User Compliance and Remediation Success After IoT Malware Notifications

Elsa Rodríguez, Susanne Verstegen, Arman Noroozian, Daisuke Inoue,
Takahiro Kasama, Michel van Eeten, Carlos Gañán.

RIPE83 Virtual Meeting
November 23rd, 2021

Agenda

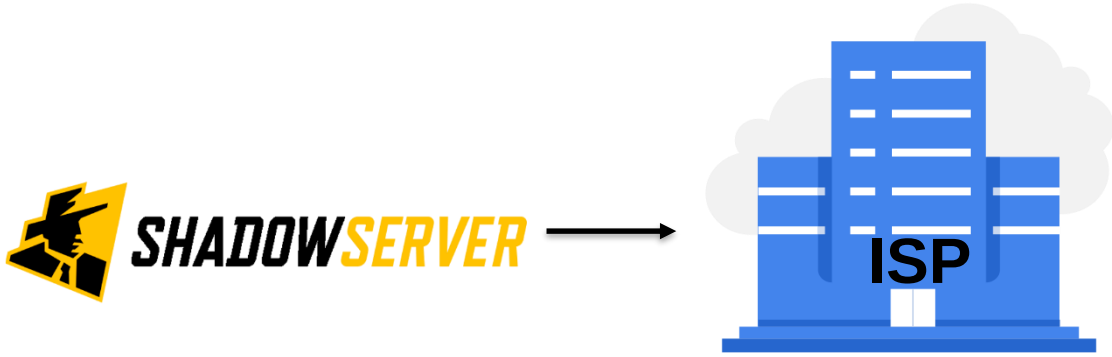
- Background
- Methodology
- Results
- Limitations
- Takeaways

TU Delft

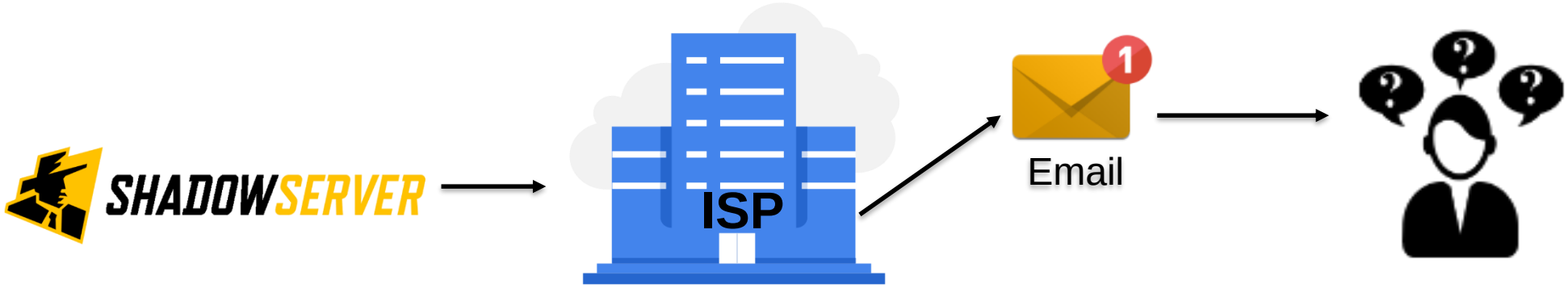
Background

- Attacks to IoT devices keep increasing and evolving.
- RFC6561 – ISPs should notify users (email, quarantaine).
- Notifications rely on users intervention.
- Mirai as case of study with a partner ISP and its subsiadiry.

