Cybersecurity, Cybercrime, Cyberwar, Cyberespionage... can the Internet community make the situation better?

Dr. Cristine Hoepers
cristine@cert.br

Computer Emergency Response Team Brazil - **CERT.br**
Brazilian Network Information Center - **NIC.br**
Brazilian Internet Steering Committee - **CGI.br**

Internet Security is in the Spotlight

Why is this happening?

- Criminals are just migrating to where the money is
- Espionage is being done where the information is
- As our critical infrastructures are increasingly connected to the Internet, this attracts attacks

Sadly, security is being used as a scapegoat for

- control measures
- surveillance
- bad legislation

But this does not mean there are no security problems...

Plenty of attacks today that won't go away easily

- **Against end users (both at home and work)**
  - **fraud, phishing, spyware, etc**
  - **botnets used for all ends**
  - **APTs (*Advanced Persistent Threats*)**

- **Password brute force against network services**
  - **SSH, FTP, Telnet, VNC, etc**

- **DDoS**
  - **reflective attacks (DRDoS) tend to increase**
    (Ex.: attacks on SpamHaus, that reached 300Gbps)

Some other attacks are rapidly increasing

Social Networks

- malware and social engineering
- hijacked accounts, specially of news agencies

Mobile devices

- in most part are malicious apps
- but there are already vulnerabilities found and exploited

CPEs, wifi routers, etc

- password brute force
- already being exploited by botnets (Ex.: Aidra)

Against Registries and Registrars

- like recent domains and ccTLDs hijacks

Part of our problems come from what has been called “irresponsibility at scale” by some

Attacks, like DDoS and Spam, that are possible or amplified by the lack of best practices’ implementation by the various players

- **From the perspective of the networks that need to implement best practices**
  - **There is no immediate benefit**
  - **The effects of the attacks from their perspective are negligible**
- **From the perspective of the networks being attacked**
  - **almost nothing can be done to stop the attack**
  - **the effects are big and complex to mitigate**

The adoption of best practices and security layers is being postponed

- BCP 38 (antispoofing)
- Botnet remediation (disinfection)
- End user awareness/education
  - the users should have a chance to understand the risks
- Other times the sectors are stuck in a “chicken and the egg” dilemma
  - DNSSEC adoption
  - DMARC (SPF, DKIM)

But the collective irresponsibility is not only a network/ISP perspective problem

Other sectors also need to leave their comfort zone

- Software development – 0-days became the norm
  - in general developers think that security is an add-on
    - to be implemented by someone else...
  - but it needs to be incorporated from design to deployment and maintenance
- Standards
  - standards are still developed not focusing enough on security issues at the early design phase
    - underestimating the threats is the most usual
- The model “design ➔ deploy ➔ fix later” is clearly not working

There are many challenges
to get major improvements...

and all of us in this room
have a part to play to start the process

Our networks need to be more resilient

There needs to be more engagement of the community for:

- **Internet Exchange Points**
- **Infrastructure redundancy**
- **DNSSEC adoption**
  - **also to enable new protocols as DANE**
- **More security on the routing system**
  - **RPKI e S-BGP**
- **Improvements or alternatives to the current digital certificate system**
  - **the current trust model is broken**

We all need to work on the end user protection

Systems should be less complex – and this requires a technology made for users, not geeks...

ISPs and network admins in general need to be more proactive to remediate malware and botnet infected devices

- **we need to have a cleaner and safer environment, examples:**
  - **RFC 6561: Recommendations for the Remediation of Bots in ISP Networks**
  - **iCODE – Australia**
  - **Botfrei.de – Germany**
  - **Irish Anti-Botnet Initiative (Botfree.ie) – Ireland**
  - **Cyber Clean Center (CCC) – Japan**
  - **Cyber Curing System / e-Call Center 118 – Korea**
  - **Anti-Botnet Working Group – Netherlands**
  - **Abuse Information Exchange – Netherlands**
  - **Autoreporter – Finland**
  - **U.S. Anti-Bot Code of Conduct (ABCs) for ISPs – US**
  - **Malware Free Switzerland – Switzerland**
  - **Advanced Cyber Defence Centre / Botfree.eu – European Union**

We need to better deal with security incidents

Incident Management needs to be more formalized

- Create CSIRTs/CERTs
- If not possible, at least abuse teams

We need to move to different models to detect infected devices and data exfiltration

- Flows, honeypots, passive DNS
- Act on incident notifications
- Act on data feeds
  - from clearinghouses like Team Cymru or ShadowServer
  - from other CSIRTs

Nothing really new in the last few slides, right?

So, why don't all networks already implement the best practices out there?

- **real life is more complex**
  - **no clear understanding of the benefits**
  - **risks of technical problems**
  - **perceived costs of implementation**
  - **consumer protection issues**
  - **legal and regulatory issues**
- **don't underestimate communication problems**
  - **technical, legal, management and police makers don't speak the same language!**

Final notes

There is no perfect and single solution

- **The sum of all different measures will make the problems more manageable**

All our words and actions can help avoid that security be misused for political reasons

- **this hinders security, privacy and stability of the Internet**

We need to think about multistakeholder engagement for security improvement, or in other words

- **all actors need to be willing to understand each others' challenges**
- **a common vocabulary needs to be developed**
- **we must set aside preconceptions**

Final notes

- Security is not “someone else’s problem”
- Everyone has a part to play
- We need to start acting and
  - implement the well known best practices
  - be more proactive
  - talk to each other
  - move to further cooperation and improved security
- And finally: this keynote has obviously not covered all security issues or countermeasures

Thank you!

Dr. Cristine Hoepers

cristine@cert.br

- **CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/
- **NIC.br – Núcleo de Informação e Coordenação do .br**
  http://www.nic.br/
- **CGI.br – Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/