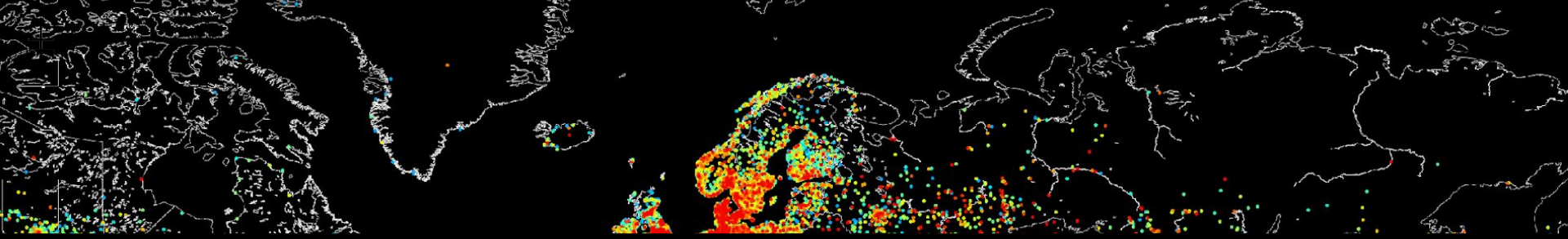


Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai

Orçun Çetin[*,±], Carlos Gañán[*], Lisette Altena[*], Takahiro Kasama[***], Daisuke Inoue[***], Kazuki Tamiya[**], Ying Tie[**], Katsunari Yoshioka[**] and Michel van Eeten[*]

Delft University of Technology, Delft, the Netherlands*
University of Kent, Canterbury, England±
Yokohama National University, Yokohama, Japan**
National Institute of Information and Communications Technology, Tokyo, Japan***

TU Delft

Mirai: The IoT Bot that Took Down Krebs and Launched a Tbps Attack on OVH

ARTICLE • 6 min. read

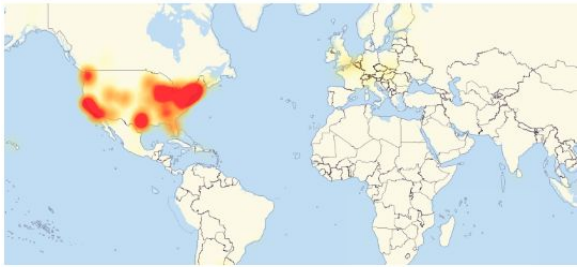
By Liron Segal

Briton who knocked Liberia offline with cyber attack jailed

Dominic Casciani
Home affairs correspondent
@BBCDomC

Massive Mirai DDoS Attack 'Breaks The Internet'

Posted on October 24, 2016 by Jeff Edwards in Endpoint Security News

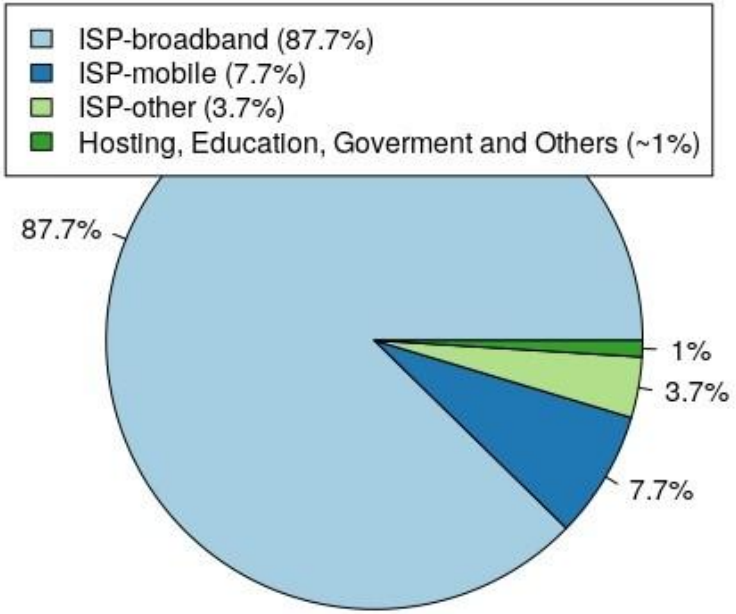


Outage map via downdetector.com

TU Delft

Where Are These Mirai Infected Devices?

