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

Lucimara Desiderá[1,2], Klaus Steding-Jessen[1], Cristine Hoepers[1]

[1]Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)
Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
São Paulo – SP – Brasil

[2]Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG)
Latin American and Caribbean Network Operators Group (LACNOG)
Department of Montevideo – Oriental Republic of Uruguay

{lucimara,jessen,cristine}@cert.br

Abstract. *Due to vulnerabilities in CPEs' embedded software and default configuration, these devices have been the target of several types of abuse. This scenario, that entails additional costs to Internet Service Providers, has been the motivation for several anti-abuse and network operators' working groups to come together and define a set of minimum security requirements for CPEs. This paper is a case study, which describes the process of building these security requirements in a multistakeholder working group, that had the participation of professionals with different expertise areas and from several countries. We also present the main consensus points, that are part of the final recommendations of the working group.*

Resumo. *Devido a vulnerabilidades no software embarcado e nas configurações padrão, CPEs (Computer Premises Equipments) têm sido alvo de uma variedade de abusos. Este cenário, que traz prejuízos diversos aos provedores de acesso, motivou diversos grupos de trabalho anti-abuso e de operações de rede a reunir-se e definir um conjunto de requisitos mínimos de segurança para estes dispositivos. Este artigo é um estudo de caso, que descreve o processo de construção destes requisitos em um grupo de trabalho multissetorial e com participação de profissionais de diversos países e especialidades. Também são apresentados os principais pontos que foram consenso e que fazem parte da recomendação final deste grupo de trabalho.*

1. Introdução

CPE (do inglês *Customer Premise Equipment*) é o equipamento utilizado para conectar assinantes à rede de um Provedor de Serviços de Internet (*Internet Service Provider* — ISP). Exemplos de CPE incluem *modems* (cabo, xDSL, fibra) e roteadores WiFi, entre outros.

Devido a vulnerabilidades no *software* embarcado e nas configurações padrão, os CPEs têm sido alvo de uma variedade de abusos, que vão desde a exploração de serviços mal configurados e de credenciais de autenticação padrão, até o completo comprometimento por *malware*. O objetivo de muitos desses abusos é conduzir ataques de negação

de serviço (DoS), mineração não autorizada de criptomoeda, propagação de *malware*, *spam*, alteração de servidores DNS para facilitar ataques de *phishing*, entre outros abusos [Vixie et al. 2014].

Nos últimos anos tem crescido a exploração de dispositivos com software embarcado para a criação de *botnets* para os mais diversos fins. Um subconjunto destes dispositivos, os CPE, tem sido comprometidos também para alteração de suas configurações de servidor DNS, de maneira que todos os dispositivos que estão em uma mesma residência ou estabelecimento comercial tenham partes de suas consultas respondidas de forma maliciosa.

Este cenário, que traz prejuízos diversos aos provedores de acesso, motivou diversos grupos de trabalho anti-abuso e de operações de rede a reunir-se e definir um conjunto de requisitos mínimos de segurança. Estes requisitos enfatizam a necessidade de gerência remota de dispositivos e uma postura proativa por parte dos fabricantes com relação ao tratamento de vulnerabilidades e a disponibilização de correções de segurança.

Neste artigo descrevemos o processo de construção destes requisitos em um grupo de trabalho multissetorial e com participação de profissionais de diversos países e especialidades. Também são apresentados os principais pontos que foram consenso e que fazem parte da recomendação final deste grupo de trabalho.

2. Identificação da Necessidade de uma Recomendação Global

Embora ataques a CPEs estivessem ocorrendo desde 2015 para alteração de servidores DNS, bem como *botnets* em sistemas embarcados já fossem de conhecimento há algum tempo, em novembro de 2016 ocorreu o primeiro caso de repercussão global que levou à instabilidade de um ISP. No dia 26 de novembro de 2016 foi liberado na Internet uma variante do *malware* Mirai que explorava uma vulnerabilidade no protocolo de gerência remota de uma versão específica de *chipset*, que era utilizada por diversos fabricantes de CPEs [Hoepers 2016, Hoepers 2017].

