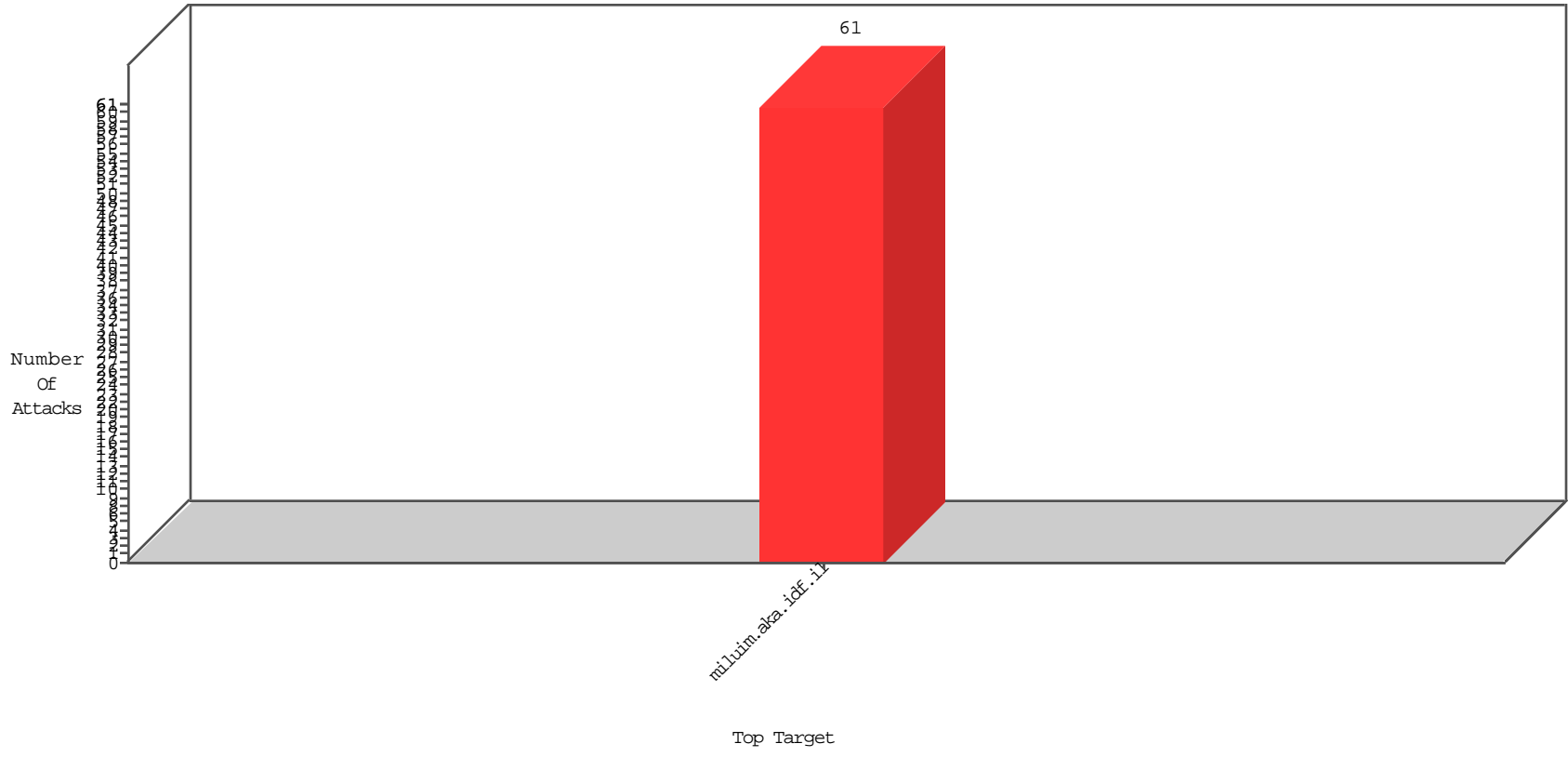


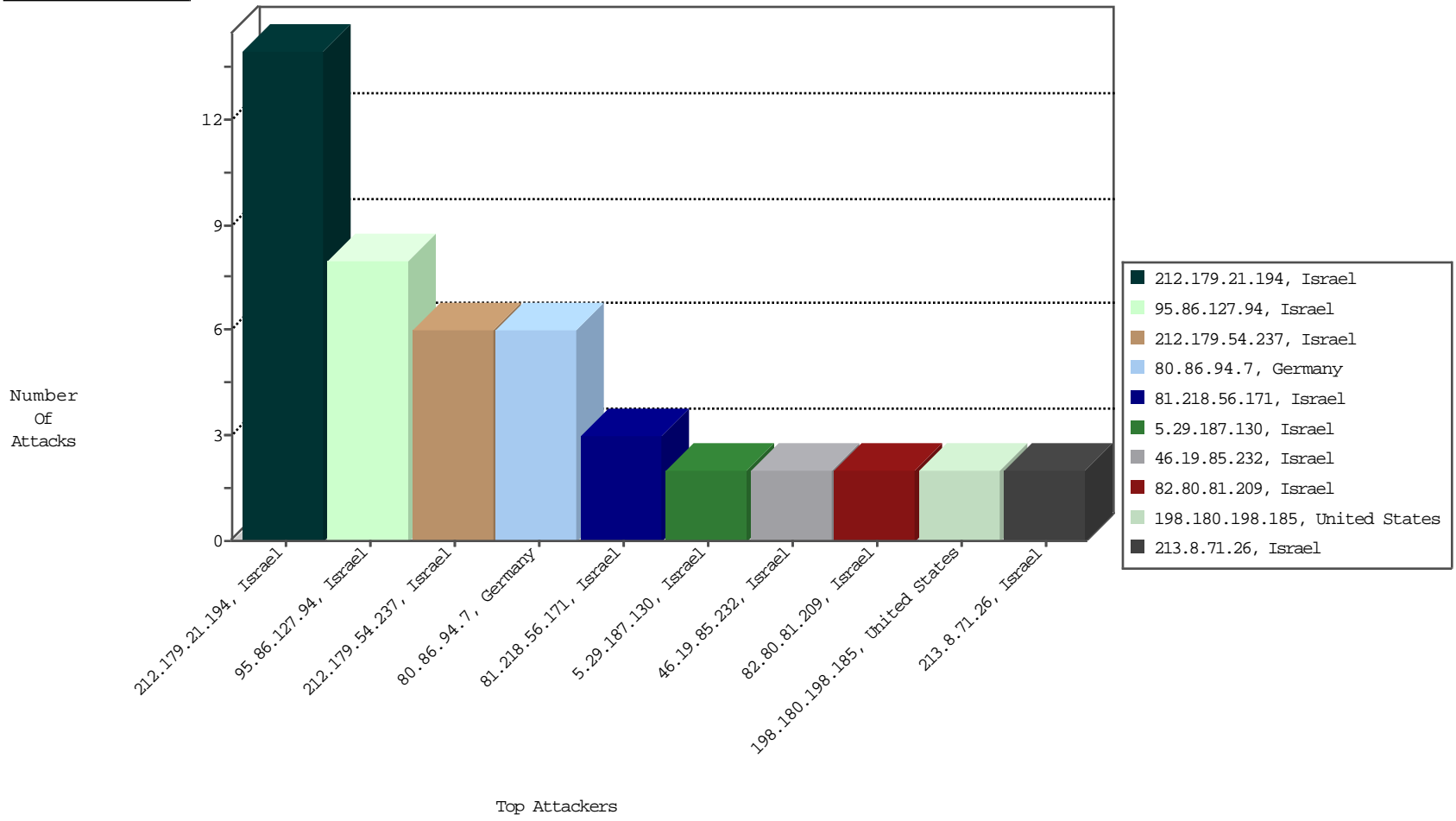
Focused IP Under Attack Daily Report



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	BEL-Israel	6
83.209.148.23	Sweden	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
184.105.139.116	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.126	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1

02-24-2016 to 02-25-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.120.204.172	Israel	147.237.0.120	miluim.aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
42.119.112.63	Vietnam	147.237.0.120	miluim.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.5.9.71	China	147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
185.93.187.109		147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
198.180.198.185	United States	147.237.0.120	miluim.aka.idf.i	ET SCAN NMAP -sS window 4096	1
23.101.130.223	United States	147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
45.63.48.159		147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
183.3.202.115	China	147.237.0.120	miluim.aka.idf.i	ET SCAN Potential SSH Scan	1
198.180.198.185	United States	147.237.0.120	miluim.aka.idf.i	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
5.22.134.223	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2313
79.177.206.29	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.52.86	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
109.66.18.74	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.52.54.122	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	792
79.180.168.205	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	720
2.54.0.146	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	513
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	378
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
46.19.86.218	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	198
2.52.156.43	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	197
31.154.150.67	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.180.216	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.48.196	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.88.5.103	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.126.24		147.237.0.120	miluim.aka.idf.i	drop	SAM rule	drop	132
217.194.198.109	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	57
217.194.198.109	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	57
46.19.85.225	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
185.120.126.23		147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
46.19.85.36	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.36	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
2.52.158.62	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
94.230.86.211	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	28
79.182.96.103	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
79.183.160.81	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
109.64.24.176	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
