

A world map with a black background. The landmasses are outlined in white. Numerous small, colored dots (red, orange, yellow, green, blue) are scattered across the map, representing data points. The highest density of dots is in North America, particularly in the United States, where they form a large, bright orange and red mass. Other significant clusters are visible in Europe, Africa, and Asia.

# Hacks, Sticks and Carrots

## Improving the Incentives for Cybersecurity

### Michel van Eeten

```
mov     esi, eax
push    0                ; lpszHeaders
push    ecx              ; http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
push    esi              ; hInternet
call    ds:InternetOpenUrlA
mov     edi, eax
push    esi              ; hInternet
mov     esi, ds:InternetCloseHandle
test    edi, edi
jnz     short exit
call    esi ; InternetCloseHandle
push    0                ; hInternet
call    esi ; InternetCloseHandle
call    dropper_main
pop     edi
xor     eax, eax
pop     esi
add     esp, 50h
retn    10h
```

; -----

```
exit:                                     ; CODE XREF: WinMain(x,x,x,x)+65↑j
      call    esi ; InternetCloseHandle
```



# It's about economics, stupid

- Patching breaks things. Study at major network operator found that leading cause of outages was: patching.
- Over 20k vulnerabilities reported in 2017. Most are never exploited. CVSS critical score tells you nothing.

**ars TECHNICA** [BIZ & IT](#) [TECH](#) [SCIENCE](#) [POLICY](#) [CARS](#) [GAMING & CULTURE](#) [FORUMS](#) [≡](#)

*BREAKING THE INTERNET... —*

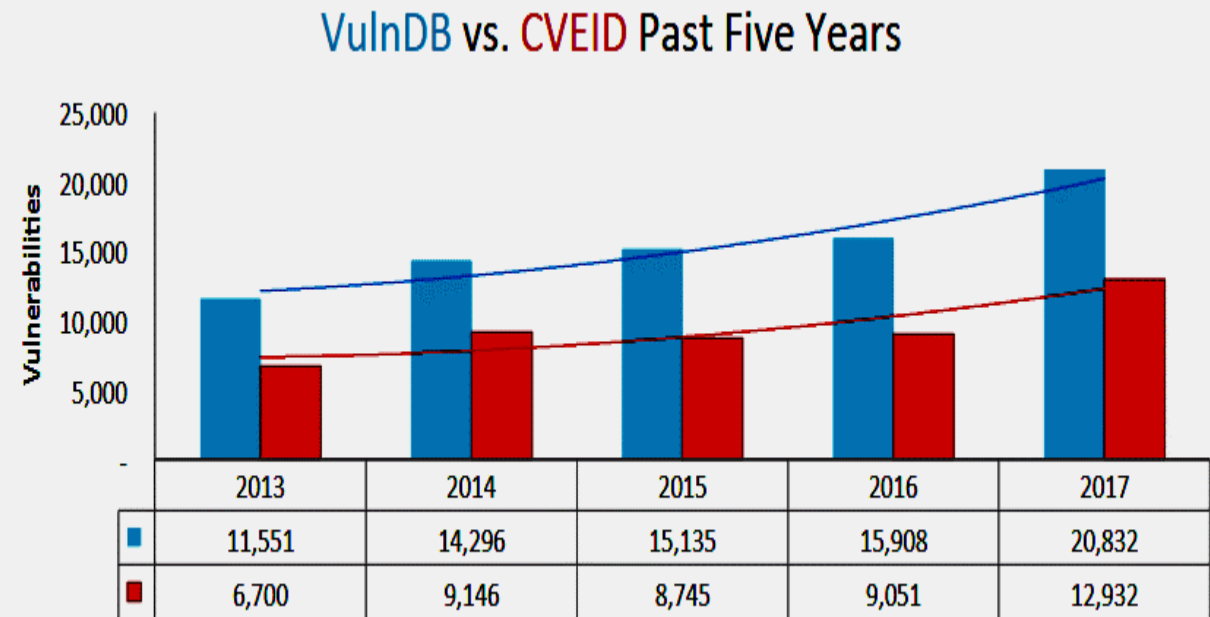

## Windows 10 update broke DHCP, knocked users off the Internet

Microsoft issued another patch on Tuesday that fixes the problem.

**TOM MENDELSON (UK)** - 12/14/2016, 2:47 PM

211  
**TU Delft**  
f

Microsoft has quietly fixed a software update it released last week, which effectively prevented Windows 10 users from connecting to the Internet or joining a local network.



