WARP

Type of Incidents and Stats

Graciela Martínez
Head of WARP

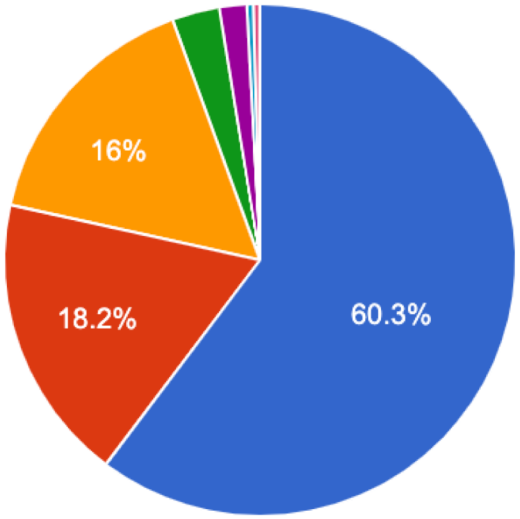
lacnic

www.lacnic.net

WARP

- Warning Advice and Reporting Point is the security incident response team of LACNIC
- We coordinate the computer security incident response that involves LACNIC´s resources
- Constituency is LACNIC´s members
  - No members are also able to report problems

Type of security incidents reported to WARP



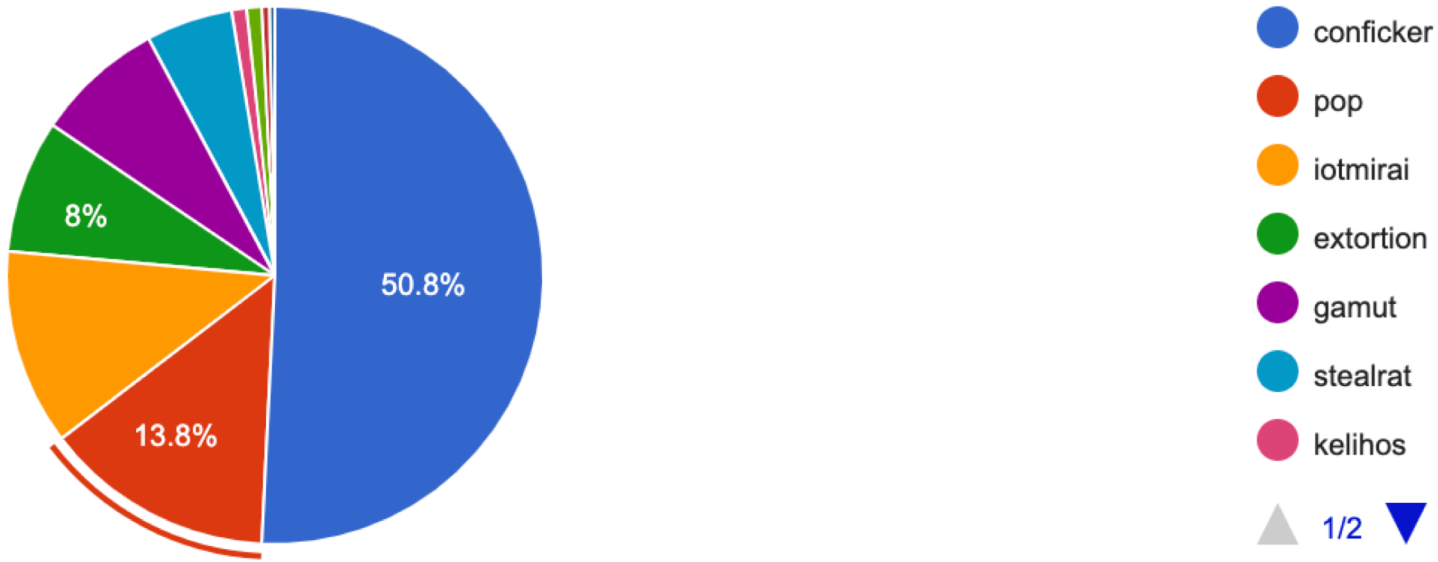
Which type of security incidents do you think are the top three ?

https://warp.lacnic.net/estadisticas/

Type of security incidents managed by WARP (historically)

https://warp.lacnic.net/estadisticas/

Most common Botnets afecting resources of our region



https://warp.lacnic.net/en/estadisticas

lacnic

WHY ?

- *"CaaS"* – Hackers have their focus on where the money is and they are well organized !
- Studies show that Internet economy means more than U$3 Trillions and cybercrime gets around 20% of it
- Spionage for stealing information of goverments, industries and so on.
- "*Hacktivismo*" – DDoS, Defacement
- They take advantage of the lack of regulations
- The increase in crimeware kits, they are cheap, and enable individuals with no previous coding experience to create, customize and distribute malware

DDoS – Distributed Denial of Services – Denegación Distribuida de Servicios

Defacement – Change the look and feel of a webpage

Botnets m s comunes que afectan a recursos de la regi n

Conficker – 79 %

- Malware - worm
- It exploits vulnerabilities of Microsoft Windows Servers
- Main function – Steal information and Spam

ACTIVE since 2008

https://warp.lacnic.net/glosario/

Ransomware

Second US town pays up to ransomware hackers

26 June 2019 Share

More than one town in Florida has been bit by ransomware lately

A town in Florida has paid $500,000 (£394,000) to hackers after a ransomware attack.

Fuente: https://www.bbc.com/news/technology-48770128

lacnic

Some problems

- Outdated or Obsolet Operating Systems
- Inadequate security measures
- Security is not consider during systems development
- Lack of implementation of best practices
  - For example : BCP 38 – Antispoofing, DNSSEC, RPKI
- Users
  - Some of them are not aware of the security threats.
  - Some of them don´t understand security issues – do not report
- Cooperation between organizations sometimes is complicated
- Lack of legislations
- Measures are taken after security incidents – and we (CSIRTS) have no feedback of lessons learned

Recommendations

- Apply patches
  - Operating Systems and applications
- Servers Hardening
- Seggregate your networks according to their goals
  - Corporate, services, control
- Apply Access list to the Internet connection
- Monitor the traffic within your network (inside & outside)
- Software control – install and execute
- Configuration changes control – hashes
- Users security awareness

Areas of work

- Resilience
  - Business continuity plan
  - Backups – tested and up-to-date
- Risks management
- Prevention
  - Have a good network design
- Detection
  - Network traffic monitor
  - Correlate events for early warnings
- Response and Recovery
  - Forensic analysis
  - Security Incident management: establish your own CSIRT
  - Be prepared for a crisis
- People? Work with your constituency to enhance the security awareness

Where do you report a security incident?

- On WARP website you can find a list of CERTs, CSIRTs by countries

https://warp.lacnic.net/csirts

https://warp.lacnic.net/mapa-csirts

- WARP - form

https://warp.lacnic.net/reportar-incidente/

¡Keep walking and working altogether!

lacnic

Muchas Gracias...

lacnic

www.lacnic.net

gmartinez@lacnic.net