94.230.86.207	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
31.154.2.162	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
31.210.187.166	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
31.154.2.162	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	alert	19
213.57.153.178	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
94.230.86.129	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
79.177.187.103	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.121	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.232	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
62.0.75.140	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
63.99.16.220	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
37.142.192.174	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
63.99.16.220	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
5.28.164.3	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.16.142.100	Cyprus	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
185.3.144.37	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
85.130.204.250	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
87.70.11.190	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
85.130.204.250	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
192.114.23.18	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
199.203.240.49	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
199.203.215.1	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
213.8.70.101	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9

02-24-2016 to 02-25-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	9
95.86.127.94	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 95.86.127.94	Block	5
80.86.94.7	Germany	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 80.86.94.7	Block	5
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Distributed PHP Attempt	Block	4
95.86.127.94	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	3
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/scriptresource.axd parameter wb48617274	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	2
82.80.81.209	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	2
82.81.32.63	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/general.aspx	Block	1
46.19.85.232	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL	Block	1
149.78.23.178	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	1
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
93.113.125.11	Romania	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /	Block	1
46.19.85.232	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method r0ssw545 in URL	Block	1
185.35.62.11	Switzerland	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
81.218.56.171	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
5.29.187.130	Israel	147.237.0.120	miluim.aka.idf.i	Distributed PHP Attempt	Block	1
5.29.187.130	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
80.86.94.7	Germany	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/sitemap/sitemap.aspx	Block	1

02-24-2016 to 02-25-2016