# I. Measuring and Hacking Incentives



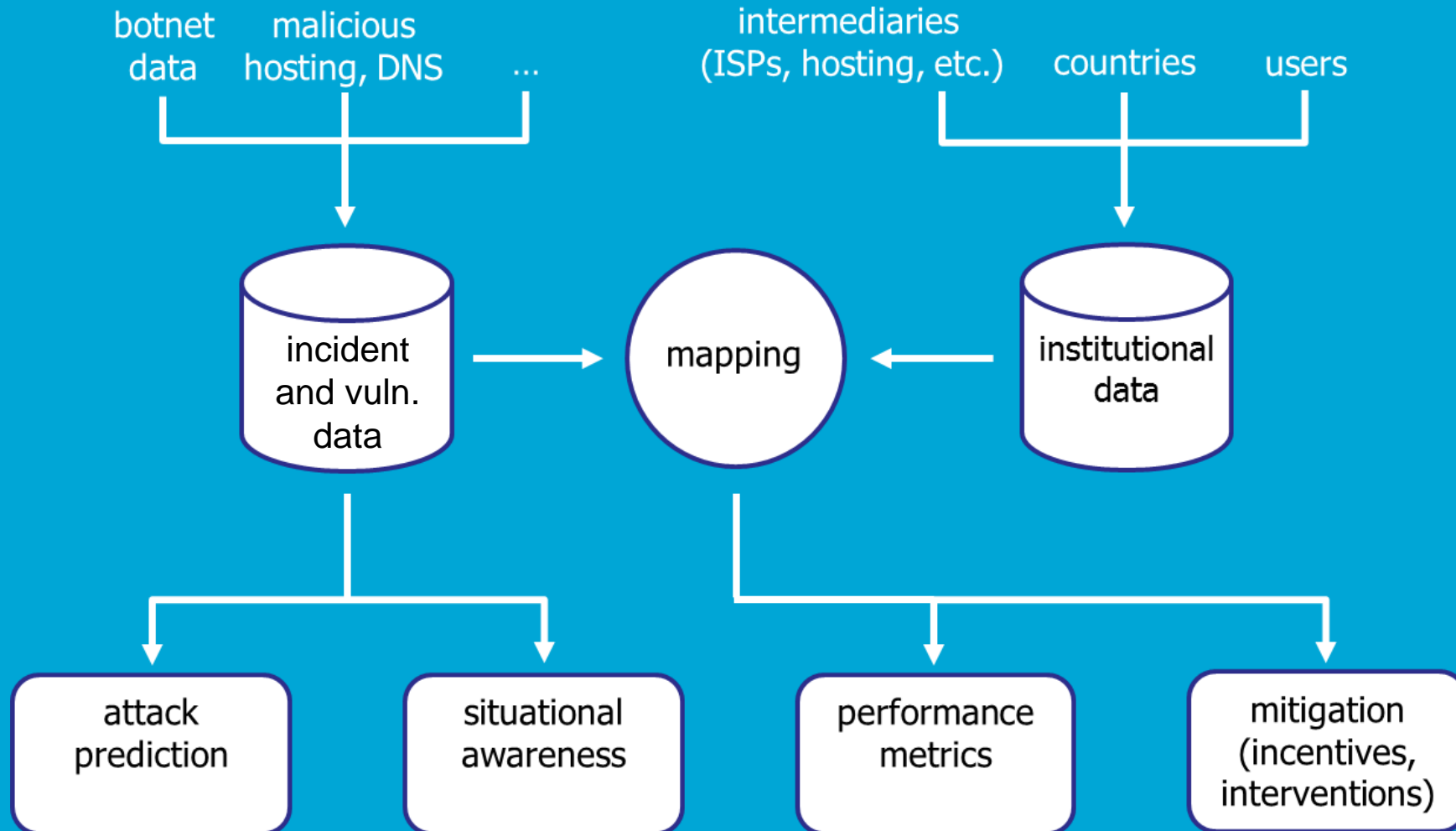




# Team Economics of Cybersecurity @ TU Delft

# SYSTEMS

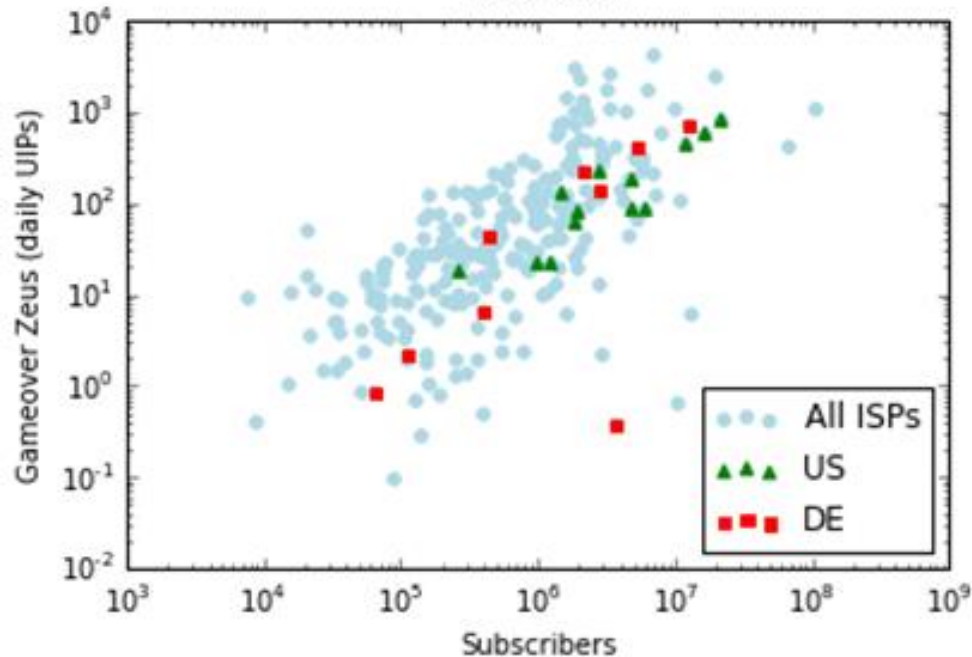
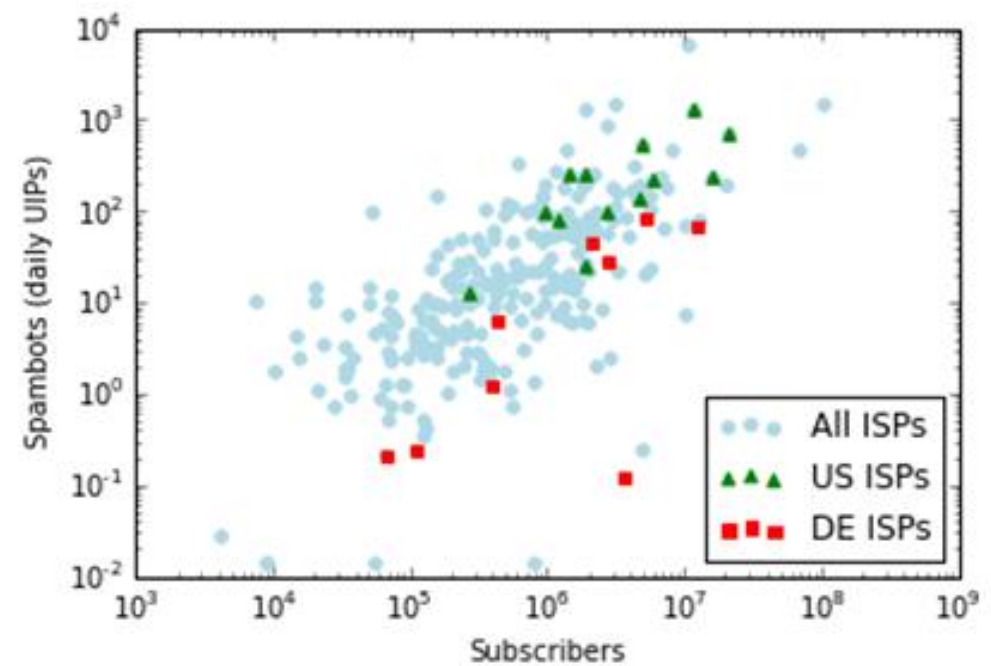
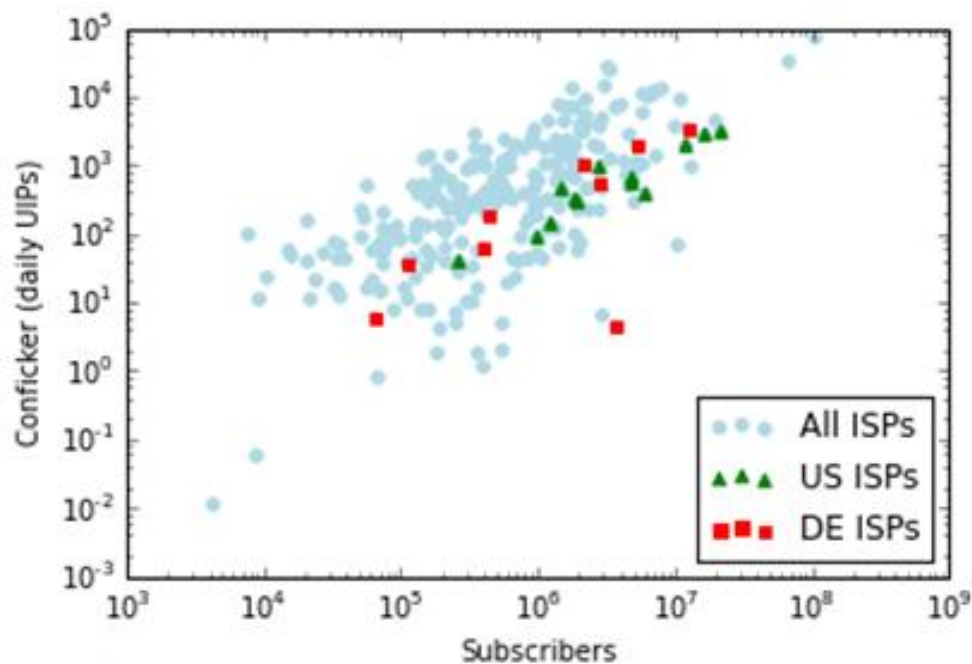
# ACTORS



