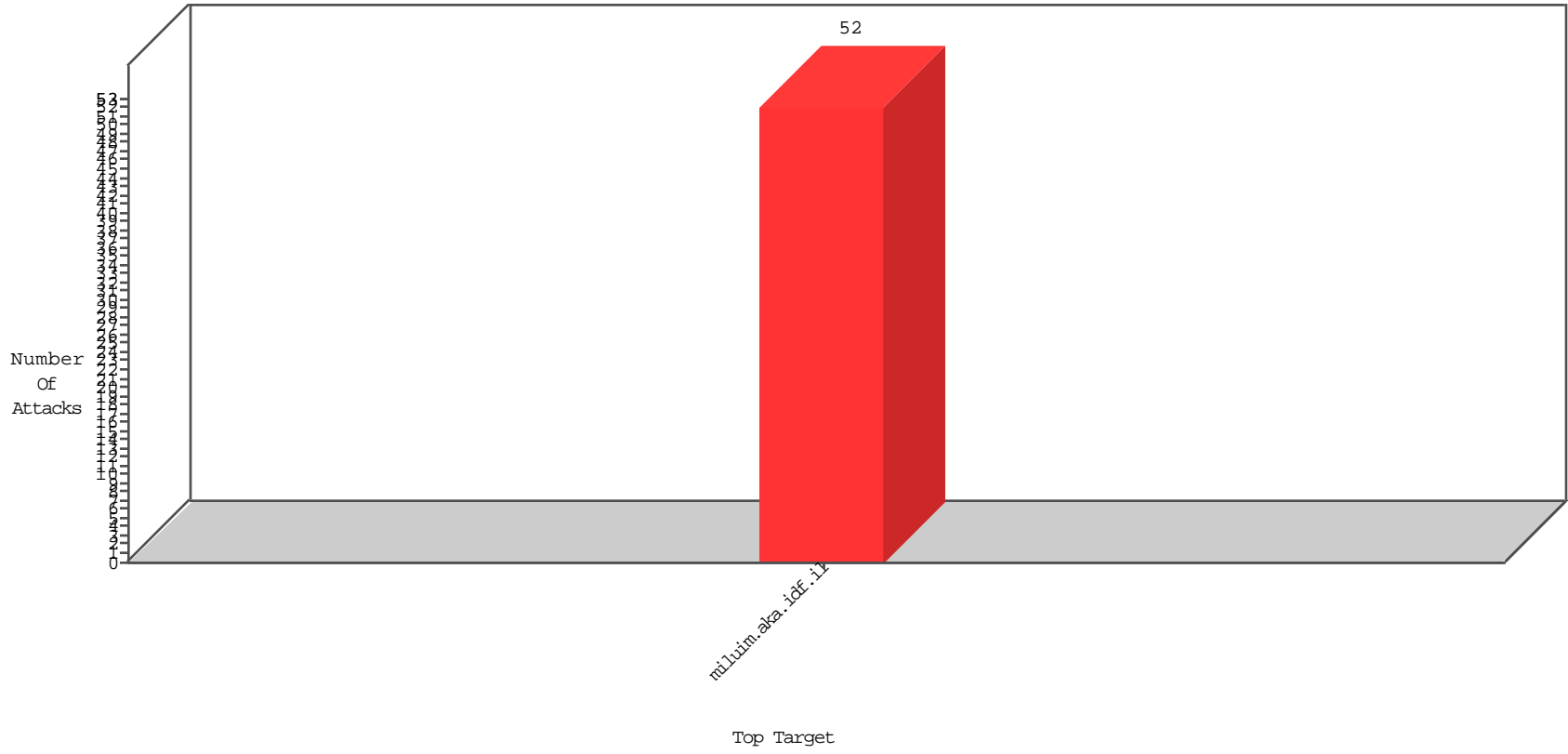


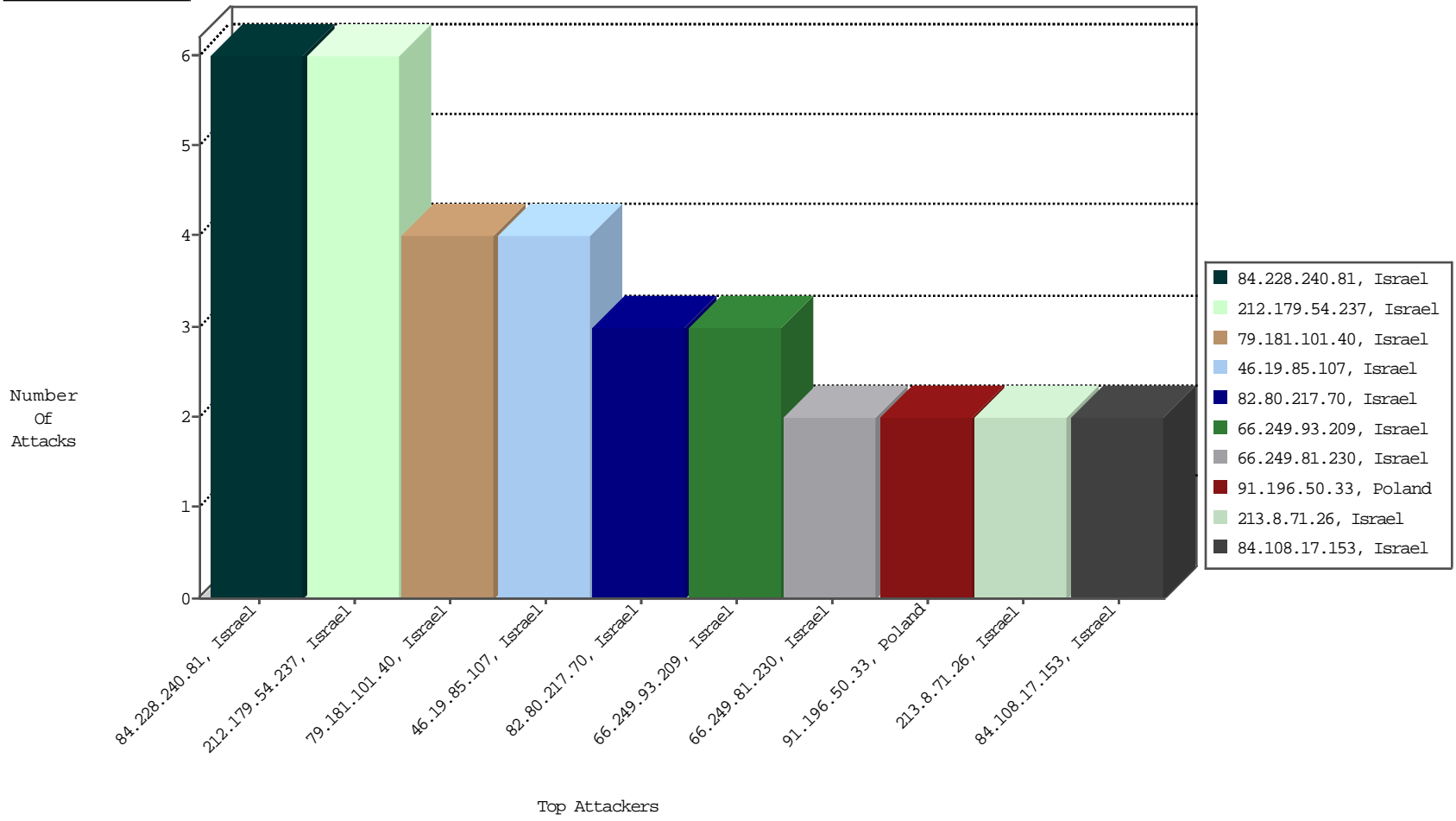
Focused IP Under Attack Daily Report



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	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	6
82.80.217.70	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
66.249.81.230	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	2
222.208.63.226	China	147.237.0.120	miluim.aka.idf.il	Invalid TCP Flags	drop	BBL-Frankfurt	2
66.249.81.227	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1

02-22-2016 to 02-23-2016

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
185.56.28.72	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
138.36.0.4		147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	Sweden	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.51.30	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
62.90.10.180	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
46.19.86.119	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
82.81.58.112	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
134.191.232.92	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	1905
79.178.122.236	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1314
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	697
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	625
37.26.148.155	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	290
37.26.148.155	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	290
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	221
46.19.85.22	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	194
79.183.129.98	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	155
79.176.61.135	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.180.15.99	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
77.127.2.70	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
77.127.163.124	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.178.31.102	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.157.246	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	134
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	101
37.26.149.174	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	100
109.226.22.11	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	92
79.178.115.36	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	92
2.54.254.131	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
37.26.149.174	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	82
46.19.86.130	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
80.246.130.169	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence		monitor	74
79.181.223.206	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	72
149.78.39.93	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
2.52.9.131	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
149.78.42.87	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	57
