

WHAT CARRIERS COULD DO, SHOULD DO AND ACTUALLY DO TO PREVENT CYBER CRIME

Enno Rey, erey@ernw.de



Who I am



- “Old-school networker“
- Started working on Layer 2–4 in the early 90s
- With special focus on security since 1997
- (Co-) Author of several books, articles and whitepapers and regular speaker on international conferences (incl. Black Hat, Hack In The Box, FutureNet)
- Founder (2001) and CTO of a highly specialized IT security consultancy [www.ernw.de] with 12 employees, based in Heidelberg/Germany and Lisbon/PT



Agenda

- What carrier space might have to do with cyber crime
- Expectations & Attitudes
- Technical controls
- The role of regulations
- Looking to the future



Definition

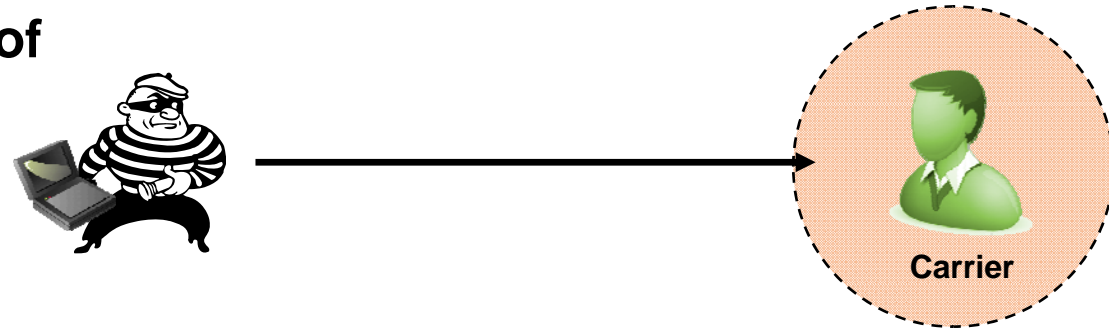
Cyber Crime:

Any crime that is facilitated or committed using a computer, network, or hardware device. [1]

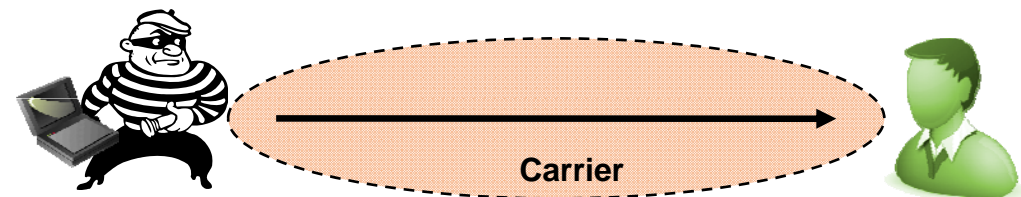


What carrier space might have to do with cyber crime

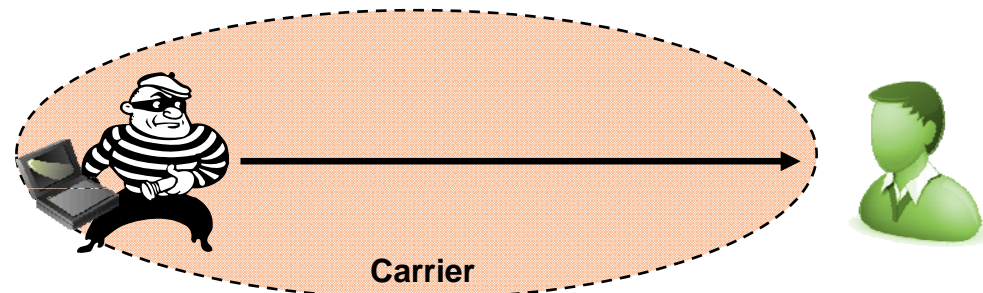
- Carrier might be a victim of cyber crime.



- Carrier's network might be a "medium" for cyber crime.

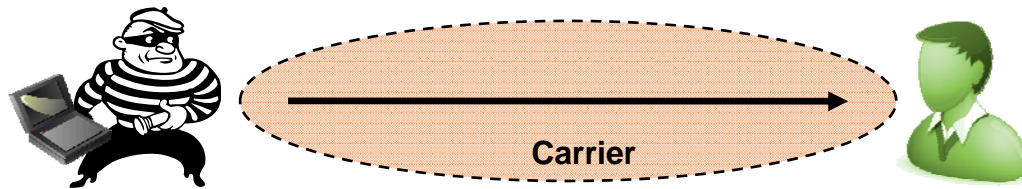


- Carrier might even be the source/originator of cyber crime (think of some governmentally controlled network structures).