# II. Peer Pressure



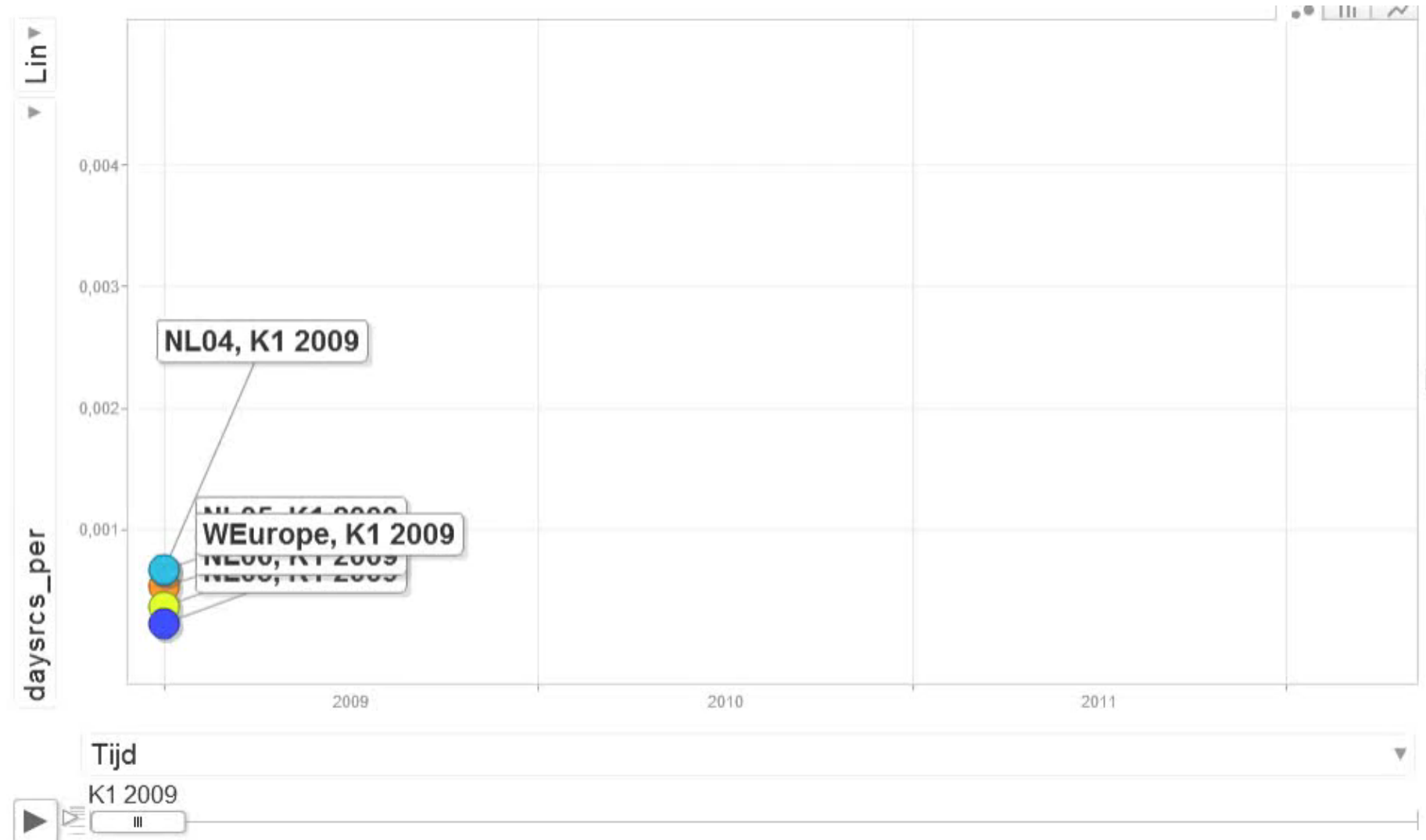




- Infection rates of ISPs of same size differ in order of magnitude, even in same market, so same regulatory framework and price competition



# Benchmarks as an incentive



# III. Reputation Effects



# Nederland 'paradijs cybercriminelen'

🕒 03-02-2013, 18:02 AANGEPAST OP 03-02-2013, 19:07 [POLITIEK](#)

Nederland is een paradijs voor cybercriminelen. Dat zegt het beveiligingsbedrijf McAfee na onderzoek. De Tweede Kamer maakt zich zorgen en wil dat er meer wordt gedaan aan internetveiligheid.

Cybercriminelen gebruiken volgens McAfee 154 servers in Nederland om dagelijks honderdduizenden computers over de hele wereld te besturen. Ze versturen spam, stelen inloggegevens en wachtwoorden, kraken bankgegevens en stelen vertrouwelijke bedrijfs- en overheidsgegevens.

Nederland wordt omschreven als een aantrekkelijk land voor cybercriminelen,

# “Netherlands Clean”

- Map abuse data\* to NL hosting providers

\* StopBadware, Shadowserver Compromised Website, Shadowserver Sandbox URL, Zeustracker C&Cs, MLAT requests, Dutch Child Pornography Hotline, PhishTank, Anti-Phishing Working Group, PSBL, private spam trap

- Control for attack surface of providers
- Rank!