- Majority of these of the infected devices (87.61%) are located in ISP broadband networks
- Only 1% reside in other types of networks including hosting, education or governmental networks

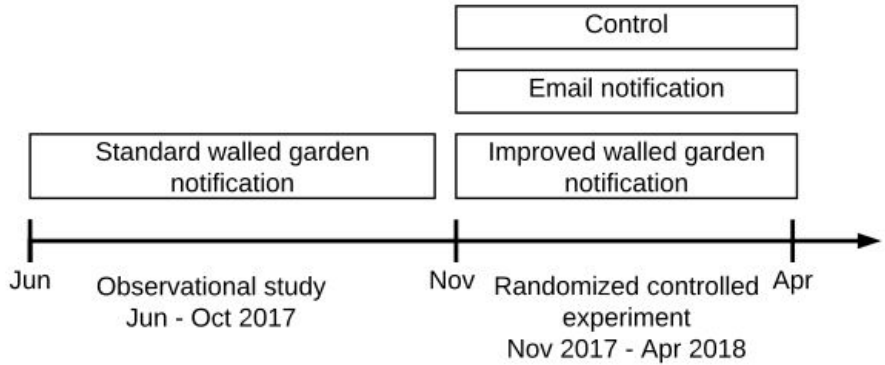


How Can We Remediate Compromised IoT devices?

- There are 3 critical challenges:
  - no public information to identify the owner of the device
  - no established communication channel to reach the owner
  - no clear and simple remediation path or notification
- ISPs can identify and notify the customers who own vulnerable and compromised devices
- But how effective would this be ?

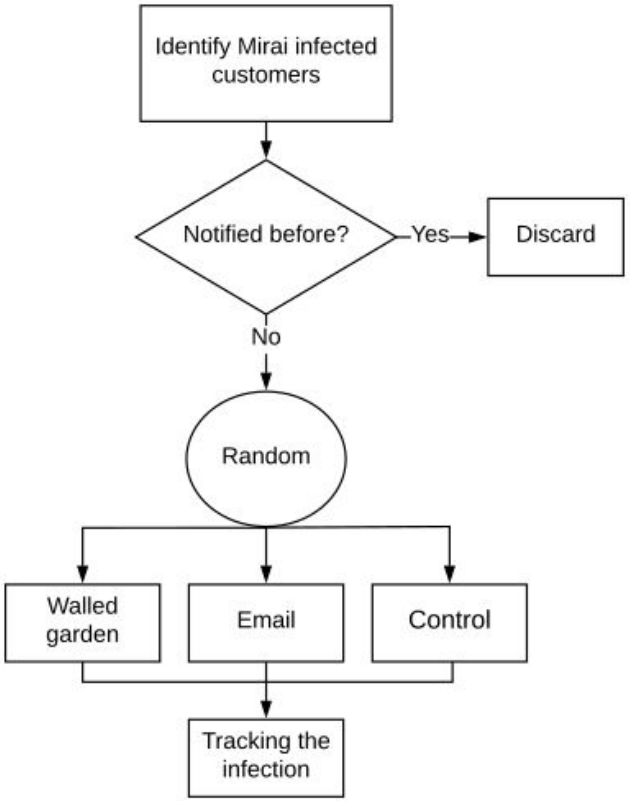
ISP IoT Cleanup Experiments

- Mid-size European ISP
- Two type of studies
  - Observational study
  - Randomized control experiment
- 220 customers