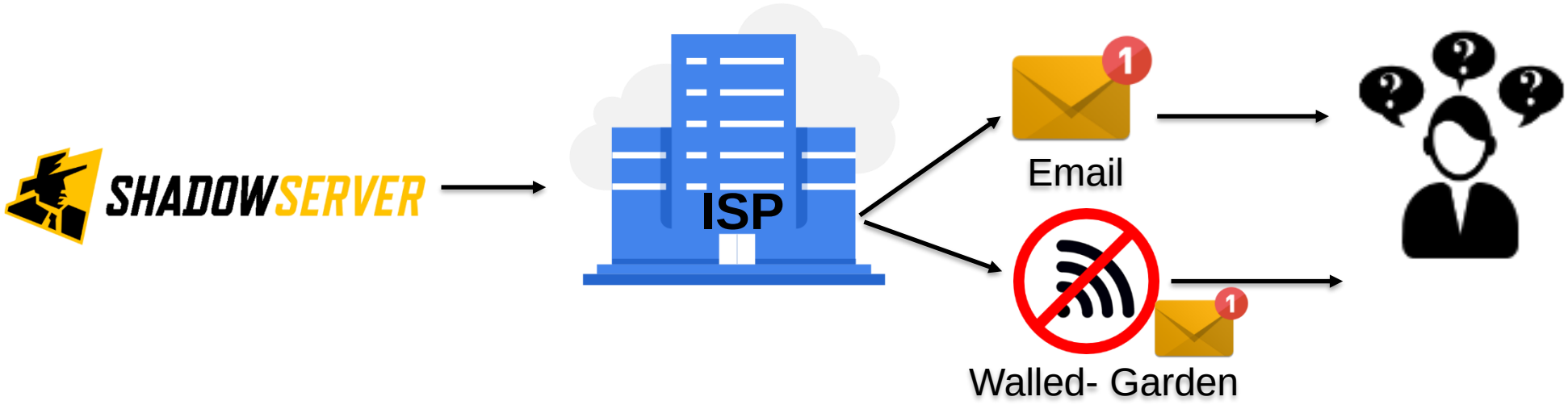
ISP Notification – recommended steps



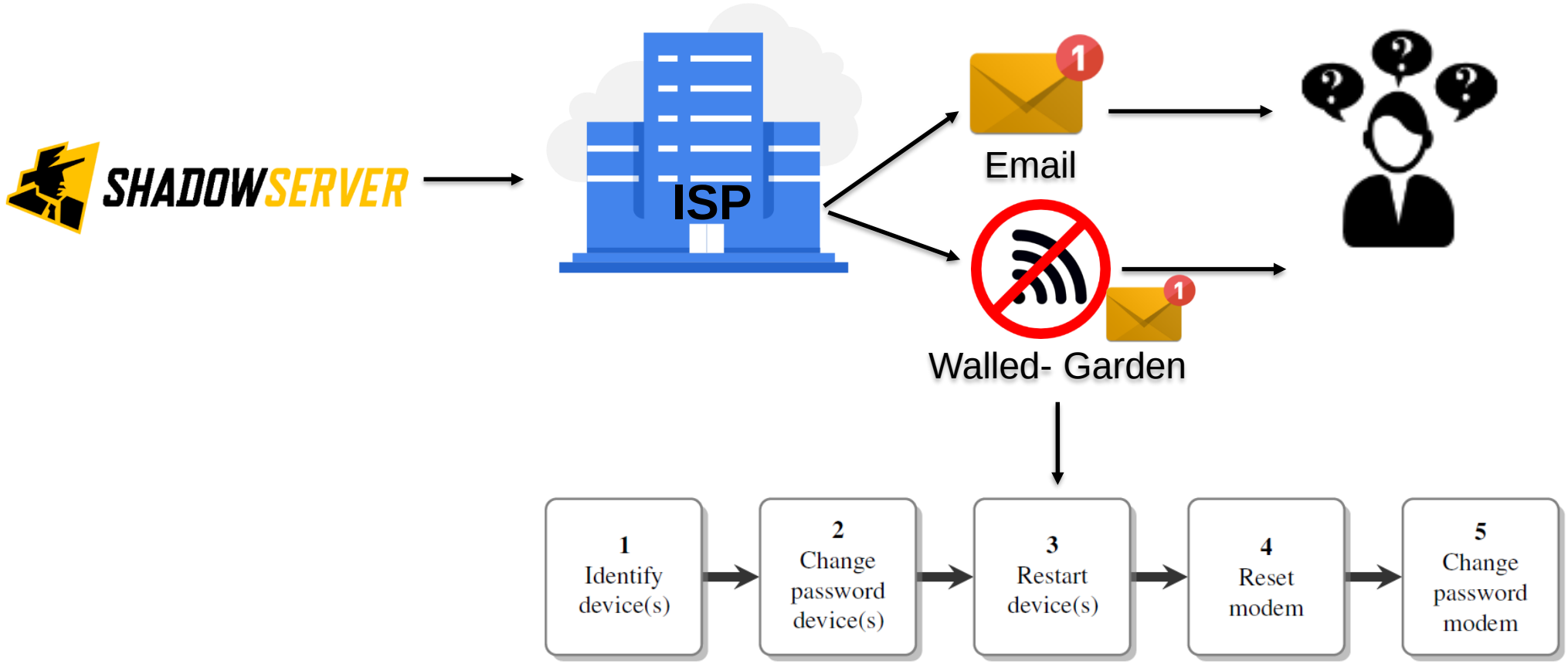
ISP Notification – recommended steps



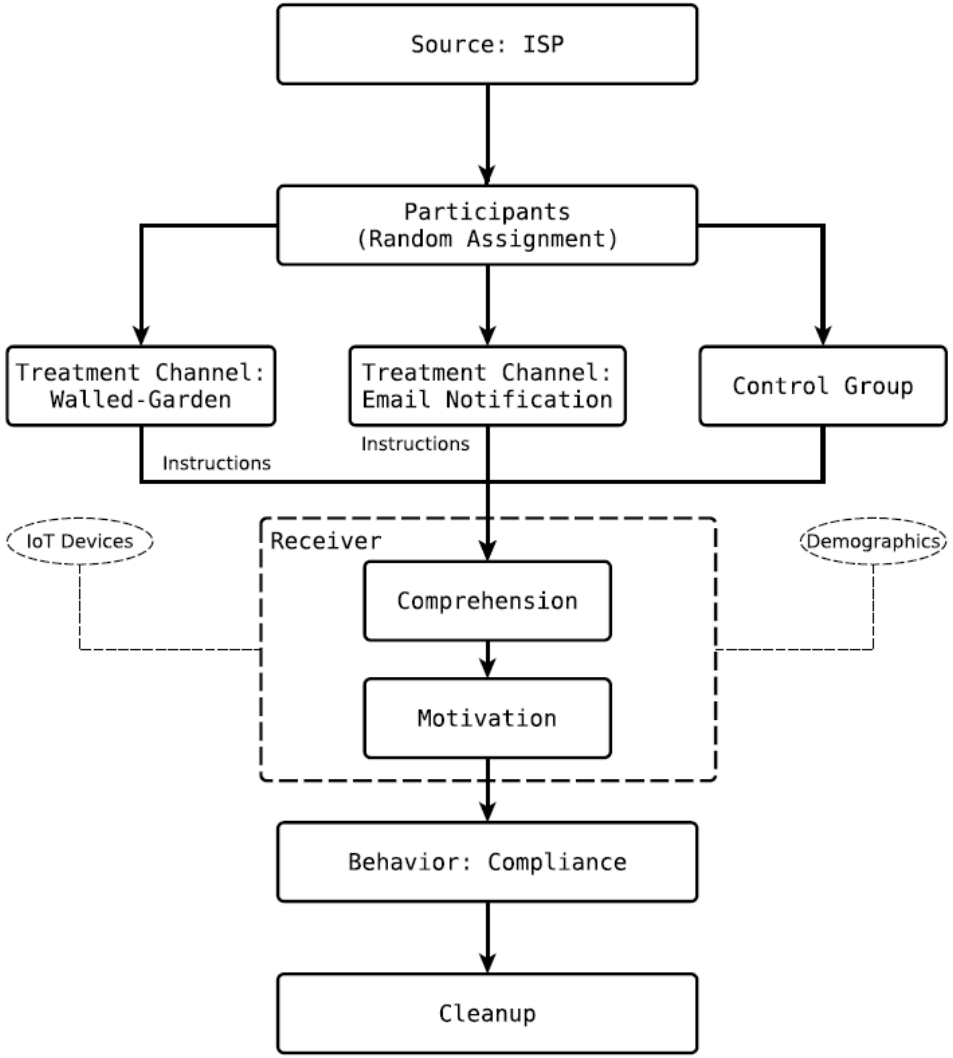
ISP Notification – recommended steps



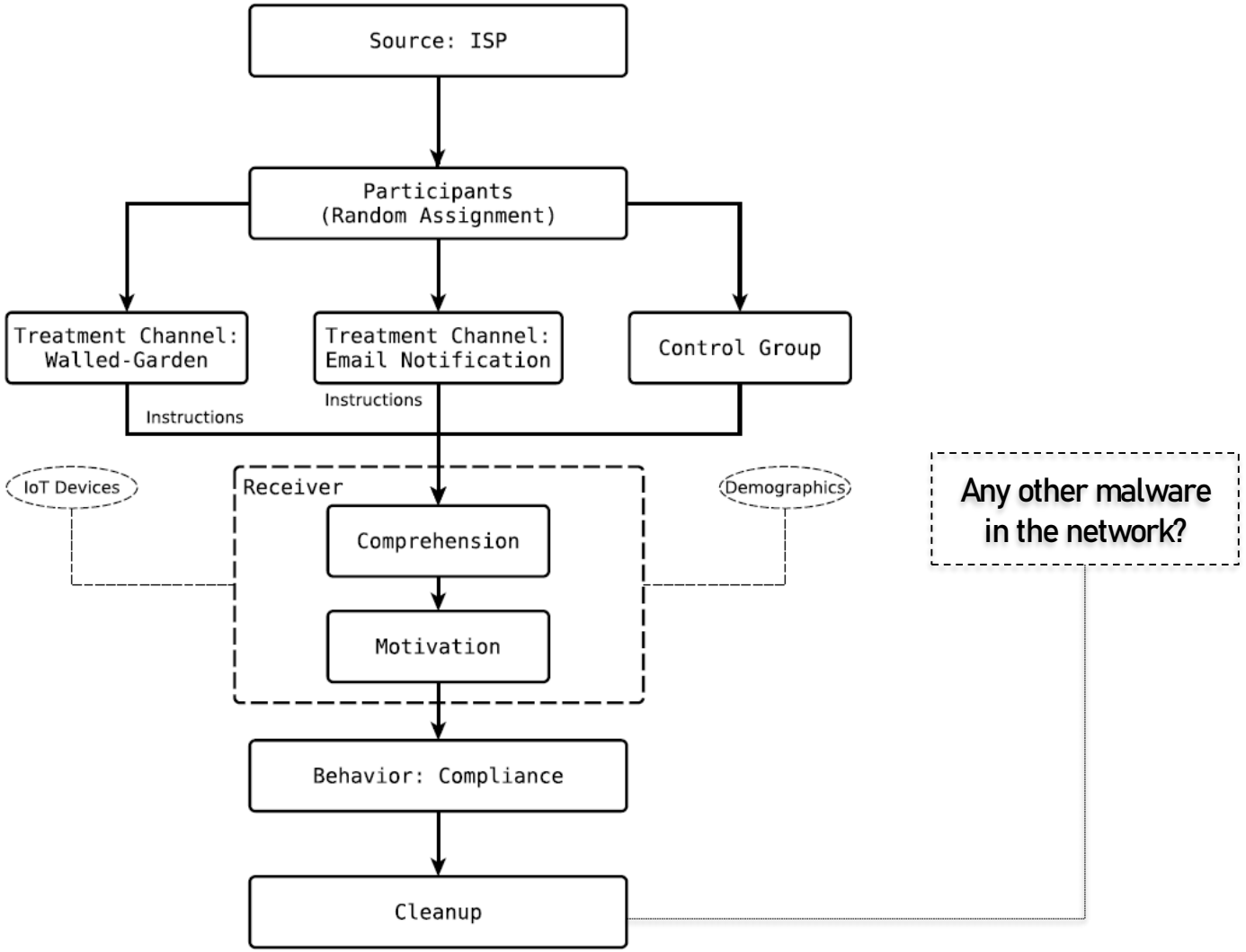
ISP Notification – recommended steps



Methodology



