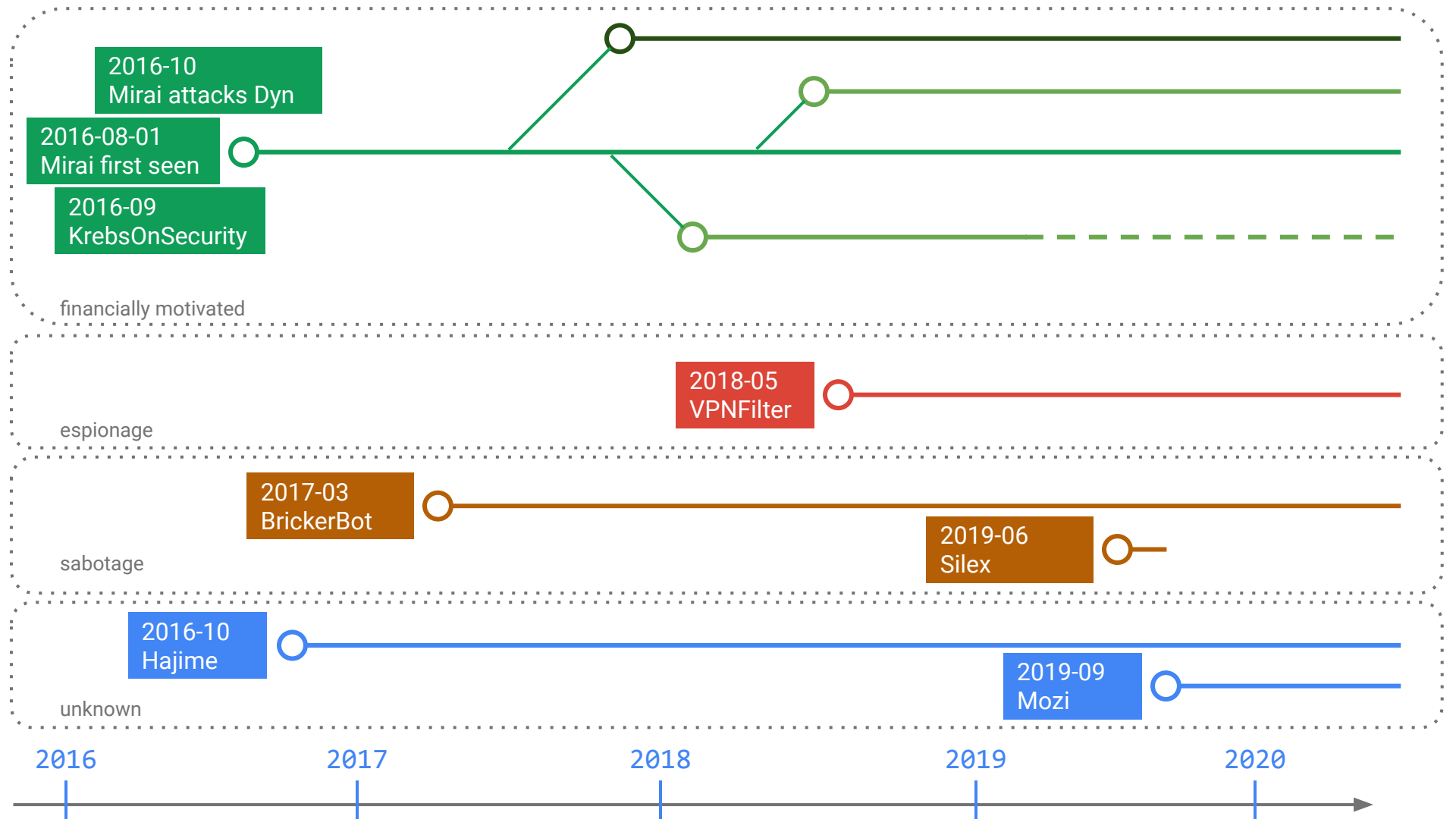
Westfälische Hochschule

A detailed look into the Mozi P2P IoT botnet

Botconf 2020

Christian Dietrich (@wavehackr), Andreas Klopsch (@hackingump1), Raphael Springer

Institute for Internet Security, Westphalian University, Germany
https://www.internet-sicherheit.de
https://chrisdietri.ch


2016-10
Mirai attacks Dyn
2016-08-01
Mirai first seen
2016-09
KrebsOnSecurity
financially motivated
2018-05
VPNFilter
espionage
2017-03
BrickerBot
2019-06
Silex
sabotage
2016-10
Hajime
2019-09
Mozi
unknown
2016
2017
2018
2019
2020

What is Mozi?