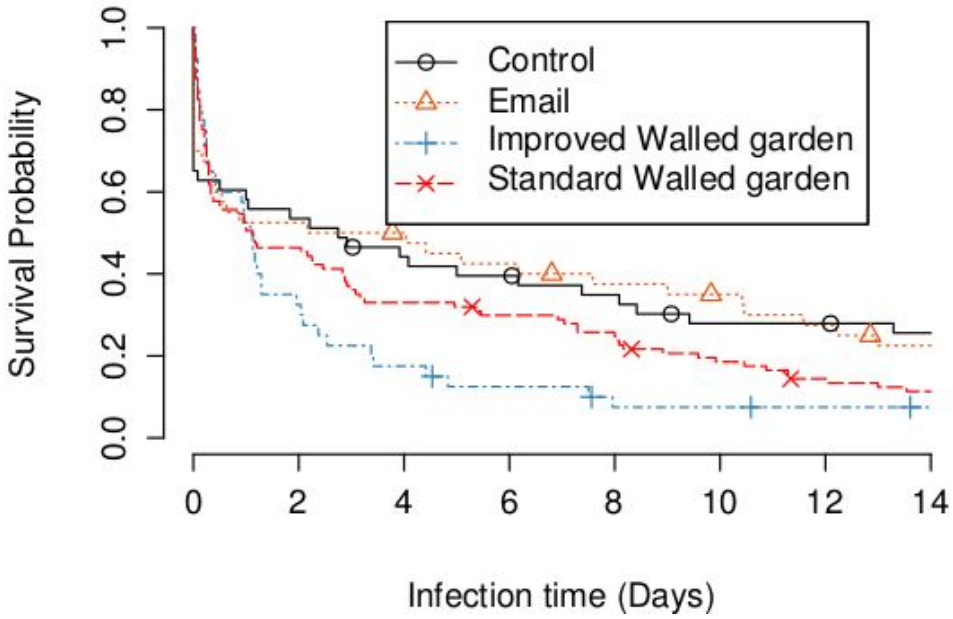
Randomized Control Experiment

- 2 Type of notifications
  - Email
  - Walled garden
- Detecting infections
  - Shadowserver drone feed
  - IoT honeypot
- Tracking infections
  - Darknet
  - Shadowserver drone feed
  - IoT honeypot



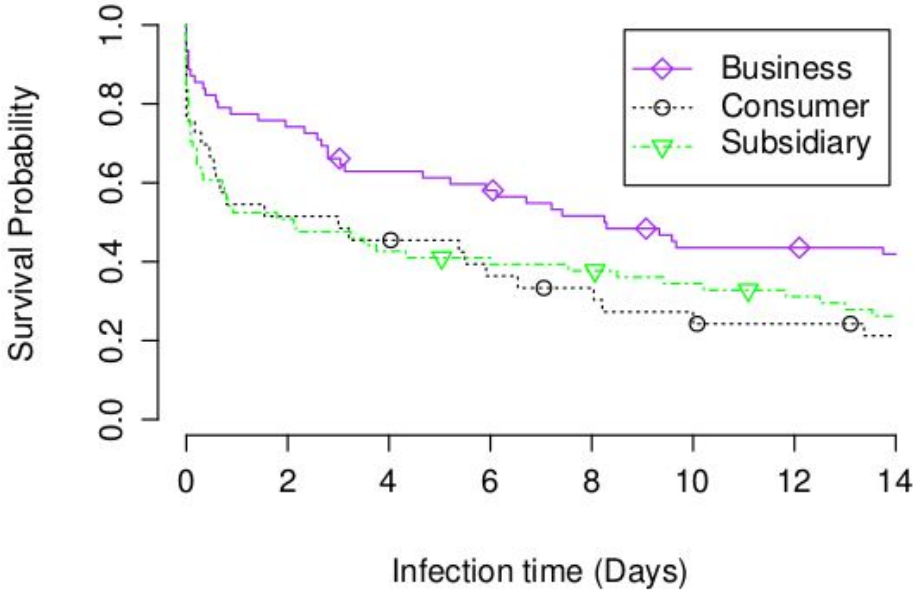
Impact of the Notifications

- Improved walled garden achieved 92% remediation
- Standard walled garden achieved 88% remediation
- Email has no observable impact



