No.30
15th October 2019

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

Dutch People Engage in IoT Clean-Up

A highlight of last week's live streamed "KPN Alert Online" seminar was the presentation of recent consumer research by the Delft University of Technology (TU Delft) on real-world consumer behaviour relating to IoT device infections.

- When prompted by their ISP, Dutch consumers were very willing to try remediating IoT device infections in their homes. Users whose PCs were quarantined via a walled garden much preferred to engage with their ISP to remediate infections rather than escape the quarantine and leave the device infected.
- Despite often flawed understanding of their ISP's generic recommendations, the efforts of Dutch consumers to remediate home IoT infections were very effective. 79% of users that were quarantined via a walled garden successfully cleaned up their IoT devices, as did 66% of those that were notified by email only.
- While the growth in consumer IoT makes new security measures in the ISP layer increasingly desirable, identifying the right business models and business metrics continues to be challenging. The TU Delft study data looks like it might help here.

The research looked at the propensity of Dutch consumers to respond to outreach from their ISP directing them on how to remediate infected IoT devices in their homes.

In one of the first such studies, TU Delft looked into the propensity of Dutch consumers to respond to outreach from their ISP directing them to remediate infected IoT devices in their homes. The study, in partnership with the Dutch Ministry of Economic Affairs, KPN and other stakeholders, began in 2018 and was completed this year.

The research identified Dutch consumers that had MIRAI infections on their IoT devices. Their ISP then took one of three courses of action in terms of reaching out to them and recommending generic remedial actions. The study sought to understand two things:

- the extent to which Dutch users were willing to act on an ISP's clean-up recommendations, even when guidance is generic and may be hard to understand.
- what Dutch users actually do with generic IoT clean-up guidance they get from their ISP and how effective their attempts at remediation really are.

A Randomized Control Trial model was used

Using a Randomized Controlled Trial (RCT) model, two different survey groups were advised by their ISP of a MIRAI infection on IoT devices in their home network. The first group was sent nothing more than an email alert together with recommended actions. The second group was 'quarantined' in a walled garden landing page i.e. internet access was restricted to a handful of critical applications.

Figure 1: Dutch Consumer Actions and Their Impact on IoT Infections

	Complied with all actions	Performed some actions or other actions	Cleaned up device
Walled garden	25%	66%	79%
Email notification only	22%	44%	66%
No notification	N/A	N/A	22%

Source: TU Delft

In the case of both groups, the ISP outreach also recommended five generic steps to remediate the infections, such as changing passwords and re-starting the device. Consistent with the RCT model, a third control group identified as having MIRAI-infected 'things' was not contacted at all.

The findings were presented by Michel Van Eeten, Professor at the Faculty of Technology, Policy and Management at Delft TU, and a member of the Dutch Cyber Security Council. The talk runs from the 9th to 50th minutes of the KPN Alert Online session. The full three-hour session can be viewed **here**. TU Delft's research paper – "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai" – can be viewed **here**. For ISPs and vendors evaluating this market, the detail of these two resources is well worth exploring.

Most users that were quarantined chose to engage in trying to remediate the infection.

In his talk, Professor Van Eeten shared a subset of the high level findings by way of a mix of hard data points and more general high level statements. Among some of the key findings of the study are the following:

- Well over 90% of all infected IoT devices are in ISP networks.
- Rather than opt out of the walled garden and resume normal service as they could have done – thereby leaving the infection un-dealt with – most users that were quarantined chose to engage in trying to remediate it.
- Around half of Dutch consumers implemented at least some of the five clean-up techniques recommended to them by their ISP. 25% of the quarantined, walled garden group and 22% of the emailed group implemented all five of them.
- 79% of users that were quarantined via a walled garden successfully cleaned up their IoT devices, as did 66% of those that were notified by email only.
- There is no correlation between a consumer's sophistication as an IT user and the propensity of their IoT devices to get infected. Consumers who consider themselves to be advanced tend to over-estimate themselves and expose themselves to high risk. Those who identify themselves as not very technology-literate take little risk.

The TU Delft study is an important contribution to ongoing deliberations around the appropriate balance of responsibilities for consumer IoT security between government, different parts of industry, and consumers themselves. This is something that HardenStance touched on in a White Paper published earlier this year: "Home Router Security: The Buck Stops Where?".

The study doesn't move the needle in terms of answering that question decisively. Clearly, the position ISPs occupy in the ecosystem makes them uniquely well placed to provide comprehensive protection to millions of users as part of a layered IoT security architecture. But the question of whether that's primarily an opportunity or a cost for an ISP – and if it's mainly a cost, who should bear it? – remains a complex one.

The study does nevertheless suggest that consumers – at least in some markets – might be better motivated, and better able, to shoulder some of the effort of mitigating IoT risk than they are given credit for. Whoever contemplates investment here – whatever model, whatever ROI or Social ROI (SROI) metrics they have in mind – some of the data from this study looks like it might be helpful.

More Information

- Contact HardenStance's Principal Analyst: patrick.donegan@hardenstance.com
- Register for free email notifications when HardenStance releases new content.
- www.hardenstance.com
- HardenStance received no payment – direct or "in kind" – for publishing this Briefing.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, ETSI and TM Forum. To learn more visit www.hardenstance.com

HardenStance Disclaimer of Warranty & Liability