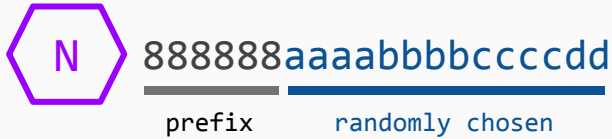
- Mozi key characteristics
  - Targets Linux-based IoT devices (MIPS LE and BE, ARM, PPC, likely also x86)
  - Exhibits unique P2P C2 comms using BitTorrent DHT protocol as carrier protocol
  - Superficially similar to Hajime, however clearly differs
  - The name ‘Mozi’ is based on filenames used in propagation

- First seen in September 2019
  - Initially publicly described by Alex Turing and Hui Wang of 360 in December 2019
  - Still actively developed, significant outbreak in September 2020

- Sample properties
  - Statically linked ELF binaries, µClibc
  - Custom UPX, header fields `p_filesize` and `p_blocksize` zeroed out as documented by Lars Wallenborn

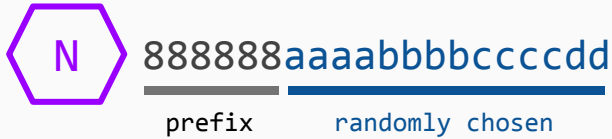
Mozi P2P C2 - Crawling

- BitTorrent DHT protocol
  - 20-byte node ID
  - XOR metric

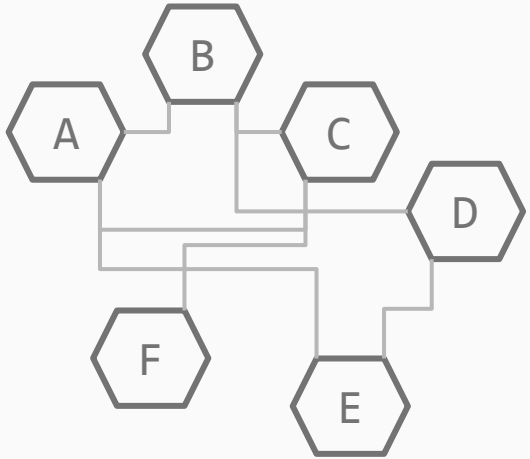


Mozi P2P C2 - Crawling

- BitTorrent DHT protocol
  - 20-byte node ID
  - XOR metric

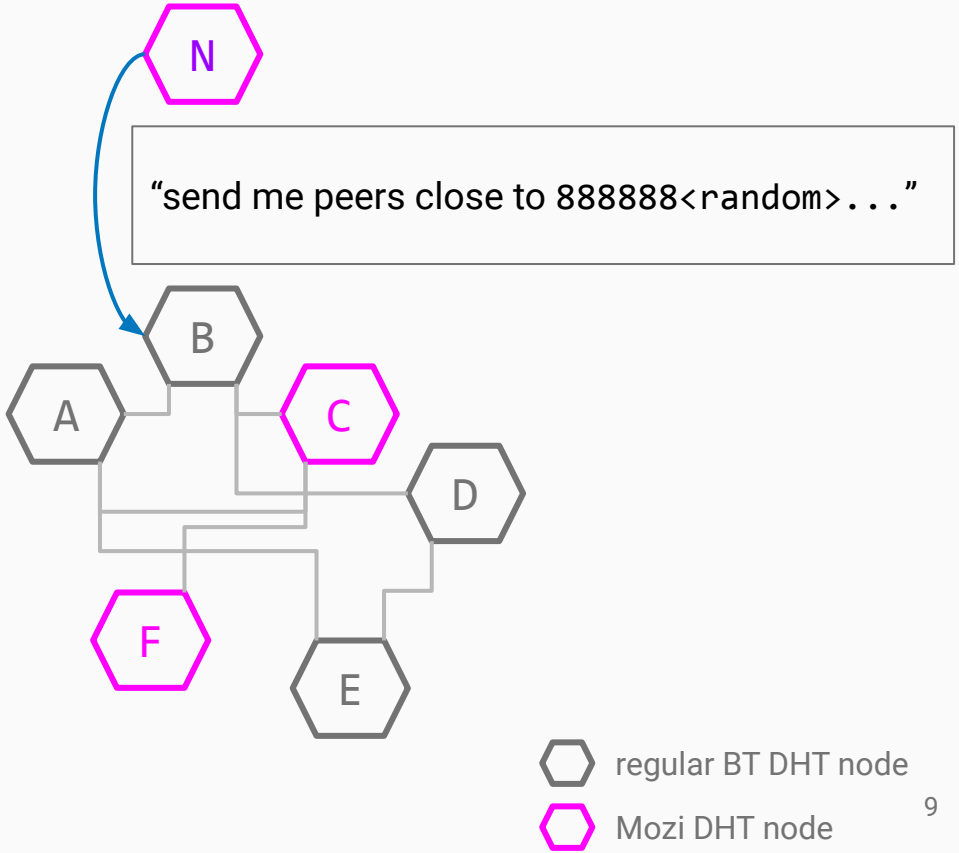


- Mozi DHT usage
  - Only two message types
    - peer list request (and response)
    - ping (and pong)
  - Gravitate around a node ID prefix, typically 888888



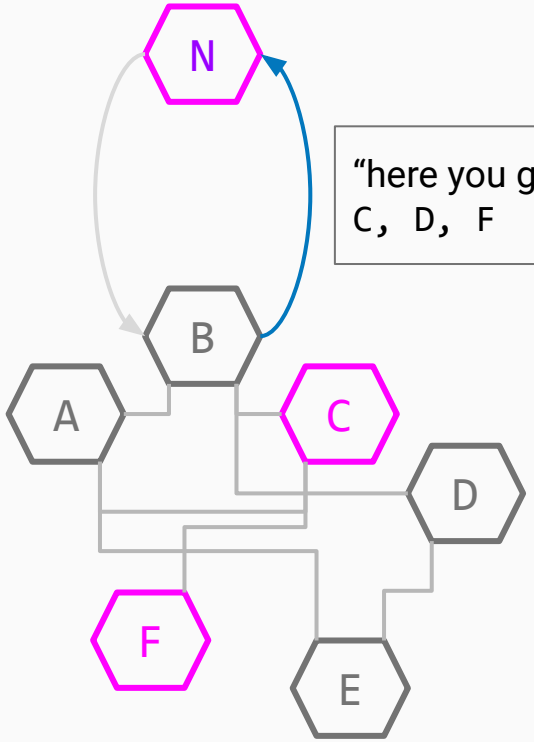
Mozi P2P C2 - Crawling

- BitTorrent DHT protocol
  - 20-byte node ID
  - XOR metric
- Mozi DHT usage
  - Only two message types
    - peer list request (and response)
    - ping (and pong)
  - Gravitate around a node ID prefix, typically 888888