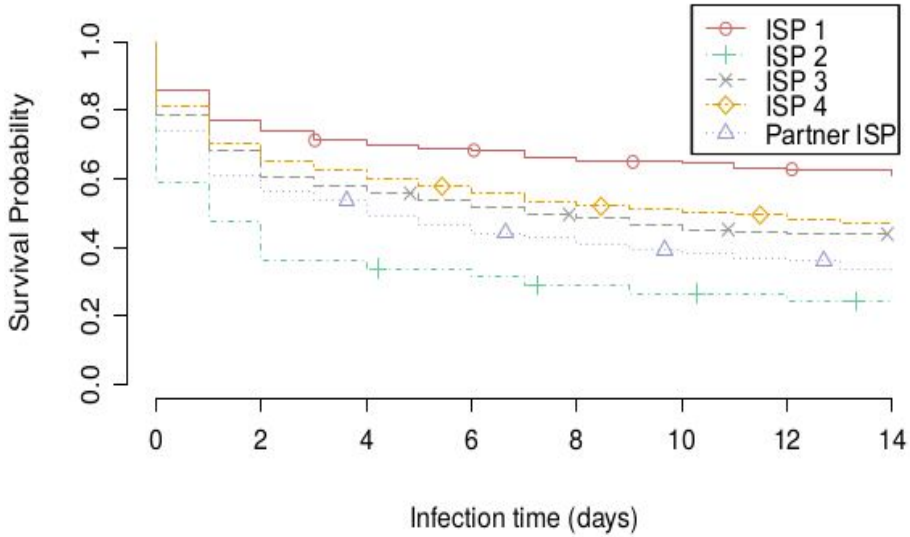
Natural Remediation In Other Networks

- No notifications are made
- Natural remediation is present in all other networks
- Infections live longer in business network



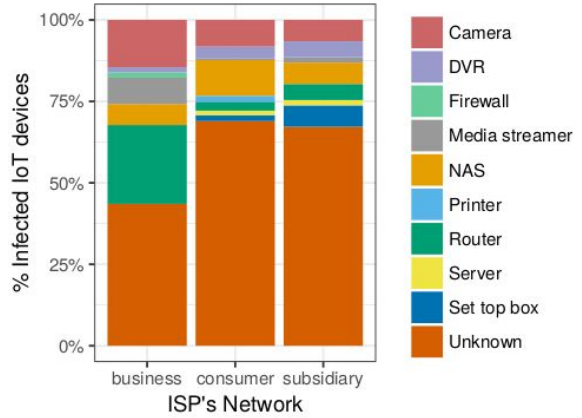
Natural Remediation In Other ISPs

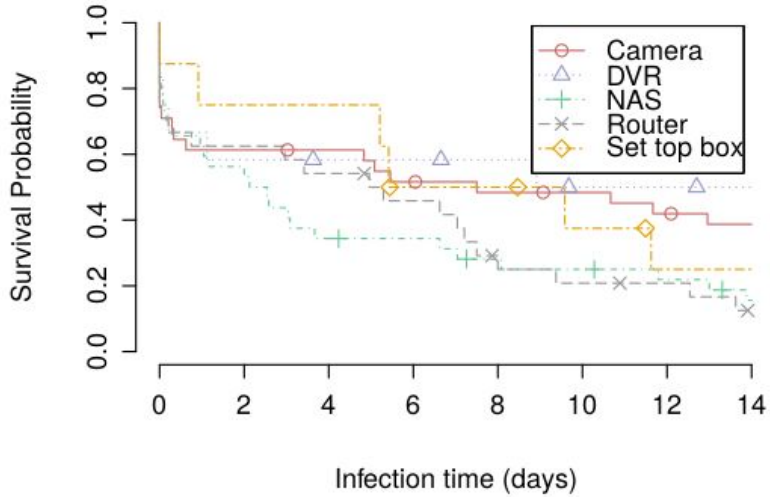
- 4 randomly chosen ISPs within the same country
- Natural remediation is visible in all ISPs



Impact of Device Type

- Not many devices are identified via scans
- Routers cleanup faster than DVRs and cameras





User experience - Phone interviews

- 76 (44%) participants
- Only 50% of the email group remember receiving the notification
- All confirmed correct email address used
- No distrust towards Improved walled garden notifications

Experimental group	Total	Received		Read		Distrust	
Email-only	16	8	(50.00 %)	6	(37.50 %)	2	(12.50 %)
Walled garden (improved)	18	18	(100 %)	18	(100 %)	0	(0.00 %)
Walled garden (standard)	42	40	(95.20 %)	36	(85.70 %)	6	(14.80 %)

User experience - Communication logs

- Only 7.5% of the email group contacted help desk
- Versus 45-52% for walled garden groups
- Lower or higher rate of seeking help is related to clean up action

Experimental group	n	email	contact form	helpdesk
Email-only	40	16 (40.0%)	–	3 (7.5%)
Walled garden (improved)	40	23 (57.5%)	31 (77.5%)	21 (52.5%)
Walled garden (standard)	97	67 (69.1%)	59 (60.8%)	44 (45.4%)