“Carrier as medium”

- Here the carrier's network is (ab-) used for criminal acts.



- Hence the carrier's role is just to transport traffic generated elsewhere and attacking entities that might (or might not) be carrier's customers.
- Attacker controlled systems (e.g. phishing websites) might (or might not) be located in carrier's network.
- During the talk I will solely focus on this scenario.



Expectations

- **Some customers expect that a carrier intercepts (“cleans”) malicious traffic in some way.**



- **Others might regard the necessary technical steps (wiretapping / traffic interception) as an “invasion to their privacy“.**
[who believes in “privacy in the internet“ anyway? ;-)]
- **Some are willing to pay for such services. Most are not.**



The *Clean Pipes / Clean Water* Analogy



- **Subscribing to “the internet“ should work like the local water supply:
“Switch on tap and get pure, drinkable water.“**
- **Consumers are (at least in some parts of the world) not required to boil or purify water.**
- **Instead suppliers are required to treat water to exacting standards.**

- **Customer: “Why do I have to pay for the spam, probes, scans, and malicious activity that my telecommunications service provider should prevent at 3 miles out versus my having to subscribe to another service to attain clean pipes at my doorstep?“ [6]**



... and why it doesn't fit

- **Sources of water pollution and “internet traffic pollution“ are fundamentally different, in several aspects.**
- **Definition of “clean water“ is different in different parts of world (ever drank water in your hotel bathroom in ... ? ;-)**
- **Who defines “clean water“ in your part? Do you want the same people to define “clean internet“??**



The "Clean Pipe" Internet?

A vertical chart showing three tiers of internet services. Each tier is represented by a colored box (grey, red, and black) with a downward-pointing arrow indicating the next tier. The top tier is "Internet Basic Service High Speed" for \$29.99, including logos for AOL, GO.com, msn, NBCi, abc, and Walt Disney Internet Group. The middle tier is "Advanced Internet Service High Speed" for \$39.99, including logos for Google, Wikipedia, and Yahoo!. The bottom tier is "Blogger Internet Service High Speed" for \$49.99, including logos for Myspace.com, YouTube, and Blogger. Each tier includes a description of the number of websites included and a note about full internet access availability.

Internet Basic Service High Speed
\$29⁹⁹
over 60 websites

Advanced Internet Service High Speed
\$39⁹⁹
over 200 websites

Blogger Internet Service High Speed
\$49⁹⁹
over 2000 websites!

Full internet access available on request. Prices subject to change at any time. (Full Access does not include access to illegal materials)



Carriers' Attitudes

- ***Mere Conduit***: "I'm just the conduit. I'm just delivering the ticking package. You can't blame me." [5]
- **Some act somehow, usually in a cooperated manner.**
 - Messaging Anti-Abuse Working Group (MAAWG)
 - Internet Watch Foundation (IWF)
 - IXP guidelines (e.g. those of LINX)
 - Best Current Practices (BCP) Sub-Series of RFCs
- **Fact is: most carriers perform "anti cyber crime steps" to some degree.**
- **Why?**
 - Collateral damage of cyber crime poses threat to availability (!!) of own infrastructure (spam to mailservers, DDoS to network connections etc.).
 - Because they fear legislation? (remember why CC industry introduced *PCI*)



Any more opinions

Bruce Schneier:

"I think that the ISPs for home users very much should be responsible. Not that it is their fault, but that they are in an excellent position to mitigate some of the risk. There is no reason why they should not offer my mother anti-spam, anti-virus, clean-pipe, automatic update. All the things I get from my helpdesk and my IT department ... they should offer to my mother. I do not think they will unless the US Government says, 'You have to'" (from [5])



Nice... anything to expect from BT then in the future? ;-)



- **“Some people complain ISPs refuse to take action about abuse and compromised computers on their networks. On the other hand, people complain when ISPs take action about abuse and compromised computers on their networks. ISPs are pretty much damned if they do, and damned if they don't.”**

Sean Donelan on NANOG mailing list, 07/22/2007
[<http://www.merit.edu/mail.archives/nanog/msg01620.html>]



Good Question

- **“So you have potentially tens of thousands of infected computers with Bots making connections to an IRC server. You know many of those bots are well-known, old bots that have built-in removal commands. But 99% of those users don't have the technical knowledge to clean their machine themselves or know what a Bot is. On the other hand, you have 1% of users are sophisticated enough to use IRC servers. And a few percentage of overlap between the two groups.**

What do you do?

