

Measurement and Analysis of Hajime, a Peer-to-Peer IoT Botnet

Stephen Herwig Katura Harvey George Hughey Richard Roberts Dave Levin
 smherwig@cs.umd.edu katura@cs.umd.edu ghughey@terpmail.umd.edu ricro@cs.umd.edu dml@cs.umd.edu

IoT Botnets Pose a Major Threat

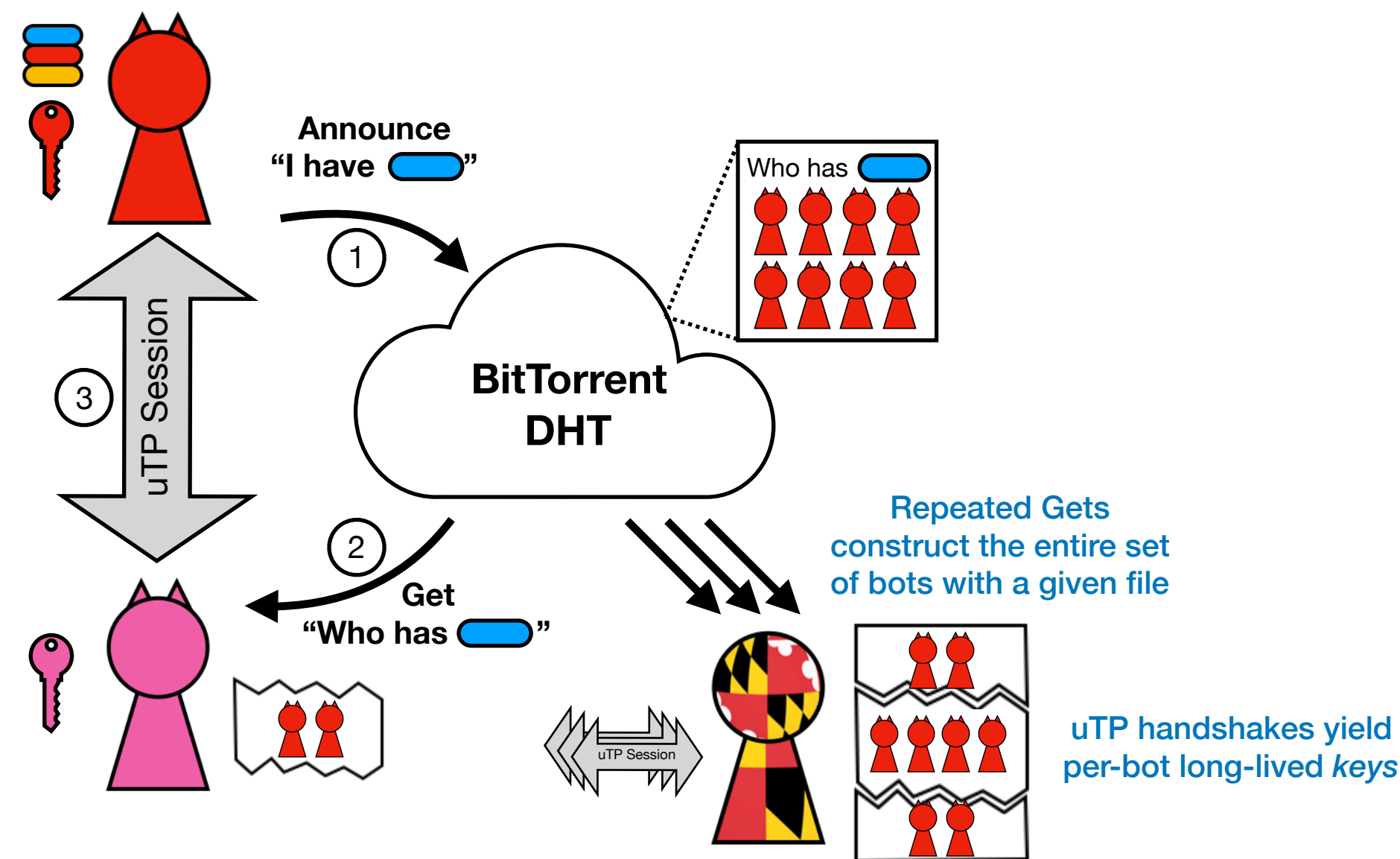
Mirai Largest DoS attacks in history

Hajime Mirai successor
 Runs on many architectures
 Regular updates, new exploits