Methodology



Consumers' interviewed

Group		Control	Email	Walled Garden	Total
ISP	Participants	85	–	43	128
	Interviewed	35 (41%)	–	28 (65%)	63 (49%)
Subsidiary	Participants	17	16	16	49
	Interviewed	10 (59%)	11 (68%)	11 (65%)	32 (65%)
Total	Participants	102	16	59	177
	Interviewed	45 (44%)	11 (68%)	39 (66%)	95 (54%)

Comprehension

Walled-garden:

- 37 out of the 39 users (95%) remember receiving and reading the notification.
- 25 out of the 37 users (67.5%) indicated they understood the notification.

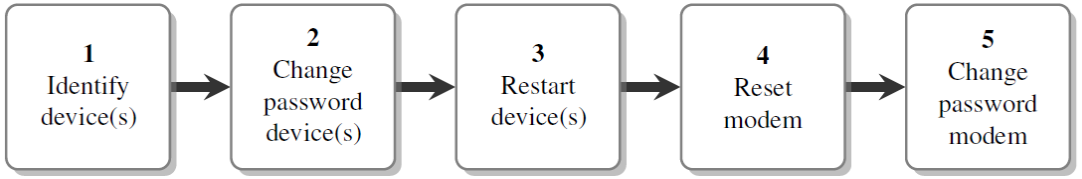
Email:

- 9 out of the 11 (82%) remember receiving and reading the notification.
- 8 out of the 9 (88%) indicated they understood the notification.