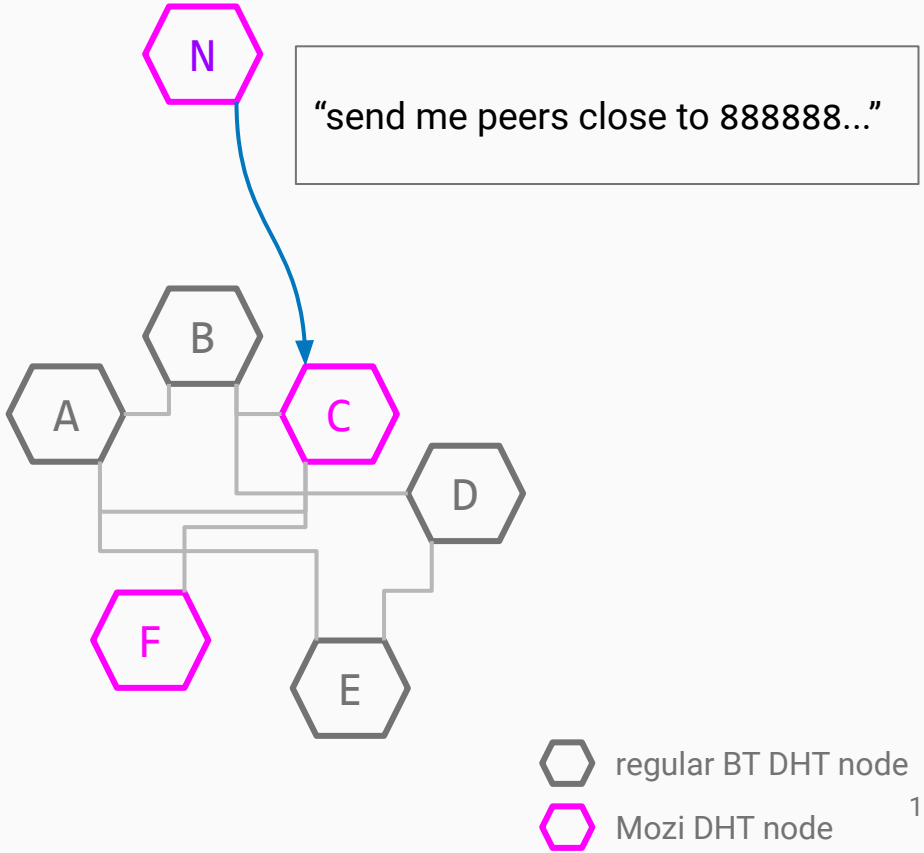
Mozi P2P C2 - Crawling

- BitTorrent DHT protocol
  - 20-byte node ID
  - XOR metric
- Mozi DHT usage
  - Only two message types
    - peer list request (and response)
    - ping (and pong)
  - Gravitate around a node ID prefix, typically 888888



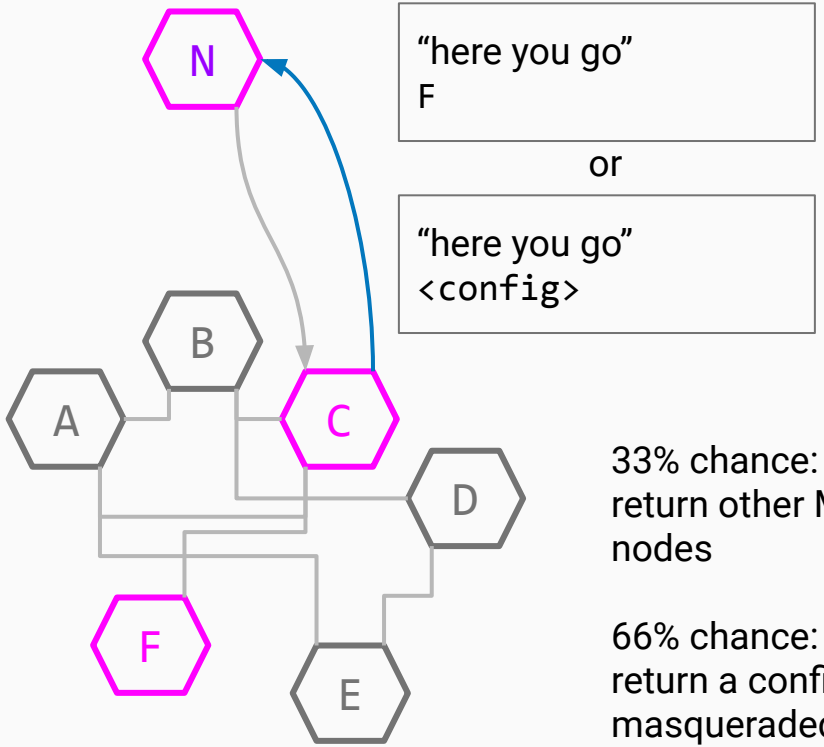
Mozi P2P C2 - Crawling

- BitTorrent DHT protocol
  - 20-byte node ID
  - XOR metric
- Mozi DHT usage
  - Only two message types
    - peer list request (and response)
    - ping (and pong)
  - Gravitate around a node ID prefix, typically 888888



Mozi P2P C2 - Crawling

- BitTorrent DHT protocol
  - 20-byte node ID
  - XOR metric
- Mozi DHT usage
  - Only two message types
    - peer list request (and response)
    - ping (and pong)
  - Gravitate around a node ID prefix, typically 888888
- Based on open source DHT library
  - Dht-bootstrap by Chroboczek
  - Initially published in 2009