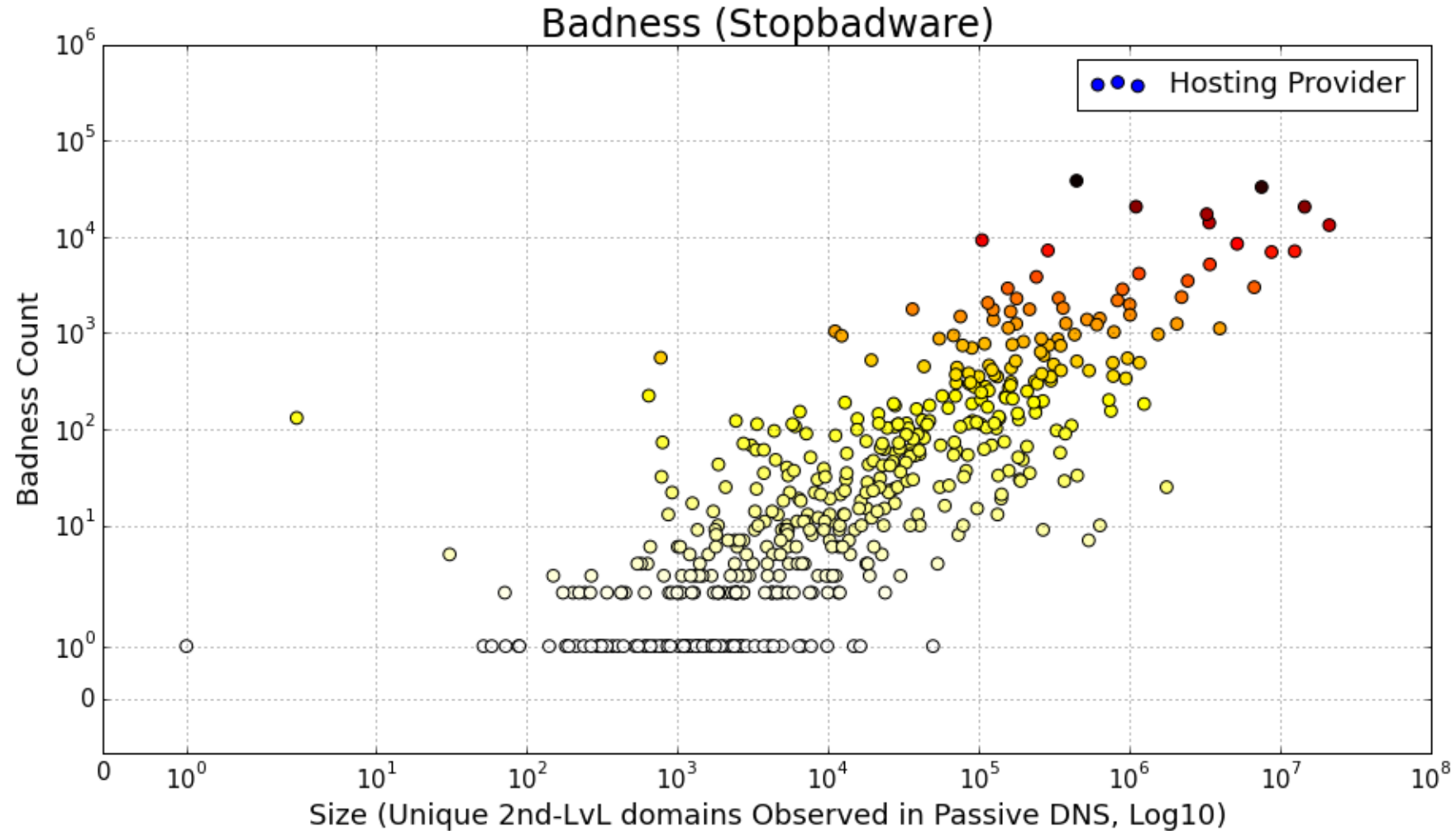


OPENBAAR  
MINISTERIE

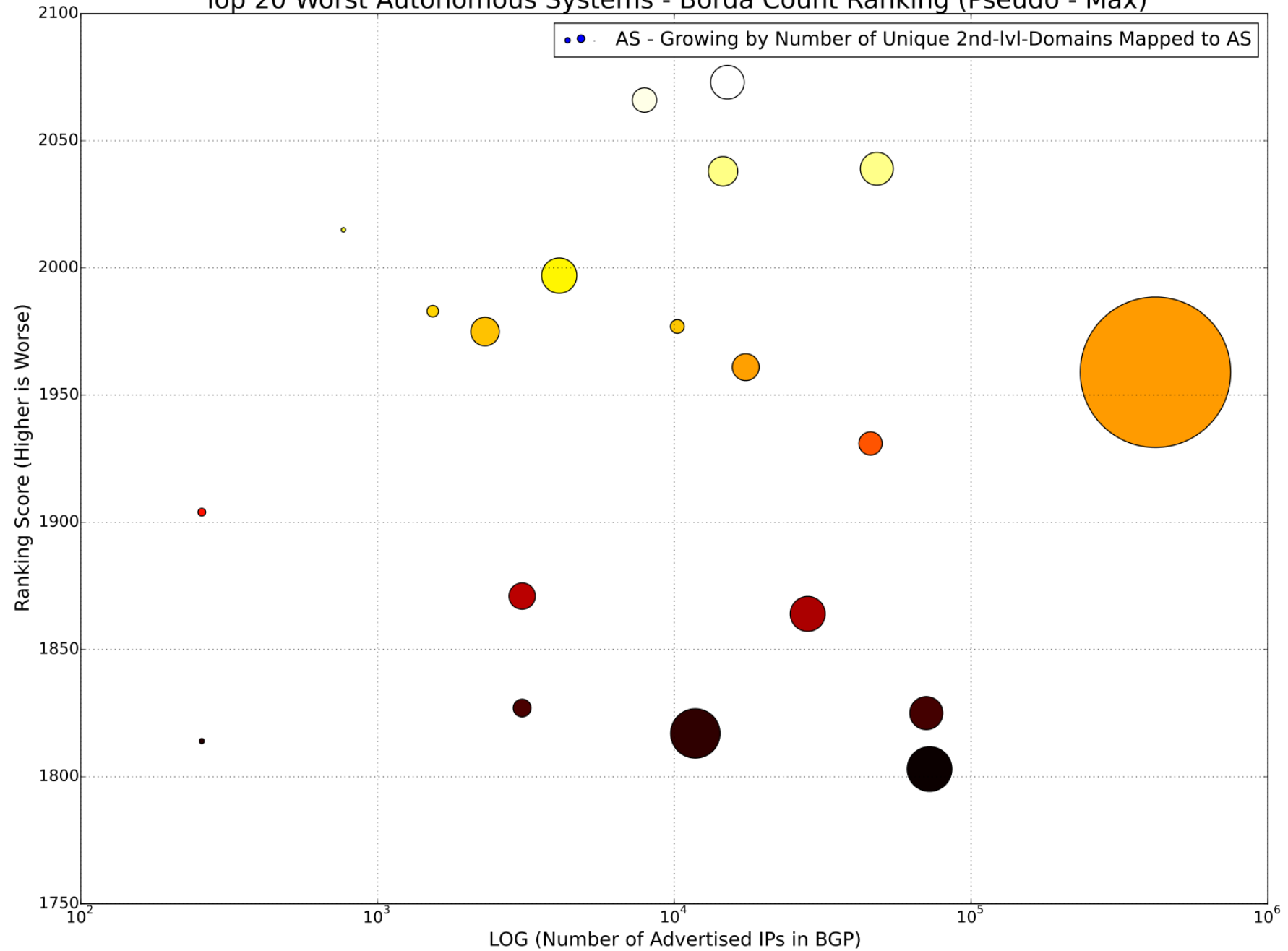




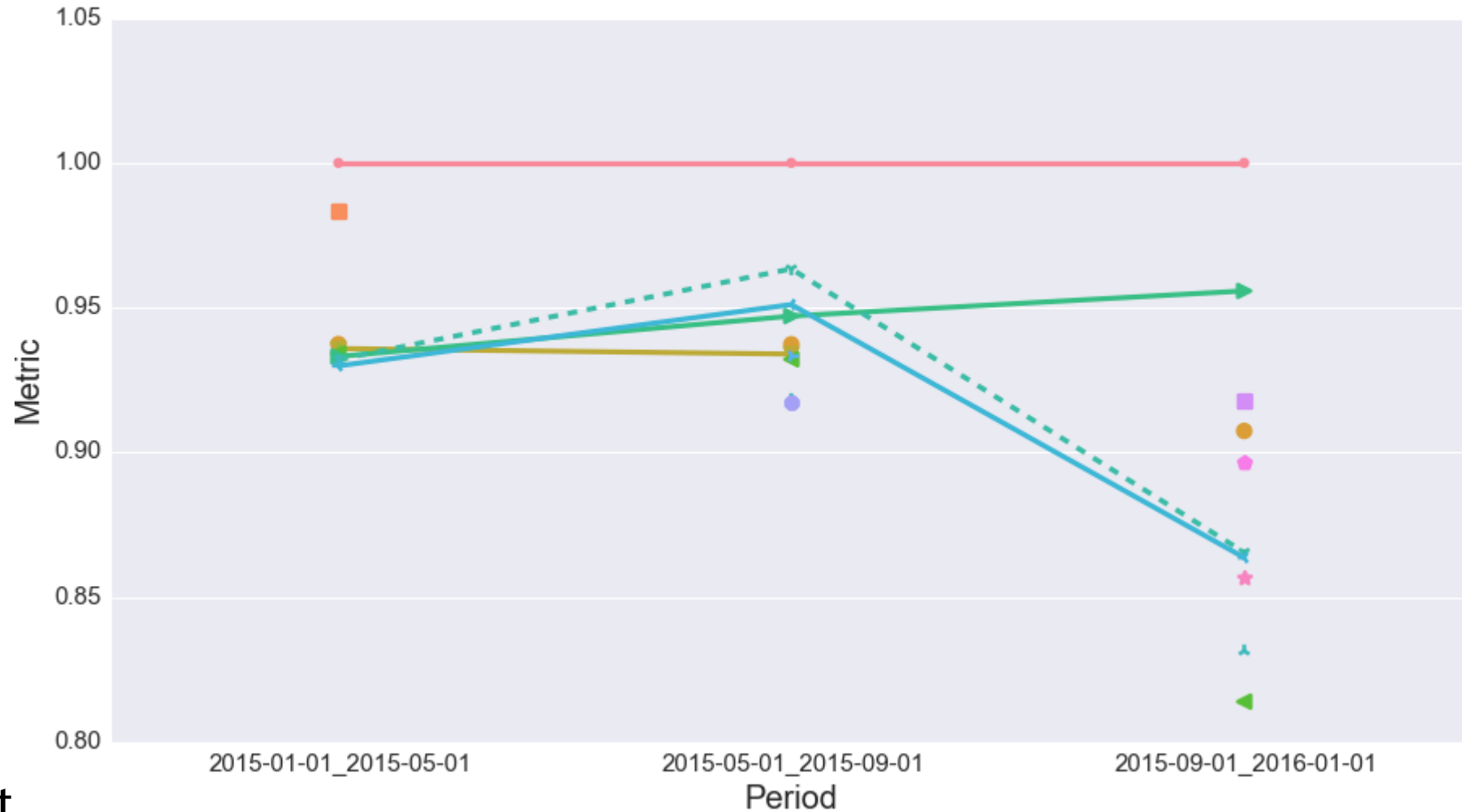
# Abuse in hosting providers



Top 20 Worst Autonomous Systems - Borda Count Ranking (Pseudo - Max)

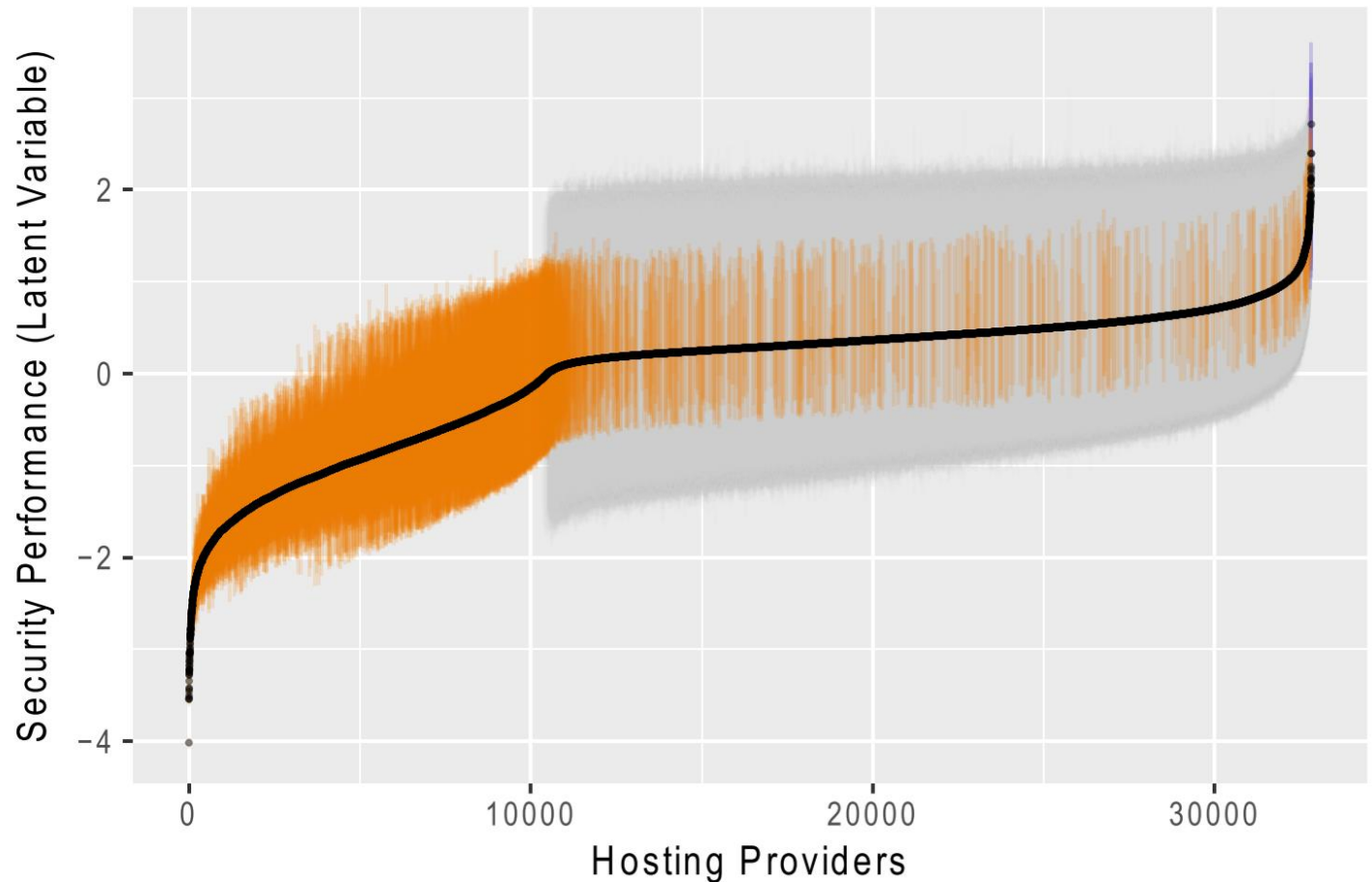


# Top 10 worst providers, before and after police intervention



# Scaling up!

- Security benchmark for global hosting market (~40k providers)
- Highly predictive of number of compromised sites (up to 99% EV)
- Collaboration with NL hosting sector to incentive providers by sharing benchmark