A Figura 1 possui dados da evolução da propagação da *botnet* Mirai desde o dia 15 de setembro de 2016, até o dia 20 de maio de 2017, conforme dados coletados pelo Projeto Honeypots Distribuídos do CERT.br[1]. Neste gráfico podemos ver que a taxa de IPs infectados tentando a propagação sofre um aumento repentino iniciado no dia 26 de novembro de 2016, com um pico no dia 27 de novembro. Também é possível observar que, apesar das notícias da mídia repercutirem que o caso afetou apenas operadoras da Europa, como a operadora alemã Deutsch Telecom, os IPs alocados à região da América Latina e Caribe (linha azul no gráfico) seguiram o mesmo padrão, sugerindo que ISPs da nossa região também foram afetados pela mesma vulnerabilidade.

Estes dados foram apresentados nas reuniões do Grupo de Trabalho "*Latin America and Caribbean Anti-Abuse Working Group* (LAC-AAWG)"[2], grupo que faz parte do LACNOG[3], fórum de operadores de redes da região atendida pelo LACNIC[4], e na reunião do Grupo de Trabalho de Engenharia e Operação de Redes do Brasil, GTER

[1] `https://honeytarg.cert.br/honeypots/`
[2] `https://www.lacnog.net/lac-aawg/`
[3] `https://www.lacnog.net/`
[4] `https://www.lacnic.net/`

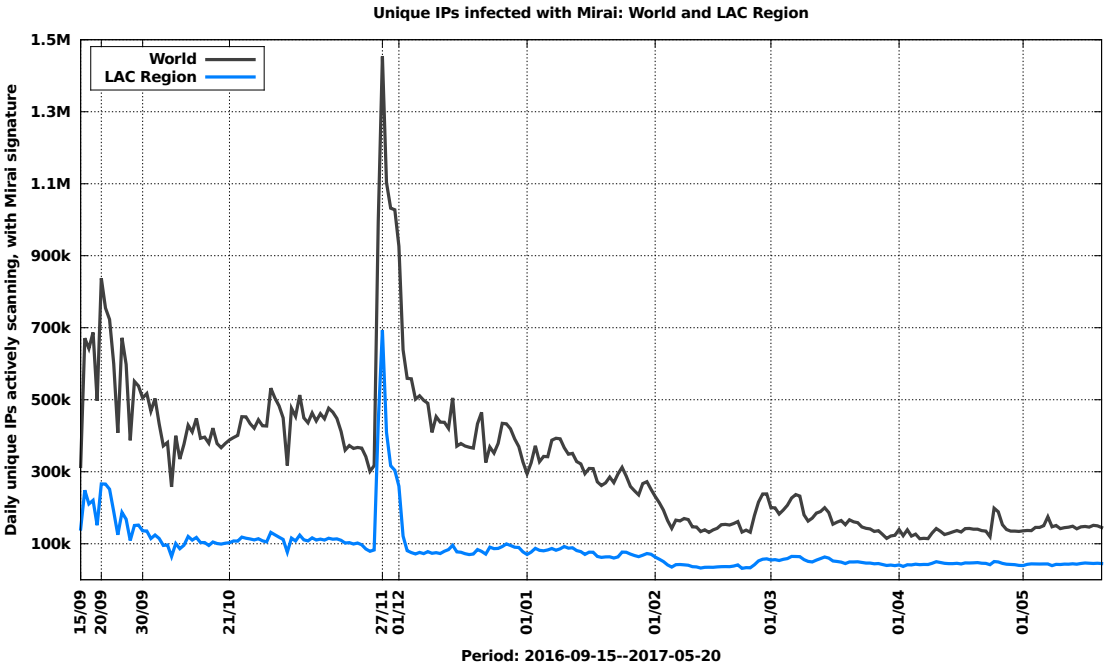

Figura 1. Endereços IP únicos, por dia, realizando varreduras com a assinatura característica da propagação da *botnet* Mirai. Fonte: [Hoepers 2017]

43 [O'Flaherty and Desiderá 2017]. Nestas reuniões também foram discutidos outros desafios em comum dos ISPs da região com relação à segurança de CPEs, incluindo a dificuldade de contato com os fabricantes, a dificuldade de especificar requisitos de segurança e de identificar versões de *firmware* executando em equipamentos dos diversos fabricantes.

Com base em todos estes pontos, na reunião de outubro de 2017 do LAC-AAWG, foi decidido que a primeira boa prática a ser desenvolvida seria um conjunto de requisitos mínimos de segurança que deveriam ser levados em conta no momento da aquisição de CPEs por ISPs [Desiderá 2018].

