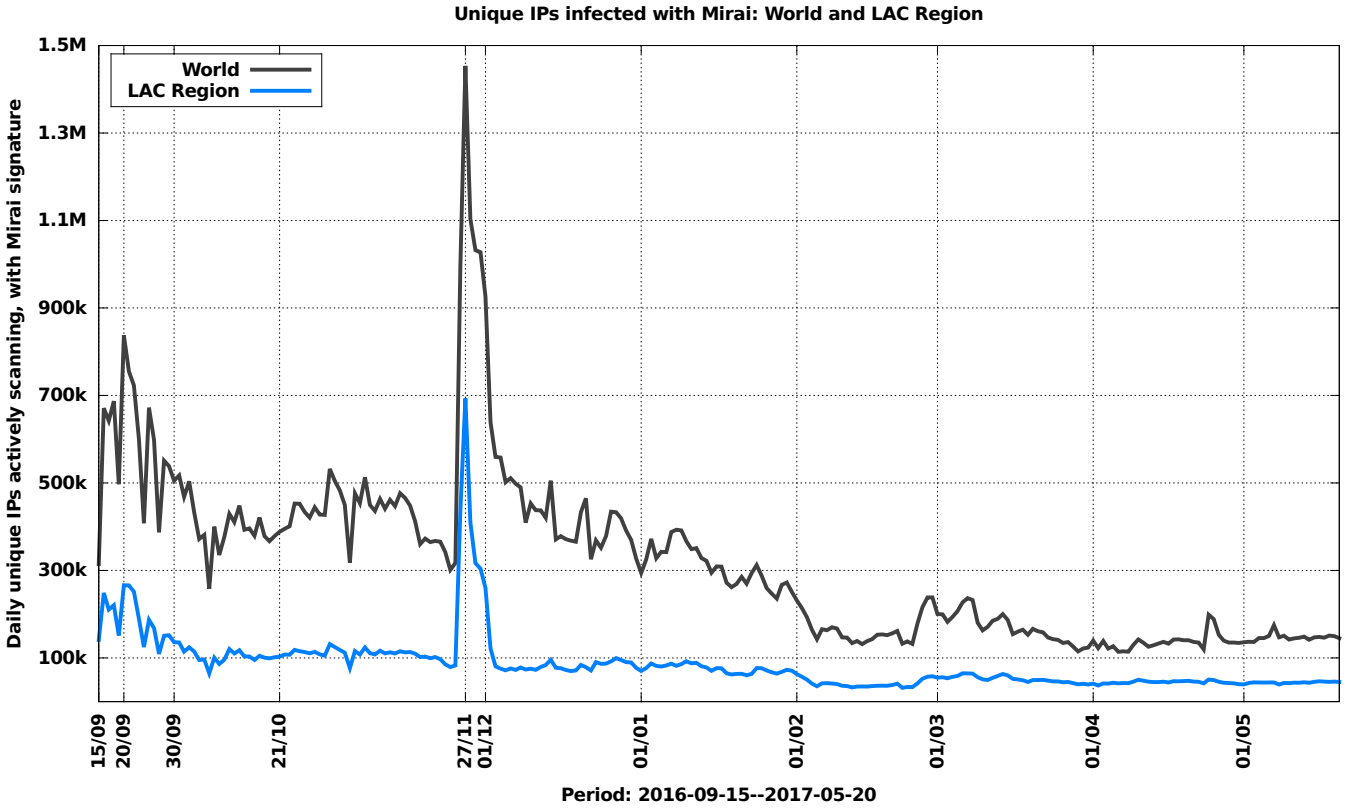
Requisitos Mínimos de Segurança para CPE: a Experiência de Construir uma Recomendação Global

(estudo de caso)

Lucimara Desiderá, Klaus Steding-Jessen, Cristine Hoepers

{lucimara,jessen,cristine}@cert.br

Malware Mirai
Dispositivos Infectados



Fonte: CERT.br

27/11 – variante para CPE (caso Deutsche Telekom)

CPE (Computer Premises Equipments) e´ o equipamento utilizado para conectar assinantes à rede de um Provedor de Serviços de Internet (ISP). Ex: modems, roteadores WiFi, etc.

Abusos, Impactos e a Comunidade de Provedores de Internet (ISP)

- **Abusos**
  - Ataques de negação de serviço
  - Mineração não autorizada de criptomoeda
  - Propagação de *malware*, *spam*
  - *A*lteração de DNS para ataques de *phishing*, etc
- **Impactos operacionais e de negócios**
  - Comprometimento da rede do provedor
  - Degradação ou indisponibilidade de serviços
  - Suporte técnico e trabalho de reparo
  - Problemas de reputação

- **Ação da comunidade via grupos de Trabalho do LACNOG[1]**
  - **LAC-AAWG** (Latin America and Caribbean Anti-Abuse Working Group)
  - **BCOP** (Best Current Operational Practices) ou Melhores Práticas Operacionais Atuais
    - É uma forma de documentar boas práticas relativas à questões operacionais de redes[2].
    - É desenvolvida pela comunidade (operadores, engenheiros, etc) por meio de grupos de trabalho (Working Groups)
    - Similar às BCPs do IETF, mas com foco em operações e não em especificação de protocolos

[1] Grupo de Operadores de Redes da América Latina e o Caribe (LACNOG) https://www.lacnog.net/
[2] Iniciativa original do RIPE NCC (https://www.ripe.net/participate/ripe/tf/bcop)