*> Enforcing escalating self-commitment*



# IV. Liability ("Polluter Pays Principle")





January 22, 2016

## Dutch watchdog sues Samsung over lack of Android security updates



*Consumer group in the Netherlands sends in the lawyers over Samsung's allegedly "poor software update policy for Android smartphones".*

The Dutch Consumers' Association that filed a lawsuit against Korean electronics firm Samsung has accused the company of having a "poor software update policy for Android smartphones". It also alleges that the firm is "guilty of unfair trade practices".

An [open letter](#) from Bart Combée, director of Consumentenbond.



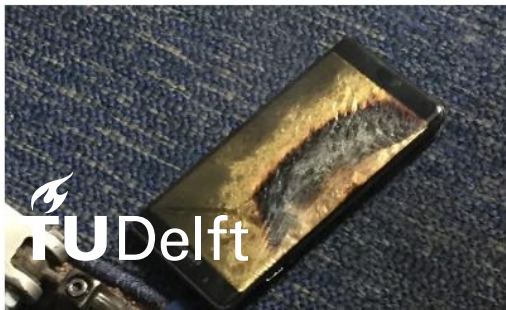
## Samsung Galaxy Note 7 to Receive Update That Forces Users to Follow Recall

Tasneem Akolawala, 07 November 2016



### HIGHLIGHTS

- The update will restrict Galaxy Note 7 to charge more than 60 percent
- A pop-up notification shows up every time you reboot the phone
- Samsung has managed to recall 85 percent Galaxy Note 7



## ASUS hit by FTC with 20-year audit for bungled router security

The US Federal Trade Commission has come down hard on ASUS for putting consumers at risk from router and cloud security failings.

By [Liam Tung](#) | February 24, 2016 -- 13:36 GMT (13:36 GMT) | Topic: [Security](#)

Taiwan-based computer maker AsusTek has agreed to be audited for the next 20 years to settle charges from the US Federal Trade Commission that its "failure to employ reasonable security practices has subjected consumers to substantial injury".



## NEWS

[Home](#) [Video](#) [World](#) [UK](#) [Business](#) [Tech](#) [Science](#) [Magazine](#) [Entertainment & Arts](#) [Health](#) [World News TV](#) [More](#)Technology

## Fiat Chrysler recalls 1.25m trucks over software error

🕒 12 May 2017 | Technology



GETTY IMAGES

Three models of Ram pickup trucks are affected

### Top Stories

**Trump 'shared secret info with Russia'**

🕒 43 minutes ago

**Mexican drug trade reporter shot dead**

🕒 30 minutes ago

**N Korea link suspected in cyber-attack**

🕒 5 hours ago

### Features



**Is France's Socialist Party dead?**

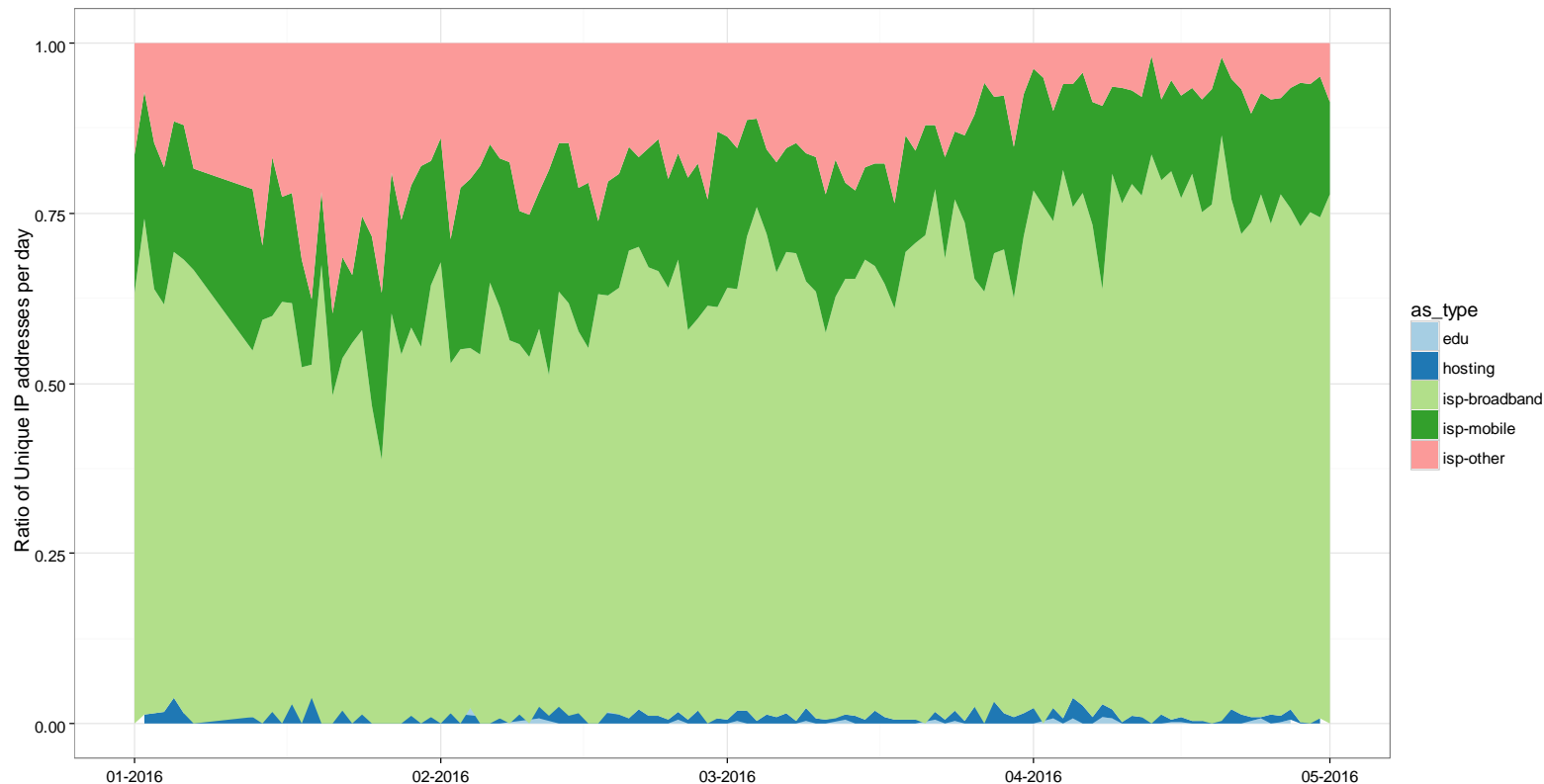
# V. Intermediary Liability ("Duty to Care")





