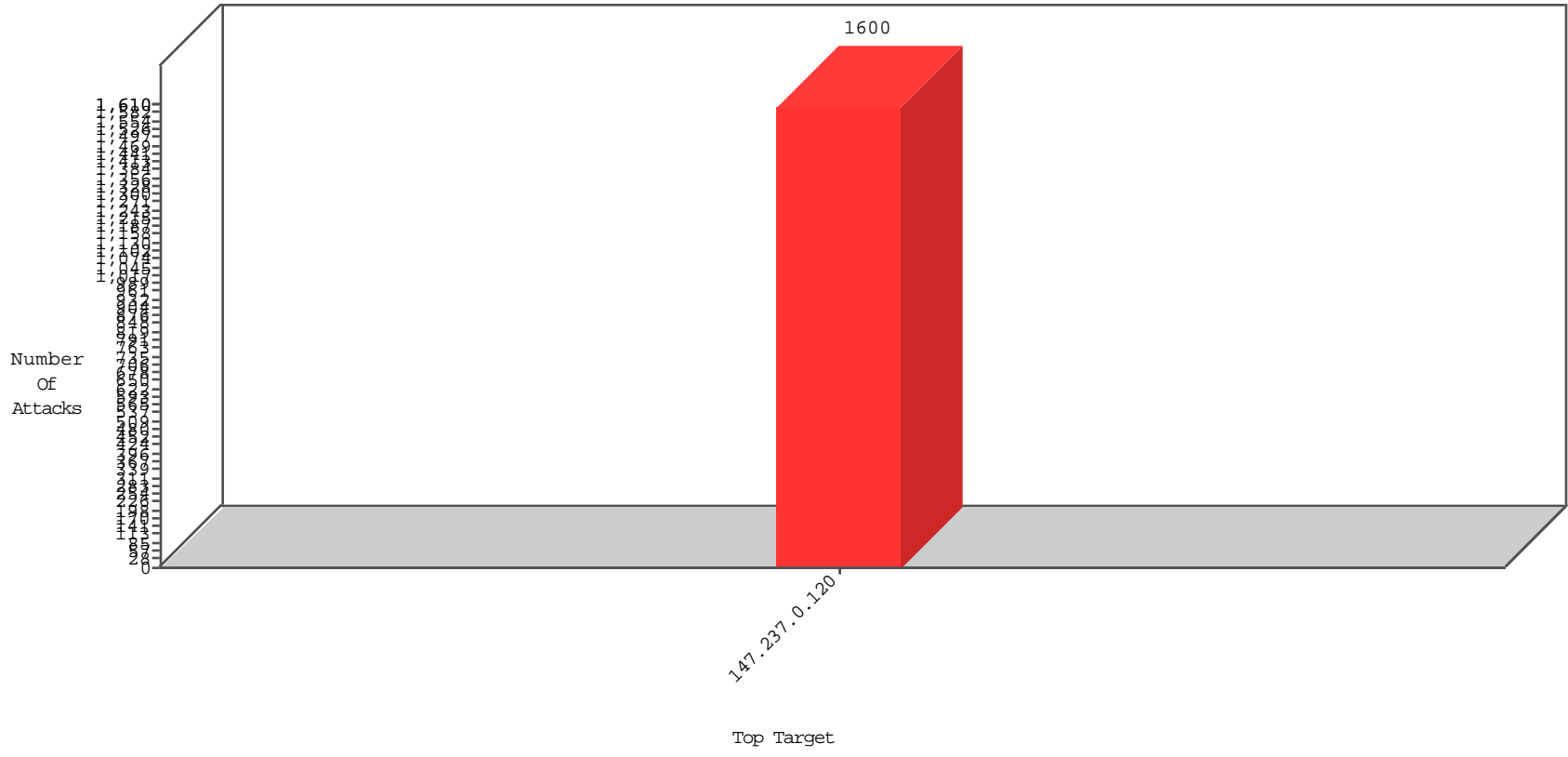


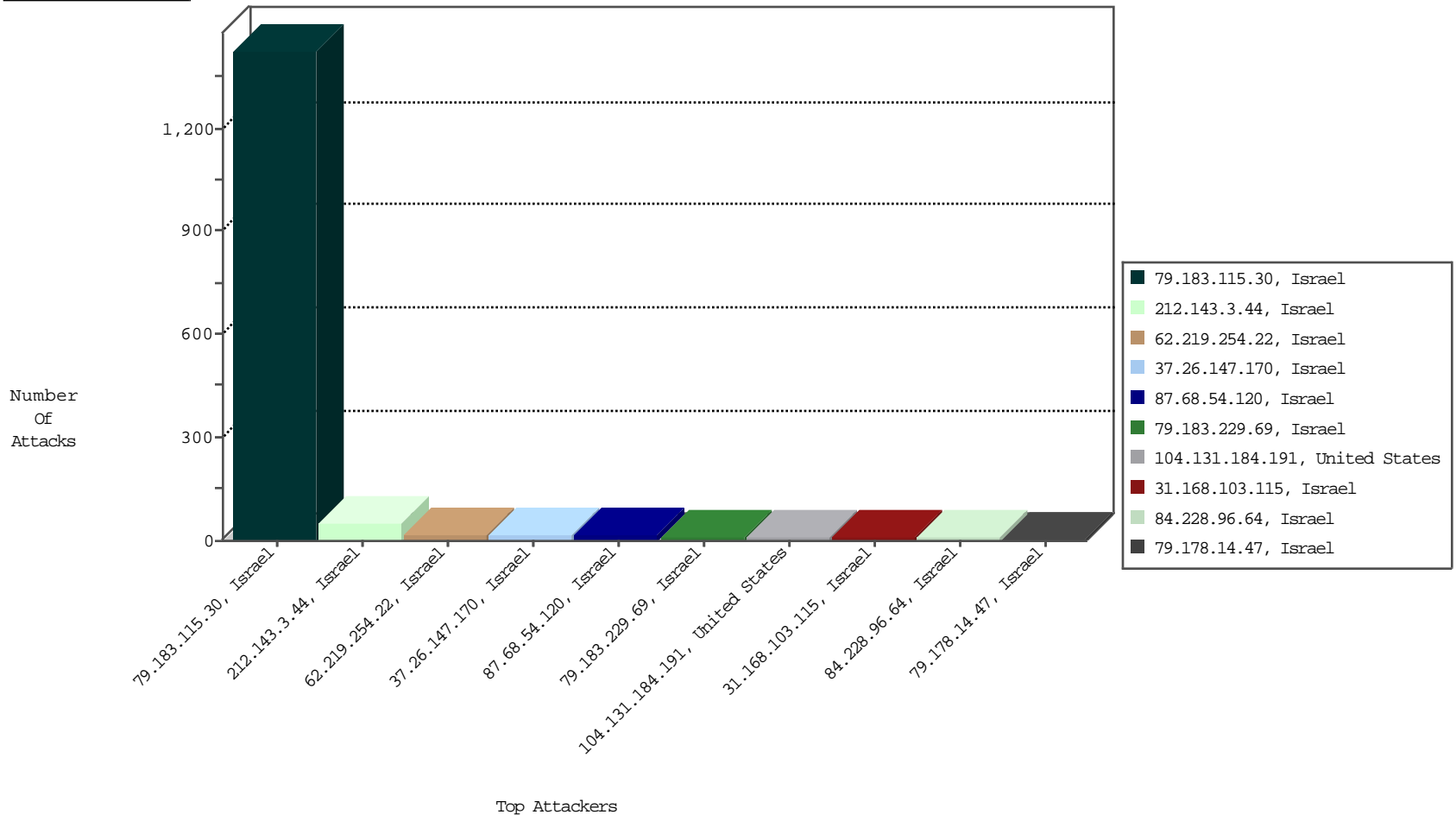
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
62.219.254.22	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BEL-Israel	18
79.183.229.69	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BEL-Israel	12
31.168.133.226	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BEL-Israel	3
37.26.147.170	Israel	147.237.0.120		Invalid TCP Flags	drop	BEL-Israel	3
81.218.206.82	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BEL-Israel	3
115.236.75.201	China	147.237.0.120		Frk_Under_Attack_Con_Tcp	drop	BEL-Frankfurt	2

11-02-2015 to 11-03-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.143.3.44	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	48