BCOP Requisitos de Segurança em CPE
A Construção do Documento

- Outubro 2017 – LACNIC28 / LACNOG 2017, Montevideo
  - Discussões iniciais e voluntários para desenvolver o documento.
- Abril 2018 – Primeiro draft para comentários
  - Principais problemas identificados:
    - Credenciais padrão para um grande número de dispositivos
    - Credenciais que não podem ser alteradas (*hard-coded*)
    - Uso de protocolos e algoritmos obsoletos e inseguros
    - Acessos não documentados (*backdoors*)
    - Falta de mecanismo de atualização automatizado e seguro para tratar problemas de segurança
    - Serviços desnecessários e/ou inseguros ativados por padrão
    - Serviços que não podem ser desativados
    - Gerenciamento remoto inseguro

BCOP Requisitos de Segurança em CPE
A Construção do Documento (cont.)

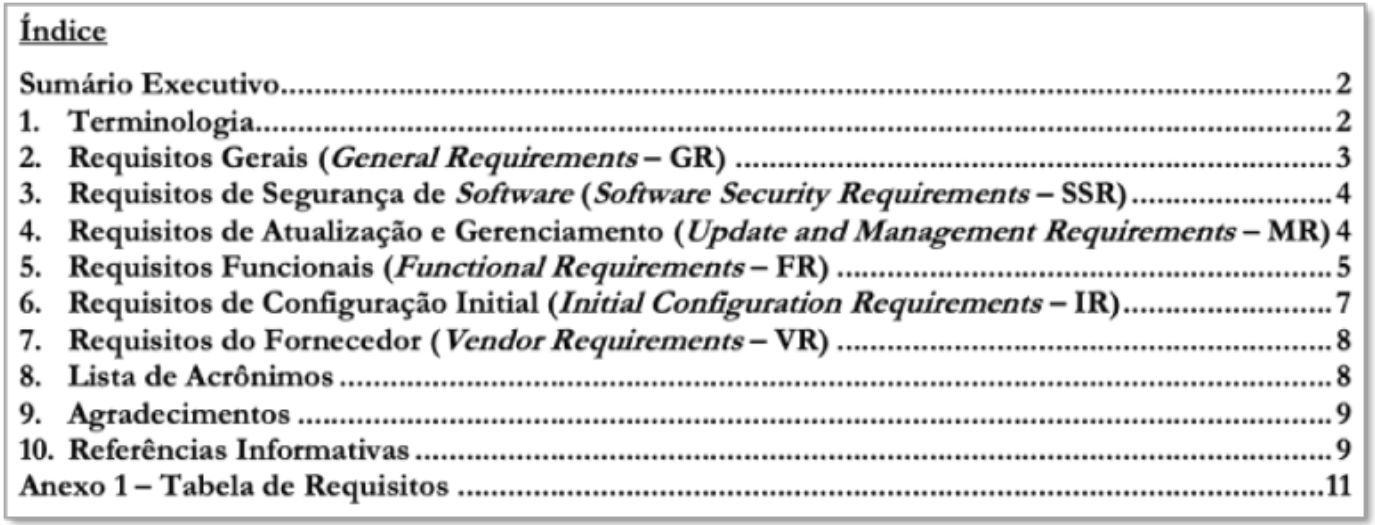
- Maio 2018 – LACNIC29, Panamá (1ª discussão presencial do draft-01)
  - Discutiu-se também questões relativas ao suporte à correções de segurança pelos fornecedores
  - M³AAWG manifesta interesse em fazer documento conjunto
- Junho 2018 – draft-02 para comentários /divulgação junto a operadoras e indústria
- Setembro 2018
  - Lançamento do draft-03 para comentários
  - Discussão presencial no LACNIC30 - LACNOG 2018, Rosario/AR
  - Longo período para comentários **(participação de colaboradores externos)**
- Dezembro 2018 – lançamento do draft-04
  - "Last Call" na lista BCOP
  - Encaminhado para **"Technical Review" pelo M³AAWG**
- Fevereiro 2019 – **reunião** M³AAWG45 San Francisco
- Março 2019 – **Drafts 05 e 06 (M³AAWG Comitê Técnico e *Senior Technical Advisors*)**
- 04 Abril 2019 – Draft-06 – **Aprovado pelo Board** do M3AAWG
- Abril/Maio 2019 – Drafts 07 e 08 – **Trabalho Editorial**
- 06 Maio 2019 – **Publicação**, LACNIC31, Punta Cana/DR
- Traduções:
  - Japonês e Coreano (disponíveis);
  - Português e Espanhol (em fase final de revisão);
  - Alemão e Francês (por vir)

A estrutura da BCOP

Um *checklist* de referência para decisões de hardware

→ Pedir aos fornecedores produtos melhores

→ **segurança por padrão**



Índice

https://www.lacnog.net/docs/lac-bcop-1

https://www.m3aawg.org/CPESecurityBP

Traduções:

https://www.m3aawg.org/published-documents

Conclusões

- Suporte e maturidade dos fornecedores é essencial
  - *Firmware* é *software*: sempre haverá erros a serem corrigidos
  - Correção rápida é primordial
- Os CPEs necessitam
  - Mecanismos automáticos de atualização
  - Gerência remota segura