We are longitudinally measuring Hajime

Goals To inform defenses and intervention:
 characterize steady-state behavior
 understand effect of new exploits on botnet

Hajime uses BitTorrent's DHT for Command-and-Control



Datasets

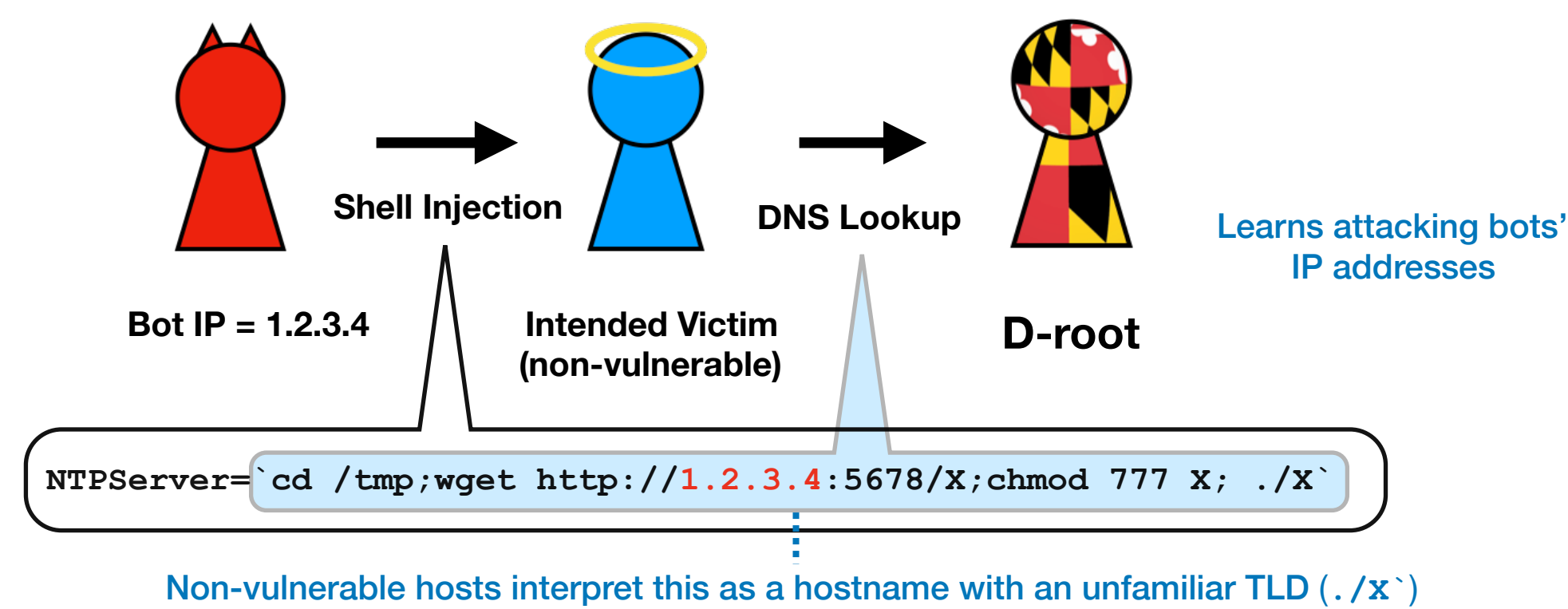
DHT Scans
 uTP Scans (10.5M keys)
 Binary reverse engineering (52 payloads)

