News Release - For Immediate Release

Recomendações Mínimas de Segurança em Roteador Doméstico Definidas nas Novas Práticas Conjuntas LACNOG e M³AAWG

MONTEVIDÉU, Uruguai e SÃO FRANCISCO, 2019/06/03–As novas recomendações de melhores práticas para os provedores de serviços de Internet (ISPs, na sigla em inglês) publicadas pelo LACNOG (Grupo de Operadores de Rede da América Latina e o Caribe) e M³AAWG (*Messaging, Malware and Mobile Anti-Abuse Working Group*) este mês definem os critérios básicos de segurança para os roteadores domésticos e outros equipamentos para conexão de usuário (*customer premise equipment,* CPE) e espera-se que ajudem a proteger a Internet contra ataques comuns, especialmente ataques de negação de serviço (DoS, na sigla em inglês) resultantes do abuso desses dispositivos. As recomendações fortalecerão os esforços de segurança dos provedores de serviço de Internet ao identificar requisitos para os dispositivos de *hardware* conectados às suas redes, que são suscetíveis à exploração quando proteções básicas são ignoradas.

O documento conjunto LACNOG-M3AAWG de Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de *Customer Premise Equipment* (CPE) está sendo traduzido para diversos idiomas para uso pelos ISPs do mundo todo. Ele foi publicado pelo Grupo de Operadores de Rede da América Latina e Caribe e o *Messaging, Malware and Mobile Anti-Abuse Working Group* e está disponível em http://www.lacnog.net/docs/lac-bcop-1 e www.m3aawg.org/CPESecurityBP ou com atuais traduções em https://www.m3aawg.org/published-documents.

As configurações de segurança e funcionalidades recomendadas são baseadas na experiência do setor e são essenciais para prevenir os ataques de negação de serviço (DoS) que fazem uso de dispositivos de infraestrutura de rede vulneráveis, dispositivos da Internet das Coisas (*Internet of Things*, IoT) e infecções por *malware*. Uma tabela de requisitos é fornecida para ajudar os ISPs a customizarem as recomendações de segurança para suas redes em um formato conciso que eles possam fornecer aos fabricantes de CPE.

Esforço mundial para fortalecer a proteção on-line

O documento atualmente está sendo traduzido para o português, espanhol, francês, alemão e japonês, e espera-se que outros idiomas venham a seguir. As melhores práticas traduzidas serão úteis no mundo todo como uma ferramenta para os ISPs estabelecerem requisitos para padrões de fábrica seguros para os CPEs que eles conectarão às suas redes, de acordo com a editora do documento, Lucimara Desiderá, coordenadora do Grupo de Trabalho Antiabuso da América Latina e Caribe (LAC-AAWG) e analista de segurança do CERT.br (o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil).

"Equipes de resposta a incidentes de segurança de computadores da América Latina identificaram a falta de segurança em CPEs como um problema sério em ataques nos últimos anos. Essas novas boas práticas irão facilitar para os ISPs negociarem com os fornecedores de CPE para garantir que os equipamentos que eles conectam às suas redes atendem a requisitos mínimos de segurança, o que ajudará a reduzir o número e a intensidade dos ataques na Internet como um todo e, consequentemente, o impacto negativo que causam nas operações dos ISPs", disse Desiderá.

As diretrizes abrangem documentação e informações de contato do fornecedor, segurança de *software*, funcionalidades de atualização e de gerência remota de dispositivo, preferências de configuração padrão, e políticas de suporte relacionadas às correções de segurança. Dentre as recomendações:

- As senhas não devem ser codificadas no *firmware*, precisam ser alteráveis e os fornecedores não devem usar a mesma senha padrão para todos os dispositivos.

- É preciso haver um mecanismo para atualizações remotas periódicas de *software*, incluindo um método para verificar a autenticidade do arquivo de atualização.
- O equipamento deve ser configurado restritivamente em vez de configurado permissivamente.