11-02-2015 to 11-03-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
37.26.147.170	Israel	147.237.0.120		POLICY-OTHER TCP packet with urgent flag attempt	15
180.153.153.117	China	147.237.0.120		ET SCAN Potential SSH Scan	1
199.101.186.159	United States	147.237.0.120		ET SCAN NMAP -sS window 3072	1
202.100.99.7	China	147.237.0.120		ET SCAN Potential SSH Scan	1
223.4.174.30	China	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
115.84.94.11	Lao People's Democratic Republic	147.237.0.120		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.210.201.106	Singapore	147.237.0.120		ET SCAN Potential SSH Scan	1
199.101.186.159	United States	147.237.0.120		ET SCAN NMAP -sS window 4096	1
212.7.209.9	Netherlands	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
66.249.83.182	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	106420
66.249.83.179	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	83791
66.249.83.185	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	78200
66.249.88.130	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	9948
66.249.88.142	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	9725
66.249.88.136	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	9119
79.183.54.43	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4608
168.63.137.102	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	3013
109.64.0.189	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.178.24.17	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.181.190.101	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.182.184.114	Israel	147.237.0.120	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1394
149.78.34.43	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	1258
66.102.9.80	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	1009
149.78.27.94	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	936
66.102.9.100	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	821
66.102.9.90	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	782
192.146.6.2	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	730
77.242.202.227	France	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	704
168.63.200.167	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	530
68.180.229.121	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	530
125.19.102.130	India	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	523
149.78.220.184	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	440
66.249.79.110	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	414
149.78.35.24	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	396
66.249.79.114	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	391
149.88.5.170	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	383
149.78.224.163	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	374
66.249.79.112	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	354
149.78.2.63	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	332
149.88.34.143	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	321
149.88.113.61	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	273
149.78.238.49	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	259
85.115.52.201	United Kingdom	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	228
66.249.75.235	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	206
109.95.74.239	Russian Federation	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	200
66.249.79.110	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	184
149.78.64.235	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	182
66.249.79.114	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	163
66.249.79.112	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	160
149.88.212.148	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	154
149.78.22.106	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	150
66.249.83.179	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.88.98.13	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	137
66.249.83.185	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	137
66.249.83.182	Israel	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	135
66.249.75.219	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	133
161.202.87.226	Netherlands	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	126
79.161.20.58	Norway	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	124
66.249.75.227	United States	147.237.0.120	Geo-location enforcement	Geo-location inbound enforcement	drop	117

11-02-2015 to 11-03-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site Signature	Device Action	Count
79.183.115.30	Israel	147.237.0.120	Suspicious Response Code	Block	1428
87.68.54.120	Israel	147.237.0.120	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	15
104.131.184.191	United States	147.237.0.120	Multiple Unauthorized URL Access from 104.131.184.191	Block	7
31.168.103.115	Israel	147.237.0.120	Multiple Unauthorized URL Access from 31.168.103.115	Block	6
84.228.96.64	Israel	147.237.0.120	PHP Attempt	Block	3
84.228.96.64	Israel	147.237.0.120	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	3
79.178.14.47	Israel	147.237.0.120	Distributed PHP Attempt	Block	2
176.12.137.138	Israel	147.237.0.120	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx&e-	Block	2
79.178.14.47	Israel	147.237.0.120	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/ajax/updatestatus.php	Block	2
79.178.14.47	Israel	147.237.0.120	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/ufi/reaction/	Block	2
62.219.99.130	Israel	147.237.0.120	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx&e?â™	Block	2
84.228.96.64	Israel	147.237.0.120	Multiple Unauthorized URL Access from 84.228.96.64	Block	1
87.68.254.48	Israel	147.237.0.120	Distributed PHP Attempt	Block	1
79.181.122.163	Israel	147.237.0.120	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
104.131.184.191	United States	147.237.0.120	Unauthorized URL Access to miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
212.143.124.12	Israel	147.237.0.120	PHP Attempt	Block	1
87.68.254.48	Israel	147.237.0.120	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
79.181.122.163	Israel	147.237.0.120	Unauthorized URL Access to www.miluim.aka.idf.il/ufi/reaction/	Block	1
31.168.103.115	Israel	147.237.0.120	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
104.171.124.84	United States	147.237.0.120	E-mail collector robots 14	Block	1
212.143.124.12	Israel	147.237.0.120	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
87.68.254.48	Israel	147.237.0.120	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/ufi/reaction/	Block	1
104.171.124.84	United States	147.237.0.120	eMail Hoarding	Block	1
79.181.122.163	Israel	147.237.0.120	Distributed PHP Attempt	Block	1

11-02-2015 to 11-03-2015