DNS Backscatter (125M queries)

Exploits

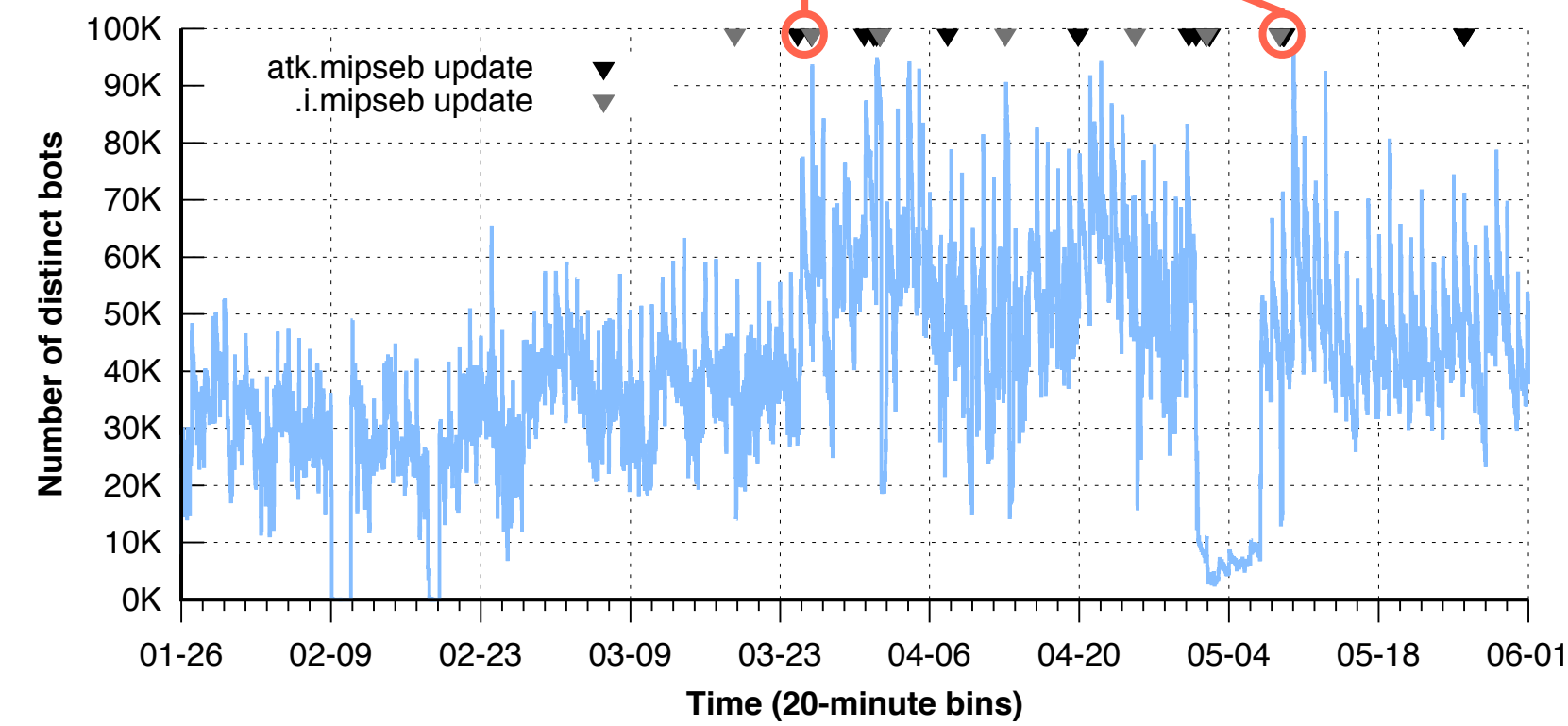
Chimay-Red
 GPON shell injection

TR-064 shell injection



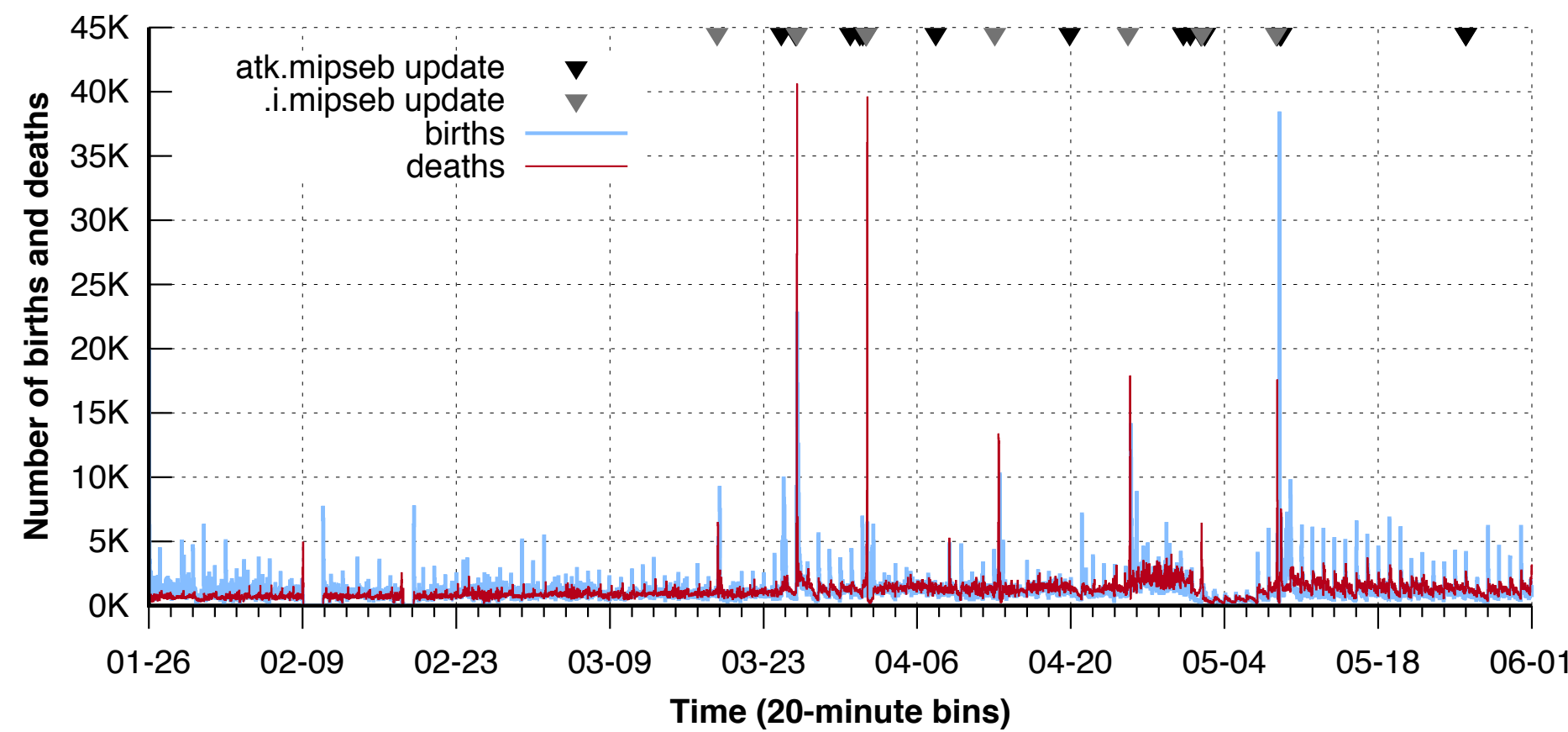