# Who operates the networks?

- NL ISPs and AbuseHub, clearinghouse of abuse data, will help clean up IoT

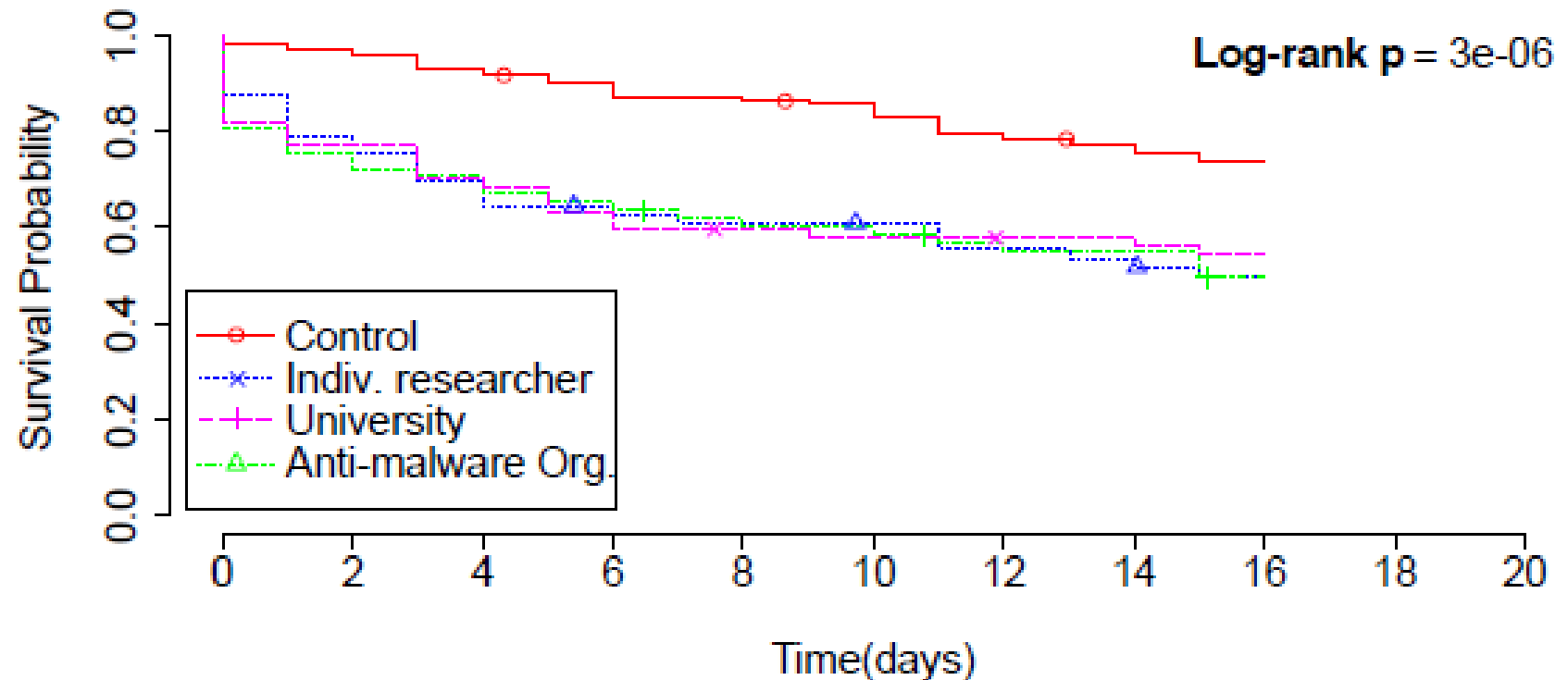


# VI. Social Norms



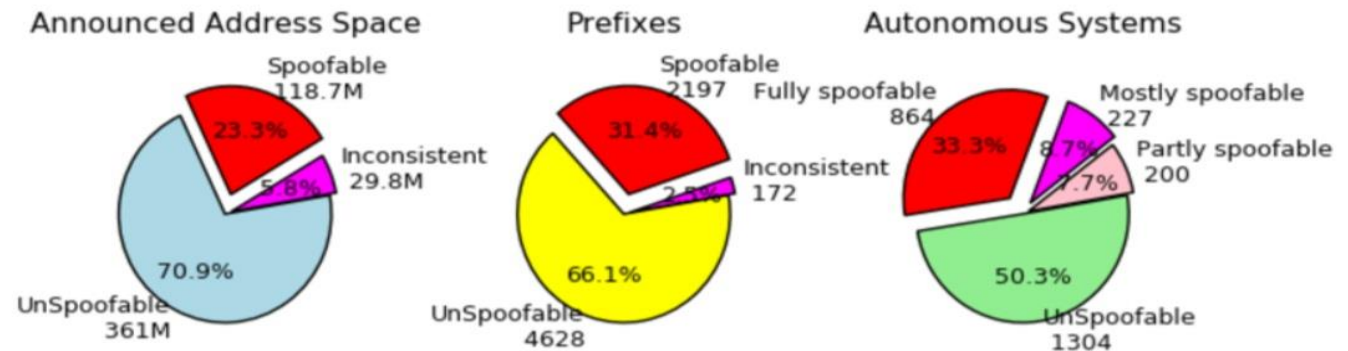
# 'Doing the right thing'

- Abuse reporting of malicious sites: voluntary clean up by providers



# 'Doing the right thing'

- The question is *not*: why aren't some providers adopting anti-spoofing measures (BCP38)? The question is: why would anyone adopt it at all?
- BCP38 is a cost to the provider, while all benefits go to the rest of the Internet
- Remarkably, lot of providers are compliant. Why? Social norms within provider community (M3AAWG, NANOG, etc)