79.181.223.206	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	56
185.27.105.66	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
46.19.85.201	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	50
84.111.38.217	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
2.52.2.45	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
149.78.42.87	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
149.78.42.87	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	42
46.19.85.126	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	40
46.19.85.126	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	40
46.121.252.217	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	38
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	38
132.64.25.35	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
46.19.85.167	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
46.19.85.94	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36

02-22-2016 to 02-23-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.19.85.107	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method rh in URL	Block	2
84.228.240.81	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	2
84.228.240.81	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	2
40.77.167.10	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	2
212.117.136.6	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter fileld in www.miluim.aka.idf.il/console/core/doc_mgr/library/manage/resource/getfilecontent.hh.asp	Block	2
84.108.17.153	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/14	Block	2
91.196.50.33	Poland	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	2
79.181.101.40	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1446-he/miluim.aspx&?â€ž	Block	2
46.19.85.107	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL	Block	2
84.228.240.81	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 84.228.240.81	Block	2
128.232.110.28	United Kingdom	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	2
79.181.101.40	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1446-he/miluim.aspx	Block	2
213.8.71.26	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
66.249.93.212	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Directory Traversal (In URL)	Block	1
195.160.242.40	Israel	147.237.0.120	miluim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 195.160.242.40	Block	1
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.i	Directory Traversal (In URL)	Block	1
66.249.93.215	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Directory Traversal (In URL)	Block	1
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.i	Directory Traversal - 16	Block	1
213.8.71.26	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/1935.gif	Block	1
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/../../images/shared/hp/gallery_page.png	Block	1

02-22-2016 to 02-23-2016