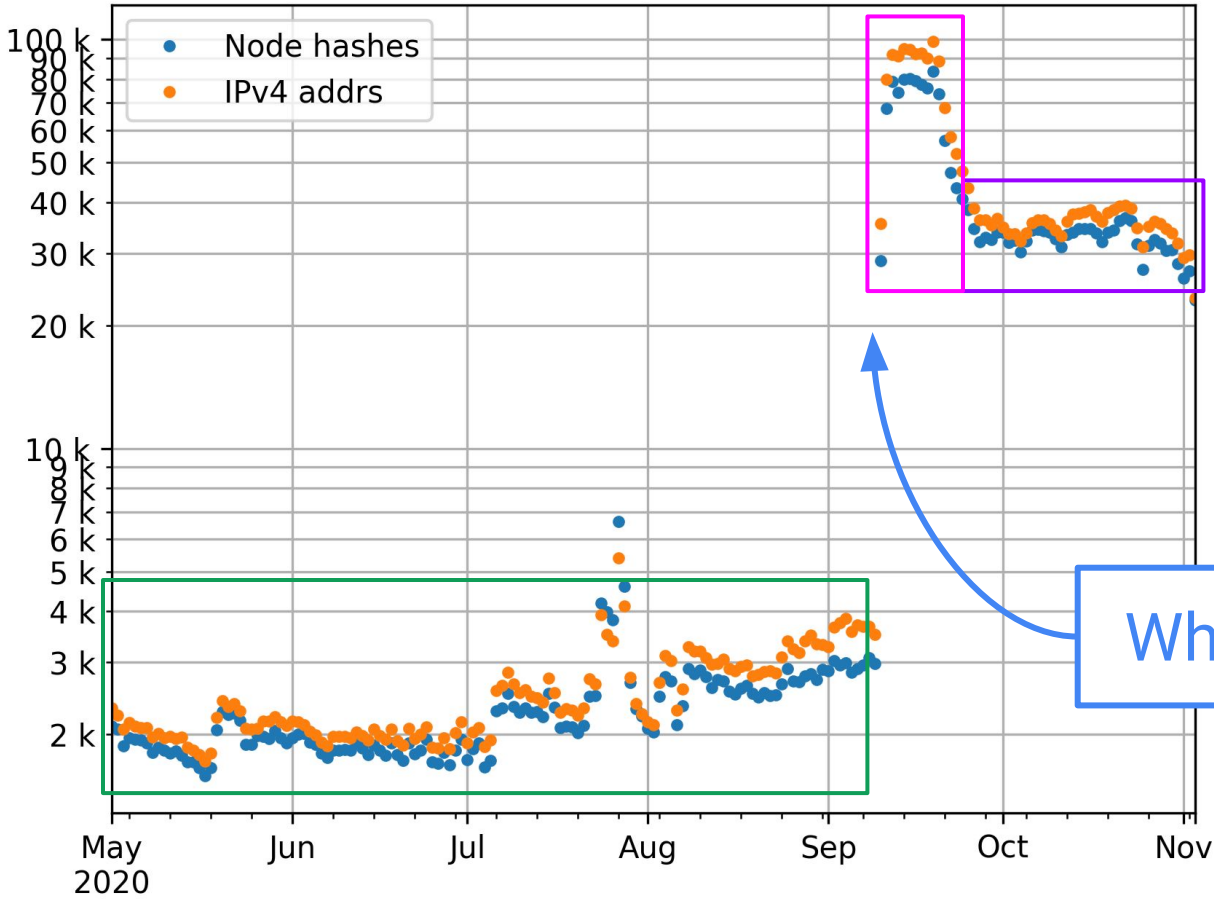
33% chance: return other Mozi nodes

66% chance: return a config, masqueraded as peerlist response

Mozi configuration and capabilities

Filter	`[cpu] / [cpux]`	Filter by CPU architecture
	`[ss] / [ssx]`	Filter by bot role (e.g., `ftp, sns, bot, botv2, sk, ssh`)
	`[sv]`	Propagate config; if set to 0 the config will not be propagated
Maintenance	`[hp]`	DHT node ID prefix, e.g. 888888
	`[nd]`	Set DHT bootstrap nodes
	`[count]`	Update the URL for infection reporting
	`[dip]`	Update the URL which serves a Mozi sample
	`[ver]`	Set the generation (version)
Capabilities	`[atk]`	Perform a DDoS attack
	`[ud]`	Update the executable from the given URL
	`[dr]`	Download and execute a signed payload from the given URL
	`[rn]`	Execute a command via shell or `system()`
	`[idp]`	Report system information to a given URL
	`[hj]`	Control network traffic manipulation

Mozi botnet population



- Botnet population
  - until 2020/07
    2.5k to 4k nodes
  - September 2020
    80k to 100k nodes
  - recently
    25k to 35k nodes

What happened here?