Botnet Size

Steady-state of ~40K bots
 Peaks of 95K after Chimay-Red and GPON exploits



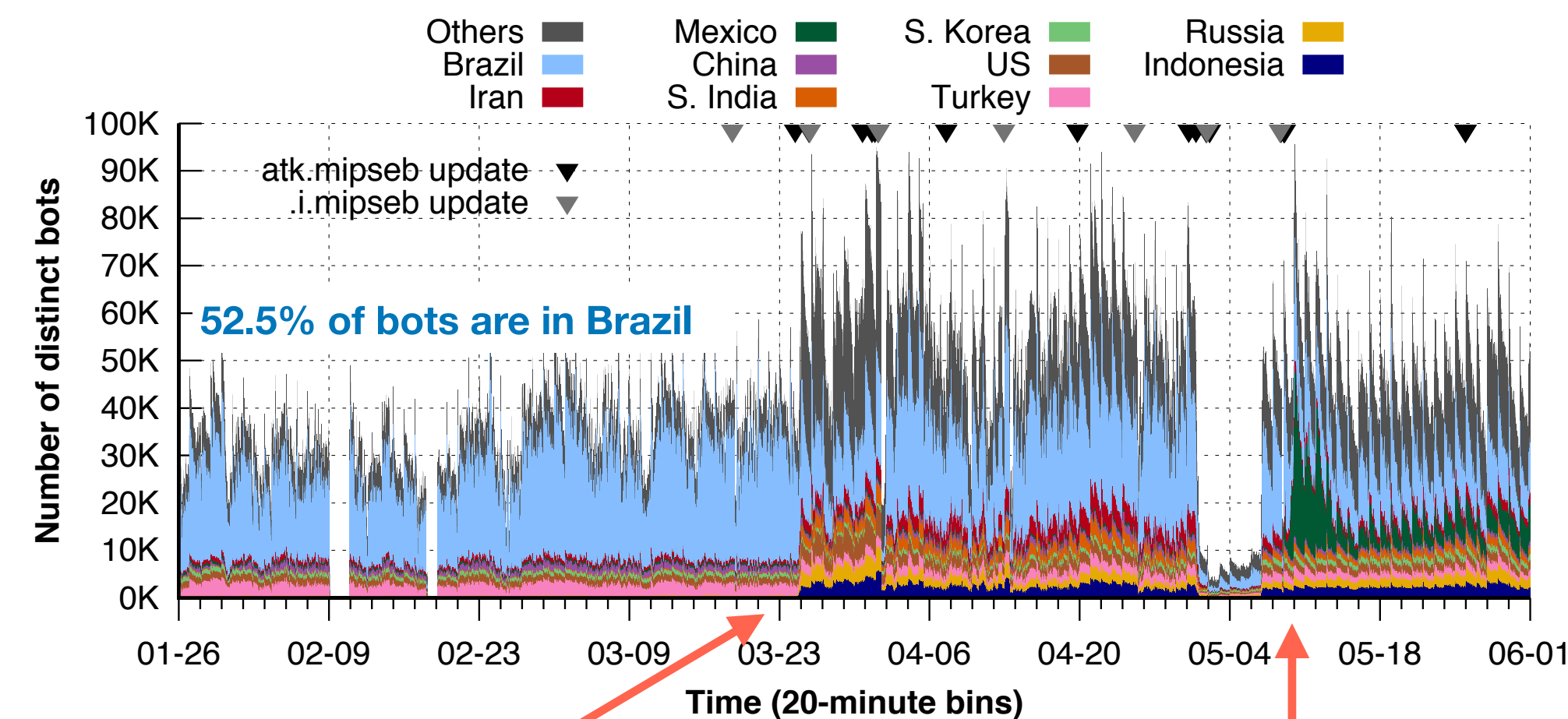
Churn

Median bot lifetime: 5 hours ⇒ Reboots and reinfections are common
 Steady-state churn: 2K



Location

The geographic makeup of IoT botnets can change rapidly



Russia goes from 500 active bots per hour to 6K following Chimay-Red.