Source:  
<https://www.caida.org/projects/spoofers/>



# VI. Certification and Standards



Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	<a href="https://ipvm.com/reports/ip-cameras-default-passwords-directory">https://ipvm.com/reports/ip-cameras-default-passwords-directory</a>
root/anko	ANKO Products DVR	<a href="http://www.cctvforum.com/viewtopic.php?f=3&amp;t=44250">http://www.cctvforum.com/viewtopic.php?f=3&amp;t=44250</a>
root/pass	Axis IP Camera, et. al	<a href="http://www.cleancss.com/router-default/Axis/0543-001">http://www.cleancss.com/router-default/Axis/0543-001</a>
root/vizxv	Dahua Camera	<a href="http://www.cam-it.org/index.php?topic=5192.0">http://www.cam-it.org/index.php?topic=5192.0</a>
root/888888	Dahua DVR	<a href="http://www.cam-it.org/index.php?topic=5035.0">http://www.cam-it.org/index.php?topic=5035.0</a>
root/666666	Dahua DVR	<a href="http://www.cam-it.org/index.php?topic=5035.0">http://www.cam-it.org/index.php?topic=5035.0</a>
root/7ujMko0vizxv	Dahua IP Camera	<a href="http://www.cam-it.org/index.php?topic=9396.0">http://www.cam-it.org/index.php?topic=9396.0</a>
root/7ujMko0admin	Dahua IP Camera	<a href="http://www.cam-it.org/index.php?topic=9396.0">http://www.cam-it.org/index.php?topic=9396.0</a>
666666/666666	Dahua IP Camera	<a href="http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW43">http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW43</a>
root/dreambox	Dreambox TV receiver	<a href="https://www.satellites.co.uk/forums/threads/reset-root-password">https://www.satellites.co.uk/forums/threads/reset-root-password</a>
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	<a href="https://news.ycombinator.com/item?id=11114012">https://news.ycombinator.com/item?id=11114012</a>
root/x3511	H.264 - Chinese DVR	<a href="http://www.cctvforum.com/viewtopic.php?f=56&amp;t=34930&amp;start=1">http://www.cctvforum.com/viewtopic.php?f=56&amp;t=34930&amp;start=1</a>
root/hi3518	HiSilicon IP Camera	<a href="https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera/">https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera/</a>
root/klv123	HiSilicon IP Camera	<a href="https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c7">https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c7</a>
root/klv1234	HiSilicon IP Camera	<a href="https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c7">https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c7</a>
root/jvbzd	HiSilicon IP Camera	<a href="https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d">https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d</a>
root/admin	IPX-DDK Network Camera	<a href="http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/">http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/</a>
root/system	IQinVision Cameras, et. al	<a href="https://ipvm.com/reports/ip-cameras-default-passwords-directory">https://ipvm.com/reports/ip-cameras-default-passwords-directory</a>
admin/meinsm	Mobotix Network Camera	<a href="http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/">http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/</a>
root/54321	Packet8 VOIP Phone, et. al	<a href="http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/4111">http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/4111</a>
root/00000000	Panasonic Printer	<a href="https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html">https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html</a>
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	<a href="https://ipvm.com/reports/ip-cameras-default-passwords-directory">https://ipvm.com/reports/ip-cameras-default-passwords-directory</a>
root/xmhdipc	Shenzhen Anran Security Camera	<a href="https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI">https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI</a>
admin/smcadmin	SMC Routers	<a href="http://www.cleancss.com/router-default/SMC/ROUTER">http://www.cleancss.com/router-default/SMC/ROUTER</a>
root/toshiba	Toshiba Network Camera	<a href="http://faq.surveillixdvr.support.com/index.php?action=artikel&amp;cat=4&amp;id=8&amp;artlang=en">http://faq.surveillixdvr.support.com/index.php?action=artikel&amp;cat=4&amp;id=8&amp;artlang=en</a>
ubnt/ubnt	Ubiquiti AirOS Router	<a href="http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm">http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm</a>



*> Leveraging CE certification to stop crapware at the EU border*





# Hacking the Incentives

- ▶ Peer pressure  
(benchmark, nudging)
- ▶ Reputation effects  
(name, shame, and praise)
- ▶ Liability  
(make vendors bare the cost)
- ▶ Intermediary liability  
(duty to care, ask ISPs and  
hosters to cut off access)
- ▶ Social norms  
(community action)
- ▶ Certification and standards  
(block market access)



Thank you!

More info:  
[m.j.g.vaneeten@tudelft.nl](mailto:m.j.g.vaneeten@tudelft.nl)



# More info on underlying studies

- Noroozian, A., Ciere, M., Korczynski, M., Tajalizadehkhoob, S. & van Eeten, M. 2017. [Inferring the Security Performance of Providers from Noisy and Heterogenous Abuse Datasets](#), Workshop on the Economics of Information Security.
- Tajalizadehkhoob, S., Van Goethem, T., Korczynski, M., Noroozian, A., Böhme, R., Moore, T., Joosen, W. & van Eeten, M. 2017, [Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting](#) In: ACM Conference on Computer and Communications Security (CCS).
- M. Korczynski, S. Tajalizadehkhoob, A. Noroozian, M. Wullink, C. Hesselman, and M. van Eeten, "[Reputation Metrics Design to Improve Intermediary Incentives for Security of TLDs](#)", IEEE European Symposium on Security and Privacy (Euro S&P 2017), April 2017
- Tajalizadehkhoob, S., Böhme, R., Gañán, C., Korczyński, M., & Van Eeten, M. (2017). [Rotten Apples or Bad Harvest? What We Are Measuring When We Are Measuring Abuse](#). *ACM TOIT*
- Tajalizadehkhoob, S., Gañán, C., Noroozian, A., & Van Eeten, M. (2017). [The Role of Hosting Providers in Fighting Command and Control Infrastructure of Financial Malware](#). In *12th ACM Asia Symposium on Computer and Communications Security (AsiaCCS 2017)*, Abu Dhabi, April 3-8, 2017.
- Jhaveri, M. H., Cetin, O., Gañán, C., Moore, T., & Eeten, M. V. (2017). [Abuse Reporting and the Fight Against Cybercrime](#). *ACM Computing Surveys* (CSUR), 49(4), 68.
- Lone, Q., Luckie, M., Korczyński, M., & van Eeten, M. (2017). [Using Loops Observed in Traceroute to Infer the Ability to Spoof](#). In *International Conference on Passive and Active Network Measurement* (pp. 229-241). Springer.
- van Eeten, M., Lone, Q., Moura, G., Asghari, H., & Korczyński, M. (2016). [Evaluating the Impact of AbuseHUB on Botnet Mitigation](#). *arXiv preprint arXiv:1612.03101*.
- Tajalizadehkhoob, Samaneh, Maciej Korczynski, Arman Noroozian, Carlos Gañán, and Michel van Eeten. "[Apples, Oranges and Hosting Providers: Heterogeneity and Security in the Hosting Market](#)." In *IEEE Network Operations and Management Symposium (IEEE-NOMS 2016)*, Istanbul, 25-29 April 2016
- Asghari, Hadi, Michel JG van Eeten, and Johannes M. Bauer. "[Economics of Fighting Botnets: Lessons from a Decade of Mitigation](#)." In *IEEE Security & Privacy* 5, 16-23, 2015.
- Noroozian, Arman, Maciej Korczynski, Samaneh TajalizadehKhoob, and Michel van Eeten. "[Developing security reputation metrics for hosting providers](#)." In *Proceedings of the 8th USENIX Conference on Cyber Security Experimentation and Test*, pp. 5-5. USENIX Association, 2015.
- Asghari, Hadi, Michael Ciere, and Michel JG Van Eeten. "[Post-mortem of a zombie: conficker cleanup after six years](#)." In *24th USENIX Security Symposium (USENIX Security 15)*, Washington DC. 2015.