3. A Construção do Documento de Requisitos Mínimos de Segurança para Aquisição de CPEs

O produto final deste trabalho foi o desenvolvimento do documento "*LACNOG-M3AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition*" [LACNOG/M3AAWG 2019]. Este é um documento conjunto de Melhores Práticas Operacionais Atuais (*Best Current Operational Practices*, BCOP) desenvolvido pelo LACNOG e pelo M3AAWG. É o produto das versões originais do LACNOG por seus grupos de trabalho LAC-AAWG (Grupo de Trabalho Antiabuso da América Latina e o Caribe) e Grupo de Trabalho BCOP, em cooperação com o M3AAWG.

A escrita do documento teve início logo após a reunião de outubro de 2017 do LAC-AAWG. A maior parte dos trabalhos foi realizada online, através de listas de discussão por e-mail, seções de vídeo-conferência e da construção de rascunhos via plataforma *online*. O primeiro rascunho foi divulgado em abril de 2018 e discutido na reunião

presencial do LACNIC em maio de 2018.

Nestas primeiras discussões o maior foco foi em fazer um diagnóstico dos principais problemas encontrados pelos ISPs da região com os seus fornecedores de CPEs, bem como identificar quais as fraquezas mais exploradas pelos códigos maliciosos e possíveis mitigações. Neste processo foram elencadas as vulnerabilidades mais comuns presentes em CPEs:

- 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 corrigir problemas de segurança;
- Serviços desnecessários e/ou inseguros ativados por padrão;
- Serviços que não podem ser desativados;
- Gerenciamento remoto inseguro.

Após a reunião de maio de 2018, onde participaram também colaboradores de outras regiões, ficou evidente que o problema não era restrito à região da América Latina e Caribe e, a partir de então, o documento passou a ser desenvolvido para ser uma publicação do LACNOG em conjunto com o M3AAWG (*Messaging, Malware and Mobile Anti-Abuse Working Group*).

Nestas discussões também ficou claro que, do ponto de vista operacional e de resiliência para os ISPs, é muito importante que eles tenham a habilidade de instalar atualizações de *firmware* de forma ágil, bem como ter contatos com os fabricantes para notificações de vulnerabilidades e incidentes. Estes pontos também foram integrados ao documento, que passou a enfatizar o aspecto de maturidade de processos por parte dos fabricantes.

No mês de junho o segundo rascunho foi fechado e, neste ponto, foi feita uma divulgação mais ampla entre as operadoras de telecomunicações brasileiras, através do SindiTelebrasil[5], e entre os provedores de acesso nacionais, através das associações de provedores Abranet e Abrint. De forma similar, muitos profissionais de ponta em diversas áreas correlatas foram contatados e forneceram sugestões e revisões.

Todas as sugestões foram incorporadas no documento público, que teve seu terceiro rascunho discutido presencialmente na reunião de setembro do LACNIC/LACNOG. Esta versão ficou aberta para comentários até dezembro de 2018, período em que todos os comentários foram discutidos *online*.

Um quarto rascunho foi construído com base nas discussões e encaminhado para discussão e revisão pelo Comitê Técnico do M3AAWG pelo seu grupo de *Senior Advisors*[6]. Esta discussão levou a mais 2 rascunhos, discutidos *online* e na reunião presencial do M3AAWG de fevereiro de 2019. Cabe destacar também a participação ativa, ao longo do processo, de profissionais de organizações como o CERT Coordination Center e CableLabs.

[5] Sindicato Nacional das Empresas de Telefonia e de Serviços Móvel Celular e Pessoal

[6] `https://www.m3aawg.org/SeniorAdvisors`

3.1. Publicação, Divulgação e Aceitação do Documento

A aprovação final pela Diretoria do M3AAWG se deu em 04 de abril, seguida pela aprovação pela Diretoria do LACNOG, com a publicação da versão final [LACNOG/M3AAWG 2019], em inglês, nas páginas de ambas as organizações no dia 06 de maio de 2019.

Grande parte da divulgação se deu por meio de listas técnicas de operadores de redes e ISPs, seguido de *release* para imprensa de abrangência internacional. A aceitação por parte do público técnico foi grande e levou a solicitações para traduzir o material para outros idiomas: alemão, coreano, espanhol, francês, japonês e português.