Como um exemplo do escopo do problema, o *malware* Mirai, responsável por grandes ataques a *sites* web, contém uma tabela de mais de 60 nomes de usuários e senhas comuns padrão de fábrica que ele utiliza para acessar e infectar câmeras de segurança domésticas, roteadores domésticos e outros dispositivos IoT. As novas recomendações tornarão a tabela de *login* ineficaz, de acordo com o presidente do conselho do M³AAWG, Severin Walker.

Walker disse, "A colaboração do M³AAWG com o LACNOG e seus Grupos de Trabalho neste documento foi uma prioridade, em parte, por causa do nosso trabalho contínuo com grupos de operadores de rede e de resposta a incidentes regionais para lidar com as ameaças globais às comunicações seguras. Isso também foi importante porque precisamos continuar a evoluir o foco dos nossos membros na segurança dos dispositivos IoT, dispositivos móveis e outros dispositivos do consumidor, a fim de ajudar a prevenir ataques cada vez maiores originados a partir deles".

O documento das melhores práticas foi desenvolvido pelo LACNOG e M³AAWG e publicado na reunião LACNIC 31 na República Dominicana em 8 de maio. Ele se baseia na expertise dos grupos de trabalho do LACNOG, LAC-AAWG e grupo de trabalho BCOP, em cooperação com os membros do M³AAWG, seus assessores técnicos seniores e o comitê técnico da M³AAWG.

Sobre a LACNOG

LACNOG (www.lacnog.net) é o Grupo de Operadores de Rede da América Latina e do Caribe, conta com um Conselho de Administração, um Comitê de Programa e Grupos de Trabalho. Ele fornece um ambiente para que os operadores de rede e qualquer parte interessada troquem experiências e conhecimento através de listas de e-mail, grupos de trabalho e reuniões anuais. O LACNOG também promove Grupos de Operadores de Rede (*Network Operators Groups*, NOGs) locais e fóruns de interconexão (*peering*), o desenvolvimento e a adoção das melhores práticas e atividades de treinamento técnico e tutoriais.

Sobre o *Messaging, Malware and Mobile Anti-Abuse Working Group* (M³AAWG)

O *Messaging, Malware and Mobile Anti-Abuse Working Group* (M³AAWG) é onde a indústria se reúne para trabalhar contra *bots*, *malware*, *spam*, vírus, ataques de negação de serviço e outras explorações on-line. Os membros do M³AAWG (www.m3aawg.org) representam mais de dois bilhões de caixas de mensagens de alguns dos maiores operadores de rede do mundo. Ele tira proveito do conhecimento e da experiência dos seus membros globais para combater o abuso nas redes existentes e novos serviços emergentes por meio de tecnologia, colaboração e políticas públicas. Ele também trabalha para educar os elaboradores de políticas globais sobre os problemas técnicos e operacionais relacionados aos abusos on-line e ao envio e recebimento de mensagens. Com sede em São Francisco, Califórnia, M³AAWG é impulsionada pelas necessidades do mercado e apoiada pelos principais operadores de rede e provedores de serviço de troca de mensagens.

# # #

Conselho de Administração e patrocinadores do M³AAWG : 1 & 1 Internet SE; Adobe Systems Inc.; AT&T Comcast; Endurance International Group; Facebook; Google, Inc.; LinkedIn; Mailchimp; Marketo, Inc.; Microsoft Corp.; Orange; Proofpoint; Rackspace; Return Path, Inc.; SendGrid, Inc.; Vade Secure; Valimail; VeriSign, Inc.; e Verizon Media (Yahoo & AOL).

Membros efetivos do M³AAWG: Agora, Inc.; Broadband Security, Inc.; Campaign Monitor; Cisco Systems, Inc.; CloudFlare, Inc.; dotmailer; eDataSource Inc.; ExactTarget, Inc.; IBM; iContact; Internet Initiative Japan (IIJ); Liberty Global; Listrak; Litmus; McAfee; Mimecast; Oracle Marketing Cloud; OVH; Spamhaus; Splio; Symantec; USAA; e Wish.

Uma lista completa dos membros está disponível em http://www.m3aawg.org/about/roster.

Contato de mídiat: Astra Communications, Linda Marcus, APR, LMarcus@astra.cc, +1-714-974-7973 (U.S. Pacific)