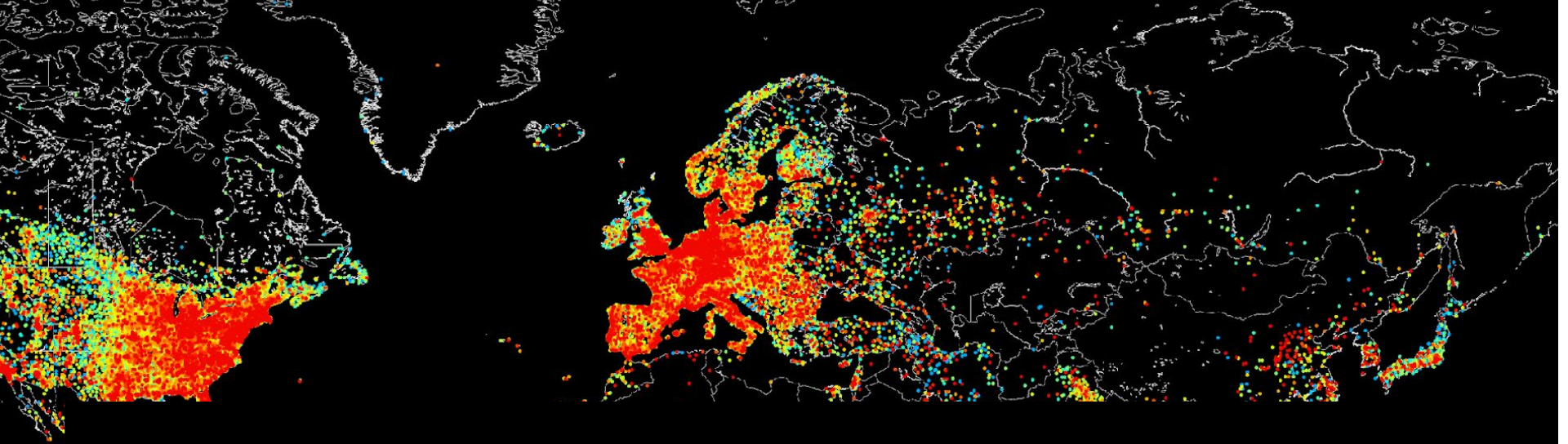
User experience - Communication logs

- Incorrect mental model of the problem
- Improved walled garden reduced the need for additional help
- Less complaints while in improved wall garden

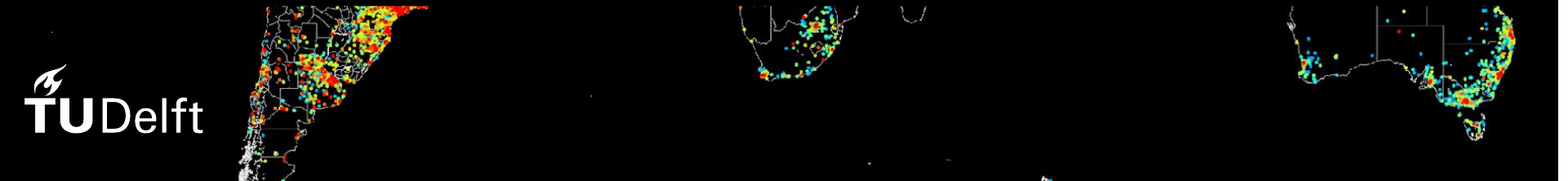
	Email-only	Walled garden (improved)	Walled garden (standard)
	n=40	n=40	n=97
Runs a virus scanner	7 (17.5%)	12 (30.0%)	32 (33.0%)
Identifies IoT device	9 (22.5%)	17 (42.5%)	58 (59.8%)
Requests additional help	2 (5.0%)	8 (20.0%)	41 (42.3%)
Wants possibility to call the abuse team	0 (0.0%)	2 (5.0%)	16 (16.5%)
Requests paid technician	0 (0.0%)	4 (10.0%)	11 (11.3%)
Disconnects device	3 (7.5%)	15 (37.5%)	42 (43.3%)
Cannot work due to quarantine	0 (0%)	4 (10.0%)	18 (18.6%)
Complaints over disruption of service	0 (0%)	1 (2.5%)	13 (13.4%)
Threatens to terminate contract	0 (0%)	1 (2.5%)	5 (5.2%)

Conclusions

- Improved walled garden remediates 92%
- Email has no observable impact above natural remediation
- High natural remediation across ISPs and networks
- Improving the content reduces the complaints to small but vocal minority that was angry or frustrated
- As more people will become aware of the threats to their IoT devices, ISP mitigation might become more accepted – or even expected



Thank you for listening!
Any questions?
Contact: f.o.cetin@tudelft.nl | f.o.cetin@kent.ac.uk



TU Delft