4. Requisitos de Segurança Identificados

Embora o foco deste artigo seja descrever o processo de desenvolver uma recomendação envolvendo diversas organizações de diversos países, cabe ressaltar que a maior parte dos especialistas consultados, muitos deles especialistas em análise de vulnerabilidades e coordenação com fabricantes, destacaram a impossibilidade de garantir a segurança dos sistemas e a importância de mecanismos de atualização rápida.

Grande parte dos requisitos aborda questões de maturidade de processos e funcionalidades de segurança que devem ser implementadas nos produtos, destacando aspectos de segurança por projeto e por padrão. Desta forma os requisitos foram divididos nas sequintes categorias:

- Requisitos Gerais (*General Requirements* – GR): descreve requisistos relacionados com a transparência com relação a componentes utilizados, dependências de *software* e licenças;
- Requisitos de Segurança de *Software* (*Software Security Requirements* – SSR): descreve boas práticas de desenvolvimento de *software* relacionadas com proteção de dados e credenciais;
- Requisitos de Atualização e Gerenciamento (*Update and Management Requirements* – MR): descreve os requisitos para realização de atualizações e gerenciamento remoto de forma segura;
- Requisitos Funcionais (*Functional Requirements* – FR): descreve características e/ou serviços e funcionalidades que devem estar presentes ou que devem ser removidos dos CPEs;
- Requisitos de Configuração Inicial (*Initial Configuration Requirements* – IR): descreve as configurações padrão de fábrica seguras que o dispositivos deve ter;
- Requisitos do Fornecedor (*Vendor Requirements* – VR): descreve requerimentos relacionados com política de suporte, política de tratamento de vulnerabilidades, ponto de contato para tratar de vulnerabilidades e divulgação de informações sobre correções de segurança e atualizações.

5. Conclusões

Durante este trabalho diversos desafios para manutenção de um parque seguro de CPEs por parte dos ISPs foram levantados. Embora não haja espaço no artigo para que enumeremos todos os desafios encontrados, cabe destacar que um dos pontos mais importantes levantado por todos foi a necessidade de atualização rápida e gerência remota destes dispositivos.

Num cenário de redes fortemente conectadas e de diversidade dos dispositivos conectados, este trabalho foi mais um a levantar a necessidade de requisitos de maturidade e processos por parte de fabricantes, mais do que a necessidade de certificação de *hardware* e *software*. Porém, ao mesmo tempo, todos levantaram a preocupação de que tais requisitos não elevem demasiado o custo dos equipamentos.

Os autores esperam, com este artigo, trazer esta experiência para a comunidade e levantar a discussão sobre definição de requisitos mínimos de segurança, com foco em mecanismos robustos de atualização e maturidade de processos por parte do fabricante. Não menos importante é o papel de usuários de tecnologia na identificação de problemas e na proposta de requisitos mínimos, pois são eles que sofrem o impacto operacional dos problemas de segurança.

Referências

Desiderá, L. (2018). BCOP Requisitos de Segurança em CPE: Um Pouco de História. IX Fórum 12. Disponível em: https://forum.ix.br/2018/.

Hoepers, C. (2016). Problemas de Segurança e Incidentes com CPEs e Outros Dispositivos. 20º Fórum de Certificação para Produtos de Telecomunicações. Disponível em: https://www.cert.br/docs/palestras/certbr-forum-anatel2016.pdf.

Hoepers, C. (2017). Notable trends in Brazil: BGP hijacking for financial fraud and the evolution of Mirai. 2017 Annual Meeting of CSIRTs with National Responsibility. Disponível em: https://www.cert.br/docs/palestras/certbr-natcsirts2017-1.pdf.

LACNOG/M3AAWG (2019). LACNOG-M3AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition. Best Current Operational Practices, LACNOG/M3AAWG. https://www.m3aawg.org/CPESecurityBP.

O'Flaherty, C. and Desiderá, L. (2017). Boas Práticas e Cooperação na Luta Contra Abusos de Rede. GTER 43. Disponível em: ftp://ftp.registro.br/pub/gter/gter43/05-LAC-AAWG.pdf.

Vixie, P., King, C., and Spring, J. (2014). Abuse of Customer Premise Equipment and Recommended Actions. Technical Report CERTCC-2014-48, SEI/CMU. https://resources.sei.cmu.edu/asset_files/WhitePaper/2014_019_001_312679.pdf.