nic.br cgi.br | cert.br

Live Intra Rede – Principais Ataques na Internet

30 de setembro de 2020

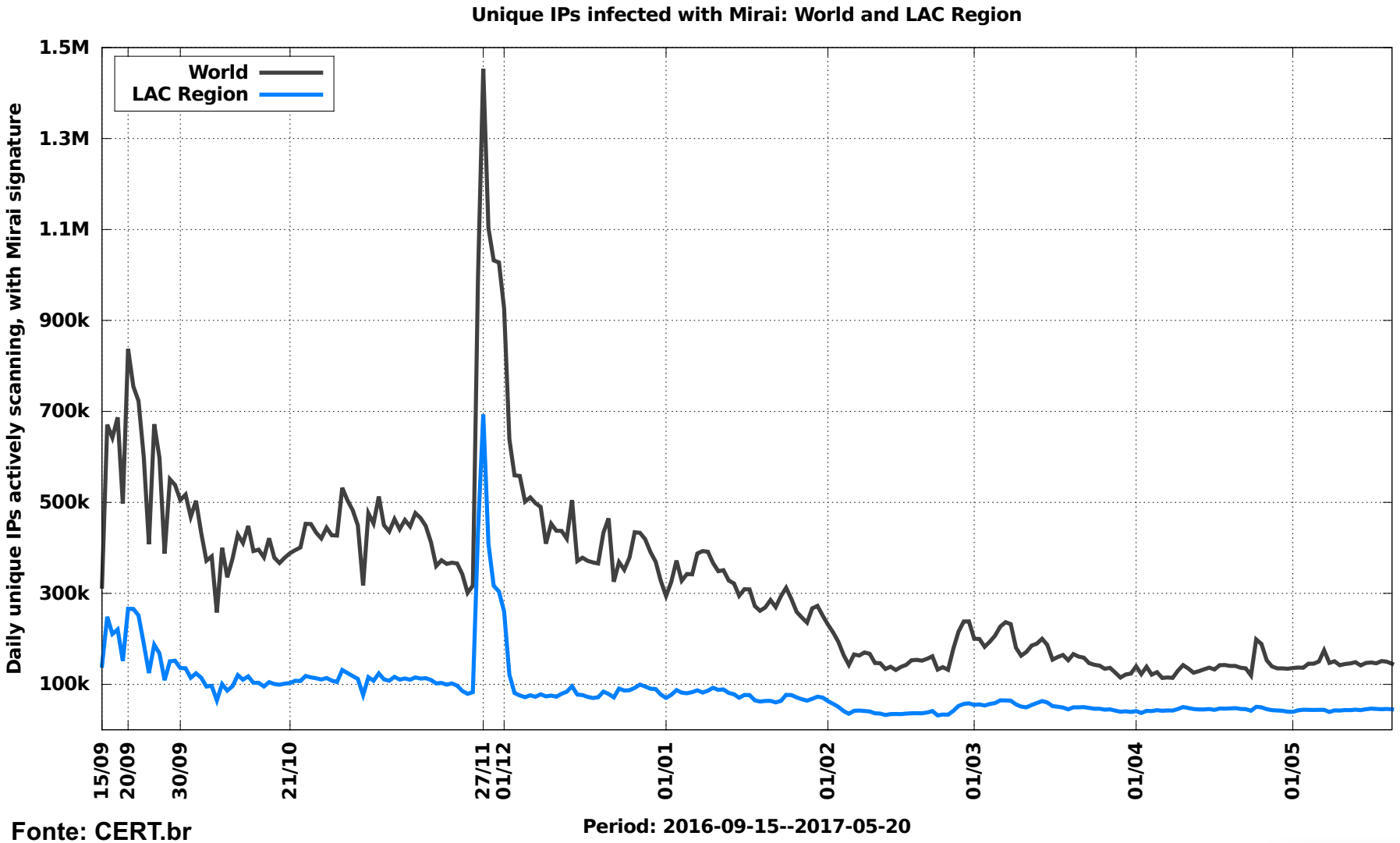
Evento *Online*

Requisitos Mínimos de Segurança para Aquisição de CPE LAC-BCOP-1

Lucimara Desiderá, M.Sc
Analista de Segurança
lucimara@cert.br

cert.br nic.br cgi.br

Malware Mirai
Dispositivos Infectados



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

CPE (Customer Premise Equipment) é o equipamento utilizado para conectar assinantes à rede de um Provedor de Serviços de Internet (ISP). Ex: modems, roteadores WiFi, etc.

(In)Segurança em IoT

Segurança é negligenciada

- até mesmo em dispositivos de segurança!
- é problema da equipe de segurança

Maioria dos fabricantes ainda repete velhos erros:

- autenticação falha ou inexistente
  - com senhas padrão comum, senhas *hardcoded*, contas ocultas (*backdoors*)
- protocolos obsoletos, sem criptografia (ex: Telnet)
- serviços desnecessários ativos por padrão

Poucos fabricantes possuem ciclo de vida de suporte/*updates*

- mecanismo de *bug report*
- distribuição de *updates*
- políticas claras

Por que se preocupar com Segurança de CPE?

Impactos operacionais e de negócios para os provedores (*ISPs*):

Comprometimento da rede do provedor

- Alguém está (ab)usando seus recursos para desferir ataques

Degradação ou indisponibilidade de serviços

- Você pode perder clientes

Suporte técnico e trabalho de reparo

- Você está perdendo dinheiro

Proteja a reputação do seu ISP

- Clientes, parceiros e listas negras

É melhor prevenir do que remediar

- Mitigar DDoS é muito custoso. É melhor evitar que o tráfego malicioso se propague.