- a. nothing**
- b. terminate tens of thousands of user accounts (of users who are mostly "innocent" except their computer was compromised)**
- c. block all IRC**
- d. redirect IRC connections to a few servers known to be used by Bots**
- e. something else**

Sean Donelan on NANOG mailing list, 07/23/2007
[<http://www.merit.edu/mail.archives/nanog/msg01663.html>]



Intermediary Conclusion

- **Asking the carriers to “clean the pipes” might be shooting-the-messenger and is a mine field.**
- ***Very different stances to be found.***
- **Let’s have a look at the technical side now...**



Variations of cyber crime relevant to carriers

- **DDoS, e.g. to perform extortion**
- **Spam**
- **Password / credential harvesting**
- **Phishing (fraud)**
- **Illegal content**



Underlying Infrastructure

- Usually most of these are performed with the help of botnets.
- “A botnet is a network of compromised machines that can be remotely controlled by an attacker.” [7]



Phases of a Bot

- **Initial Infection**
- **Contact to botmaster(s)**
- **Download of payloads / instructions**
- **Malicious actions**



Malicious Actions

- Infection of other systems (*Recruiting*).
- Relaying of spam
- Perform *Distributed Denial of Service (DDoS)* attacks.
- Automated clicks on (paid) advertisement banners.
- Abuse of systems for “file services“ (illegal content).
- Implementation of proxies for various services (SOCKS).



- **Signature based filtering of traffic**
- **Block certain addresses / parts of the net**
 - Address based filtering of traffic
 - Filtering of prefixes (routing)
- **Patch end points**

- **Most of these are'nt (currently) operationally feasible.**



Filtering of traffic (e.g. TCP Port 135)



- **Once some carriers did this (initially at *Blaster* time).**
- **Sometimes they still do (DTAG Speedport problem).**
- **Some filter for business/political reasons (VoIP).**



Prefix Filtering

- **Filtering of “bogons“ on BGP links**
- ***Team Cymru Bogon List***
- **Performed by most carriers.**

- **IRR based filtering**
 - Estimate: of 10 carriers six don't use this all
 - 2 to some degree
 - 2 to full extent



The *Walled Garden* Approach

Usually works like this:

- Monitor traffic (e.g. with netflow) for “abnormal endpoint behav.“
- Put into some quarantine and redirect to clean-up page.
- Let escape after action.
- See also [2].
- Automation is key here.



The role of CPEs

- **Quite some endpoint security problems could be avoided by deploying CPEs that are “correctly configured”.**
- **Here most carriers don't care and thus contribute to security problems (see next slide).**
- **For v6 they think about it...**
[<http://www.ietf.org/internet-drafts/draft-ietf-v6ops-cpe-simple-security-00.txt>]



Role of CPEs

xxx.yyy.195.241 is alive, Community public, Prestige 650R-T3

xxx.yyy.195.243 is alive, Community public, Prestige 650R-T3

xxx.yyy.195.246 is alive, Community public, Prestige 650R-T3

xxx.yyy.195.247 is alive,

xxx.yyy.195.248 is alive, Community public, Prestige 650R-T3

xxx.yyy.195.249 is alive,

xxx.yyy.195.250 is alive, Community public, Prestige 650R-T3

xxx.yyy.195.252 is alive, Community public, Prestige 650R-33

xxx.yyy.195.254 is alive, Community public, Prestige 650R-T3



A Note on Signature Based Filtering

The *Google Case*



- **Did you know that Google scans cached websites for *malicious content* on a large scale?**
- **If found website fed to sandbox and behaviour observed.**
- **Suspicious websites can't be directly clicked-on anymore.**
- **See: Provos et.al. *The Ghost in The Browser* [8]**

- **Ask yourselves: do they provide to clean pipes this way?**



- **For traditional botnets:**
- **Block IRC on port level / ip address based.**
- **DNS redirection + insertion of removal commands.**

- **A growing number of carriers does this.**
- **E.g. <http://www.merit.edu/mail.archives/nanog/msg01610.html>**



Contact to Botmaster, Modern Variant

- ***Fast Flux* Botnets**
- **P2P communication structures**
- **Very difficult to address for carriers.**
- **Strict(er) guidelines for registrars (?)**