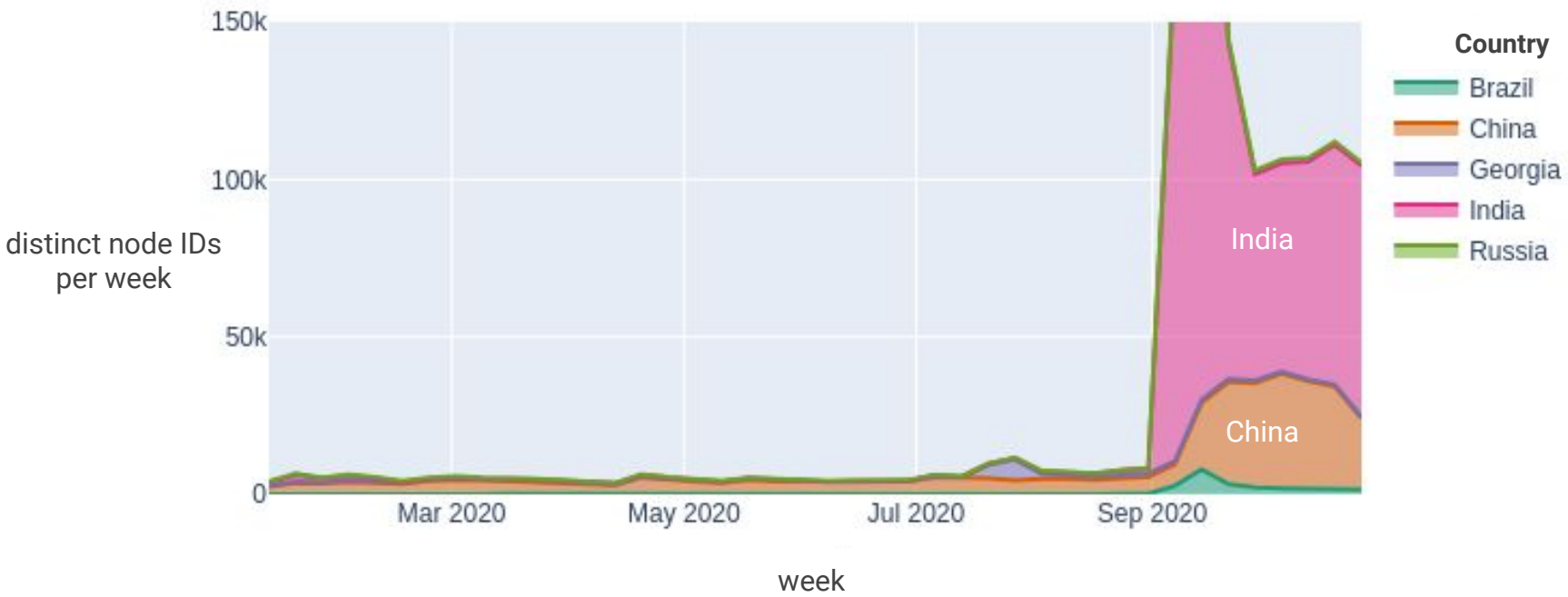
Mozi propagation

- Exploits
  - 14 HTTP-based exploits for web interfaces of IoT devices
  - Unchanged over time
- Telnet credentials
  - Hardcoded lists of login prompt patterns, usernames and passwords
  - Extended over time
  - Likely cause for spike in September 2020: New credentials added


```
BrAhMoS@15
```

BrahMos: medium range cruise missile, developed by a Russian-Indian joint venture