The GPON exploit disproportionately affects Mexico

Devices

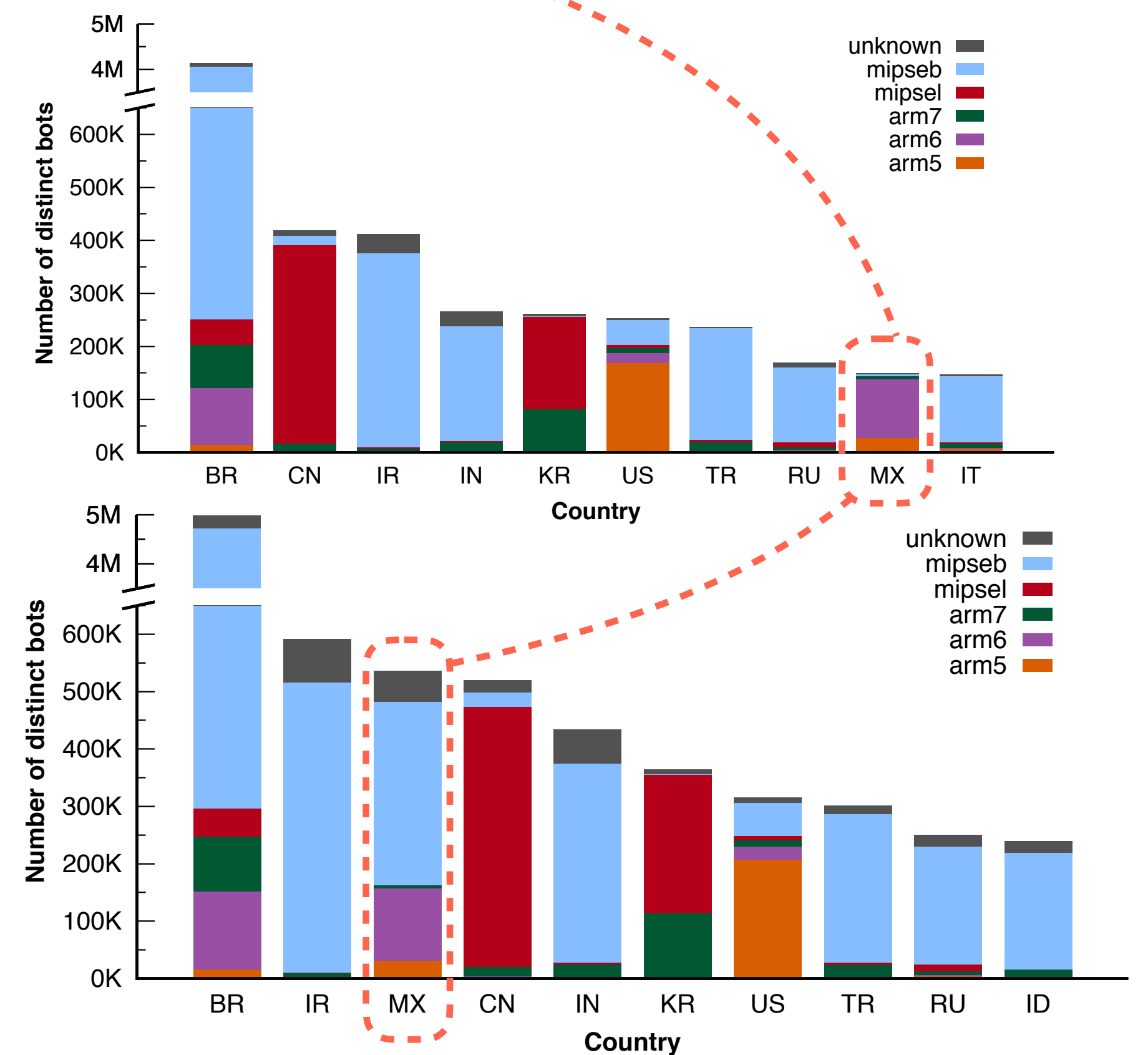
Devices overwhelmingly run MIPS

74.2% of bot devices are MIPS big endian.