Motivation

Treatment	Motivation	No. Consumers
Email-only	Safe internet is important	7 (78%)
	Malfunctioning device	1 (11%)
	No answer	1 (11%)
Walled garden	Internet back	19 (51%)
	Internet back & Safe internet is important	9 (24%)
	Safe internet is important	3 (8%)
	No answer	3 (8%)
	Malfunctioning device	1 (3%)
	Need the device	1 (3%)
	Privacy concern & safe internet	1 (3%)

Self- reported compliance



	Followed Steps					
Group	**1**	**2**	**3**	**4**	**5**	**Freq.**
Walled Garden	0	0	0	0	0	2
	1	0	0	0	0	9
	1	0	0	1	0	1
	1	0	0	1	1	4
	1	0	1	0	0	1
	1	0	1	1	0	3
	1	0	1	1	1	1
	1	1	0	0	0	2
	1	1	0	1	1	1
	1	1	1	0	0	3
	1	1	1	0	1	1
	1	1	1	1	0	2
	1	1	1	1	1	9
Email	0	0	0	0	0	2
	1	0	0	0	0	1
	1	0	0	1	0	1
	1	0	0	1	1	1
	1	1	1	0	0	1
	1	1	1	0	1	2
	1	1	1	1	1	3
Control	0	0	0	0	0	33
	1	0	0	0	0	10
	1	1	0	0	0	2

Other actions

Treatment	Additional steps	# Consumers
Email	Only followed notification steps	5(55.5%)
	Disconnected device	2(22.5%)
	Software update	1(11%)
	Disable port forwarding	1 (11%)
Walled garden	Only followed notification steps	12(31%)
	Disconnect device	9 (24%)
	Stop using the device	6 (16%)
	Software update	5 (13.5%)
	Disable port forwarding	3 (8%)
	Ask for help	2(5.5%)
Control group	Software update	8(18%)
	Stop use	2(4.4%)
	Disconnected device	1(2%)

Statistical Model: Compliance

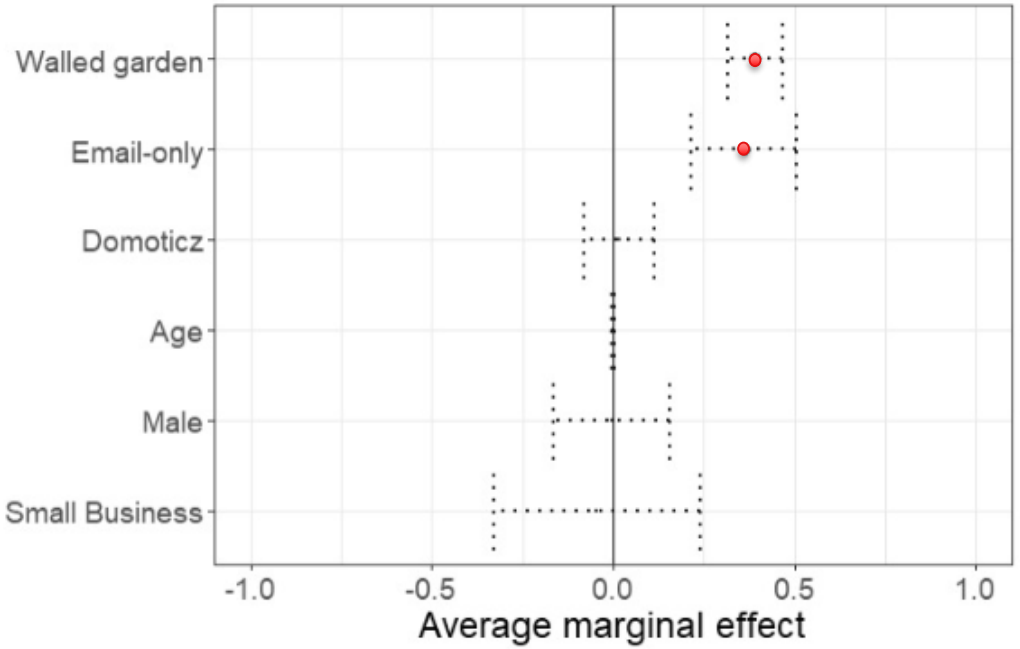


Figure 5: Average marginal effect of each predictor variable

- Consumers in the walled garden do 1.95 steps more on average respect to the control group.
- Users notified via email do 1.8 steps more on average respect to the control group.