O que devemos demandar de Desenvolvedores/Fabricantes/Indústria

Segurança *by design* e *by default*

- não opcional
- considerar requisitos de segurança desde o início projeto
- usar boas práticas de desenvolvimento seguro
- configurações padrão de fábrica seguras
  - restritiva ao invés de permissiva
  - *anti-spoofing*

***Updates* e gerenciamento remoto**

- Deve ser possível e deve ser seguro (*supply chain attacks*)

Planejar para fazer *updates* em larga escala

Ter grupo de resposta a incidentes de segurança em produto preparado para lidar com os problemas (PSIRT)➔ Maturity

Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Requisitos mínimos de segurança:

- Um *checklist* de referência para aquisição de equipamentos

Trabalho desenvolvido no LAC-AAWG – *Latin American and Caribbean Anti-Abuse Working Group*

- Editora: Lucimara, *Chair* LAC-AAWG / CERT.br

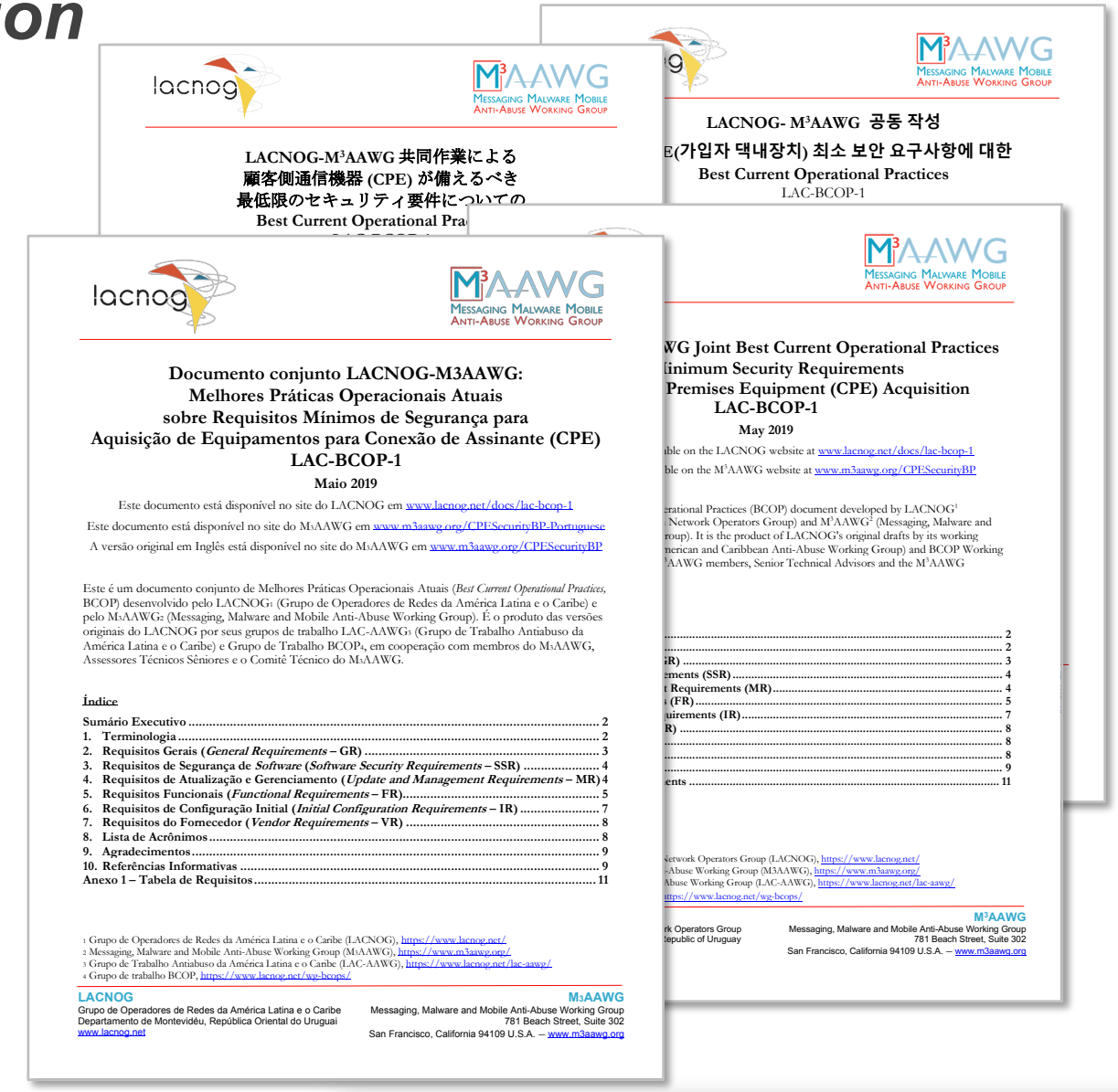
Publicação conjunta:

- **M³AAWG** - *Messaging, Malware and Mobile Anti-Abuse Working Group*
- **LACNOG** - *Latin American and Caribbean Network Operators Group*

Disponível em:

Português, Inglês, Japonês e Koreano

www.m3aawg.org/CPESecurityBP
www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP-Portuguese



Obrigada!

lucimara@cert.br

Notificações para: cert@cert.br

@certbr

www.cert.br

30 de setembro de 2020

nic.br cgi.br

www.nic.br | www.cgi.br