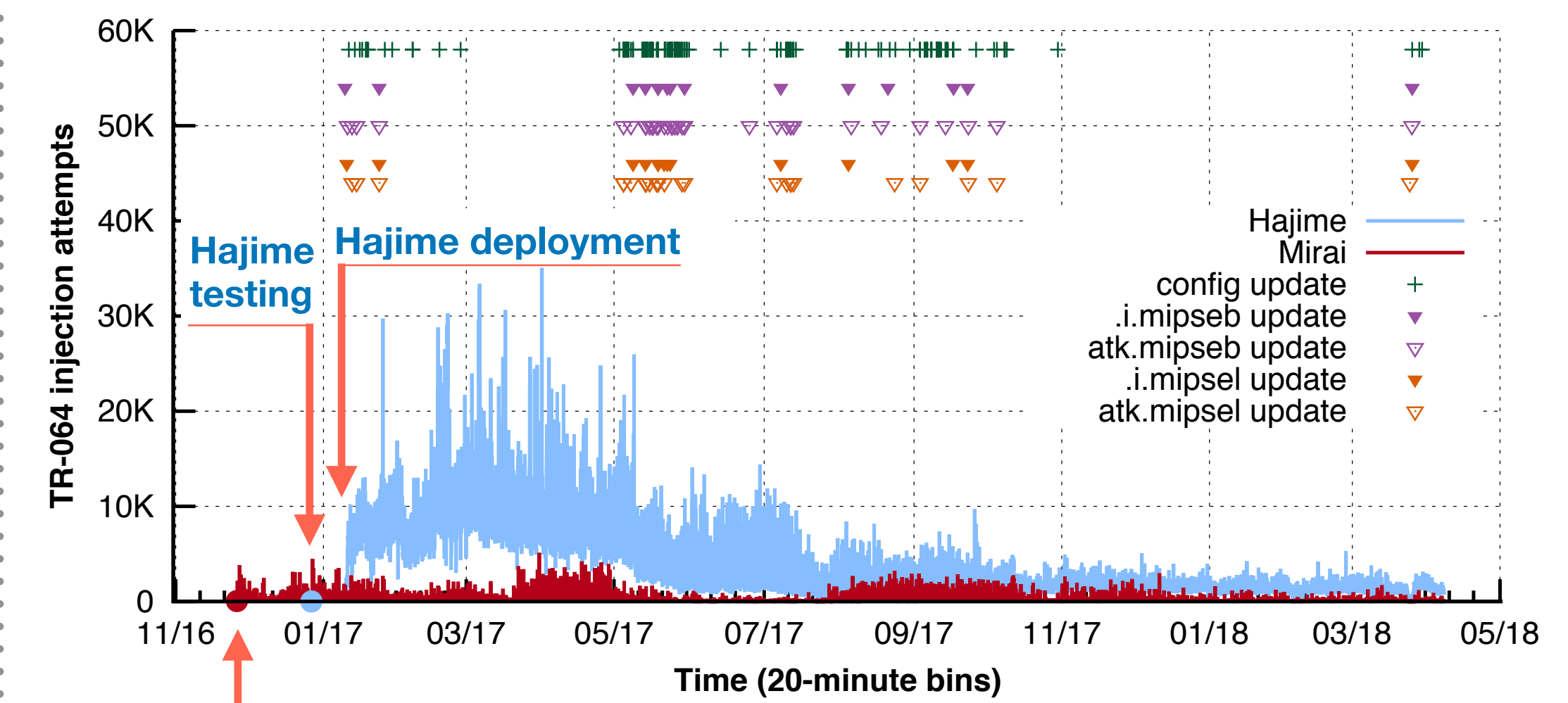
Exploit Effects

Chimay-Red increases proportion of MikroTik bots from 0.79% to 80.29%.

GPON exploit changes Mexico from primarily ARM to MIPS.



Evolution of TR-064 Exploit



Mirai deployment