Population shift across countries

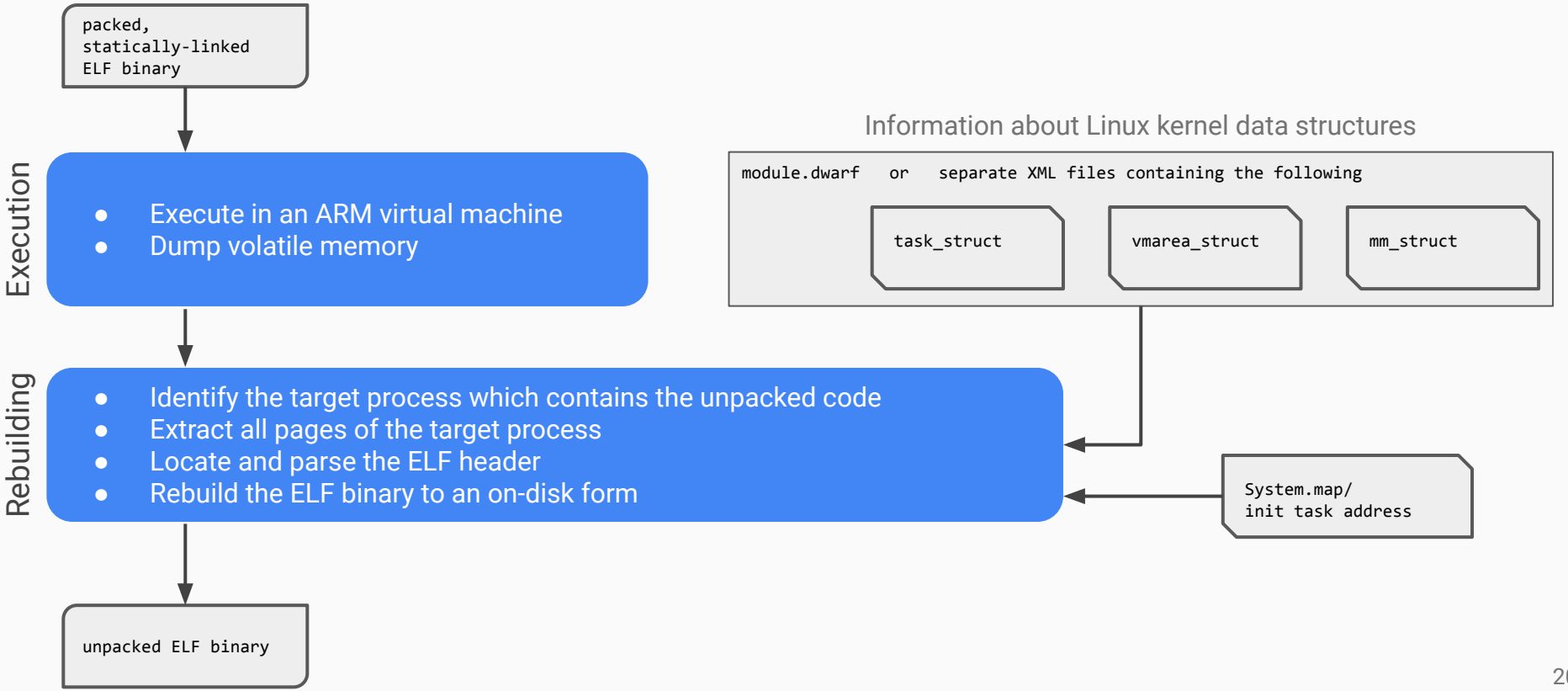


Unpacking ELF samples on ARM

- Dynamically unpacking samples
  - Unpacking PE samples on Windows is practically solved
    - See https://www.unpac.me/ by OpenAnalysis

- We address dynamic unpacking ELF on ARM
  - Packing appears to become more popular for Linux/IoT malware
  - Goal: Have a service up and running at https://iot.if-is.net by end of 2020

Unpacking ELF samples on ARM



Open issues

- No attack observed so far
  - Possibly a visibility issue
  - Specific nodes may be tasked individually
  - Configs can be marked to not propagate
  - Hajime: No attack seen in years
- Interesting functionality
  - Network traffic manipulation
  - Ongoing development

Acknowledgements

- URLhaus, abuse.ch
- The ShadowServer foundation
- ICS CERT of CNCERT
- Netlab 360.com
- Norman Schmidt

Thank you.

Christian Dietrich, Andreas Klopsch, Raphael Springer