When consumers are informed about compromised IoT, they are willing to act.

Statistical Model: Cleanup

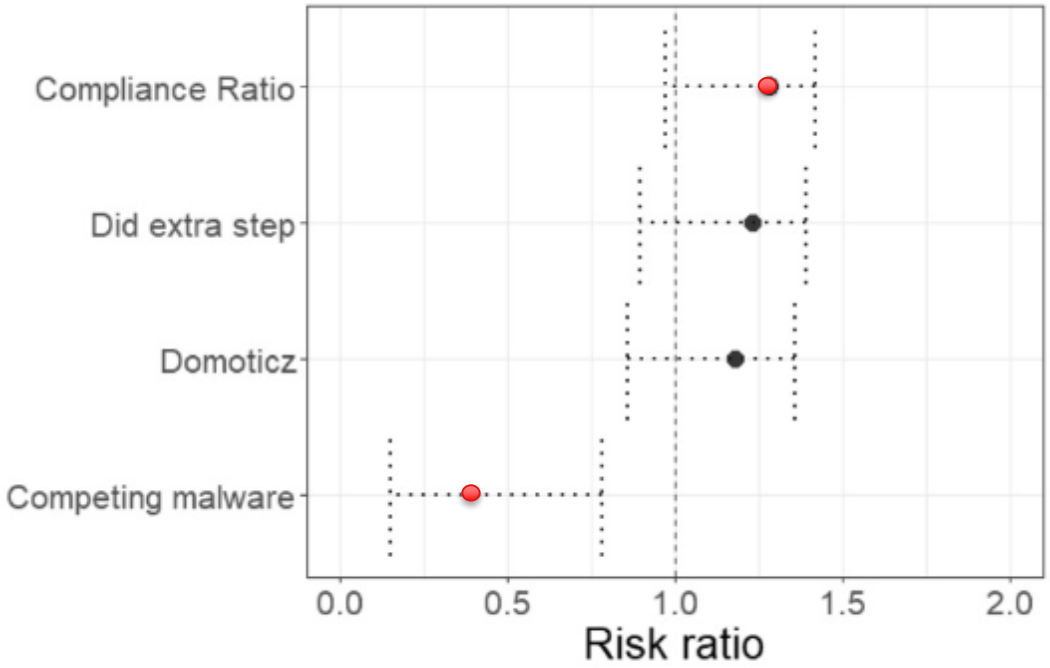


Figure 7: Relative Risk Model 3 on remediation

- Compliance ratio increases the probability of remediation by 32% as compared to the control group.
- Competing malware presence in the home network decrease the probability of remediation by 54%

User compliance with the recommended steps might not apply to all types of malware. Some devices remain infected or are being reinfected in the network.

IoT malware analysis has confirmed that some families fight for control over vulnerable devices.

Consumers' experience

- 24 out of the 39 users (61%) of the interviewed consumers in the Walled- garden group were satisfied by being reached.

- 11 (100%) in the email group were satifisfied.

Limitations

- We rely on self-reported behavior.
- Only one ISP and its subsidiary involved in the study.
- Small email treatment group to make robust inferences.

Takeaways

- In the walled garden group, 92% got cleaned up versus 82% in the email group.
- An increase in the compliance ratio increase the probability of remediation by 32%.
- If the user's device was infected with competing malware, this reduced the probability of remediation by 54%.

Q & A

More info:

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2021, 1–21
https://doi.org/10.1093/cybsec/tyab015
Research paper

Research paper

User compliance and remediation success after IoT malware notifications

Elsa Rodríguez[1,*], Susanne Verstegen[1], Arman Noroozian[1], Daisuke Inoue[2], Takahiro Kasama[2], Michel van Eeten[1] and Carlos H. Gañán[1]

[1]Organisation and Governance, Delft University of Technology, Jaffalaan 5, 2628 BX Delft, The Netherlands and [2]National Institute of Information and Communications Technology, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan

*Correspondence address. Organisation and Governance, Delft University of Technology, Jaffalaan 5, 2628 BX Delft, The Netherlands. Tel: +31-64-54-37915; E-mail: e.r.turciosrodriguez@tudelft.nl

Received 17 September 2020; revised 17 May 2021; accepted 16 June 2021

https://doi.org/10.1093/cybsec/tyab015

@elsarebecat

e.r.turciosrodri@tudelft.nl