Download Instructions / Payloads



- **Possible (but not feasible): Signature based filtering**
- **Monitoring**

- **Again: difficult to address**

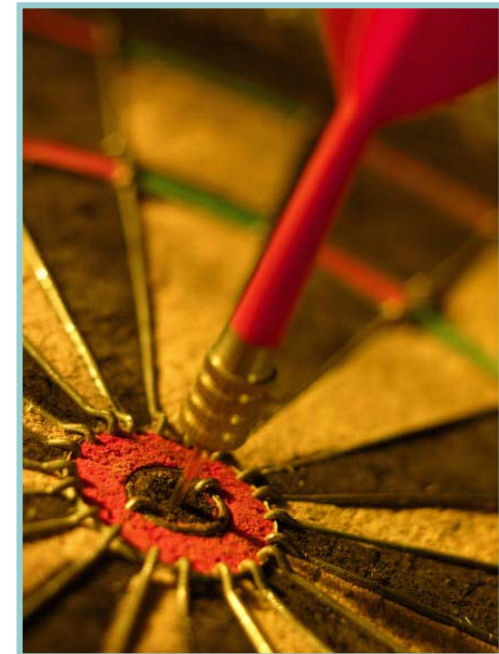


- **Signature based filtering**
 - **Rate limiting (of customer segments)**
 - In contrast to ever growing bandwidths
 - **Port based filtering**
 - **Ingress Filtering as of RFC 2827 / 3704 (BCP 38 / 84) to prevent spoofed connections? [do bots need to spoof?]**
 - **Again: *walled garden*.**
-
- **As for Ingress Filtering: *Tragedy of the Commons* ??**



Technical Controls, Spam

- **Block port 25 outbound for some segments (dial-up, broadband, hotspots)**
- **Rate-limit for some segments (dial-up, broadband) or force users to use certain relay**
- **Most do**
- **Why: Spam = major customer pain**
 - Political regulation may appear



Technical Controls, DDoS

- **Cooperation between carriers**
 - Early warning systems
 - Blackholing / shunning
- **Seems to work to some degree on large scale**
- **Why? Major pain of carriers themselves.**



Technical Controls, Illegal Content



- **Signature / hash based filtering**
- **Blacklisting**
- **Block P2P**

- **For some content (child porn) in some parts of the world done on a large scale (e.g. IWF in UK).**



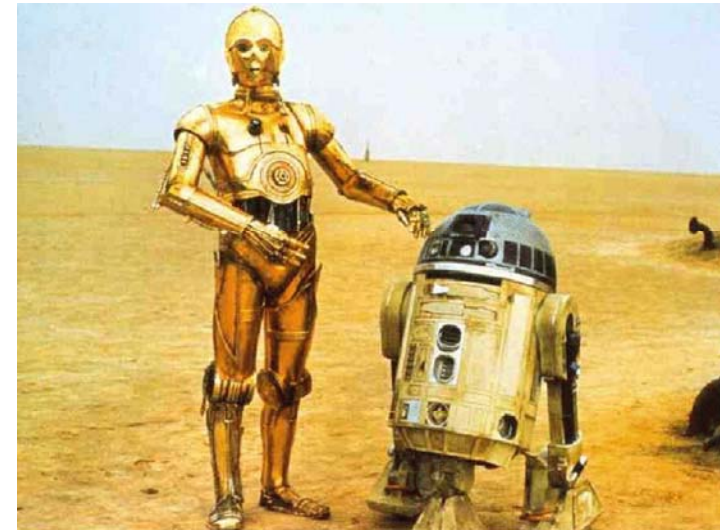
The Role of Regulations

- **In most countries the carriers are already under heavy regulation, for different reasons.
[CALEA in US, TKÜV in Germany etc.]**
- **In some countries there's even more "governmental influence"... have a look at your neighbors.**
- **Asking for "clean pipe regulations" may be short-sighted and this stuff might only be solved with concerted effort (if at all). I expect to see such things though.**



Outlook on the future

- **Technical measures seem possible to some degree.**
- **Question 1: why should carriers burden? Are they responsible?**
- **Question 2: do *we want* this?**
- **However, as said: we'll see this (regulation) stuff anyway.**



Questions?



Thanks for your attention!



References

- [1] Sarah Gordon & Richard Ford: On the definition and classification of cybercrime
<http://www.springerlink.com/content/e370t47k73321114/fulltext.pdf>
- [2] MAAWG BEST PRACTICES FOR THE USE OF A WALLED GARDEN:
http://www.maawg.org/about/whitepapers/MAAWG_Walled_Garden_BP_2007-09.pdf
- [3] MAAWG Managing Port 25 for Residential or Dynamic IP Space
http://www.maawg.org/port25/MAAWG_Port25rec0511.pdf
- [4] LINX BCP on Spam (“UBE“): https://www.linx.net/good/bcp/ube-bcp-v2_0.html
- [5] (UK) House of Lords: Science and Technology – Fifth Report, Chapter 3:
<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16506.htm>
- [6] <http://blogs.csoonline.com/node/290>
- [7] <http://www.honeynet.org/papers/bots/>
- [8] http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf

