News Release

For Immediate Release

MAAWG ataca bots com a nova orientação para ISP para restauração das máquinas infectadas dos usuários finais

Recomendações para a indústria podem melhorar a remoção do bot para o consumidor

SÃO FRANCISCO, 31 de julho /PRNewswire/ -- Com o crescente problema de infestação de bot contribuindo para spam, roubo de identidade e fraude online, o Messaging Anti-Abuse Working Group (MAAWG - Grupo de Trabalho de Antiabuso de Mensagens) emitiu seu primeiro documento de melhores práticas buscando ajudar o trabalho global da indústria de ISP mais estreitamente com os consumidores para reconhecer e remover as infecções bot das máquinas dos usuários finais. Este documento apresenta uma abordagem de três etapas com recomendações para a detecção do bot, notificação dos usuários sobre o problema com o computador, e orientação sobre como remover o malware.

O bot, ou malware rodado nos computadores dos usuários sem o seu conhecimento, é responsável pela geração de 90 por cento de spam e também pode ser usado para roubar informação pessoal ou fazer parte de ataques DDOS (distributed denial of service - negação distribuída de serviço). O Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks (Melhores Práticas Comuns para Atenuação de Infecção de Bot em Larga Escala de Redes Residenciais) (Versão 1.0) do MAAWG apresenta as estratégias usadas por alguns dos maiores ISPs do mundo, no entanto, ele foi desenvolvido para ser adaptado para operadoras de redes menores e para levar em consideração as diferenças jurídicas e de processo dos países.

"O Bot provoca uma aflição global e estas melhores práticas são uma etapa importante na informação da indústria sobre os processos apropriados para ajudar a proteção dos consumidores. Estamos compartilhando a experiência dos nossos membros globais para que as operadoras de rede de todo o lugar possam atacar este problema com maior agressividade. Como indústria, estamos nos tornando mais pró-ativos ao alertar os clientes quando os bots são detectados nos seus computadores e ao ajudar os usuários a remover o malware antes que ele possa afetá-los", disse o Chairman do MAAWG, Michael O'Reirdan.

As novas melhores práticas apresentam várias opções de alerta para os clientes quando seus computadores são infectados e sugestões de como ajudar os usuários finais a limparem seus sistemas. O documento discute os métodos de detecção do bot, notificação do cliente, e o uso da tecnologia walled gardens para limitar a exposição das máquinas infectadas na Internet. Algumas recomendações:

-- Além de proteger a privacidade dos usuários, as operadoras de rede podem usar várias ferramentas para detectar os computadores infectados dos usuários finais, incluindo DNS, escaneamento do espaço de PI para identificar os computadores vulneráveis, e a coleta de informação do tráfego de PI de endereços de comando e controle conhecidos.

-- Email, ligações para clientes, envio de correspondência e walled gardens, são ferramentas de notificação comuns, cada uma delas possuindo suas próprias considerações. As mensagens no navegador são consideradas um dos métodos mais eficientes para alertar os clientes, mas também podem ter uma implementação tecnicamente difícil.

-- Os ISPs têm que manter um portal de segurança bem divulgado, com instruções para a remoção do bot para o usuário final.

O documento também apresenta exemplos de mensagens para o usuário final e uma lista de ferramentas para detecção e remoção de malware. As melhores práticas continuarão a ser revisadas para indicar novos procedimentos e a evolução das novas ameaças de bots.

Usuários subestimam a ameaça do bot

Um bot que reside no computador do consumidor normalmente faz parte de uma rede maior de máquinas programadas para executar operações específicas e clandestinas sob o controle de um "botmaster" (mestre). O malware normalmente é instalado em máquinas de consumidores desavisados quando eles clicam em um email infectado ou baixam código ilícito de um Web site comprometido. O bot foi criado para operar sorrateiramente - por exemplo, envio de spam ou gravação de senhas e informação pessoal sem o conhecimento dos seus proprietários - dificultando que os usuários finais descubram que suas máquinas estão infectadas.

Enquanto que 80 por cento dos consumidores têm conhecimento do bot, somente 20 por cento acreditam que poderão ser infectados, de acordo com uma pesquisa do MAAWG publicada em julho (a pesquisa e seus releases estão disponíveis no www.MAAWG.org). "Os ISPs têm que adotar medidas para proteger os usuários, mas também precisam informar constantemente seus clientes e trabalhar em conjunto com eles para conter a propagação do bot", disse O'Reirdan.

As novas melhores práticas de atenuação do bot fazem parte do trabalho constante do MAAWG de confrontar o abuso de mensagens. Anteriormente, o MAAWG publicou as melhores práticas para a gestão da porta 25, uso da tecnologia walled garden, compartilhamento do espaço de endereço de PI, práticas de repasse de email, e melhores práticas de comunicação dos remetentes, dentre outros tópicos.

As Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks do MAAWG podem ser baixadas no Web site da organização no www.MAAWG.org. A pesquisa de consumidor do MAAWG, documentos publicados e melhores práticas também estão disponíveis no site.

Sobre o Messaging Anti-Abuse Working Group (MAAWG)

O Messaging Anti-Abuse Working Group (MAAWG - Grupo de Trabalho de Antiabuso de Mensagens) é onde a indústria de mensagens pode se unir para trabalhar contra spam, vírus, ataque de negação de serviço e outras explorações online. O MAAWG (www.MAAWG.org) representa quase um bilhão de caixas postais de algumas das maiores operadoras de rede do mundo. É a única organização a abordar o abuso de mensagens completamente, com o envolvimento sistemático de todos os aspectos do problema, incluindo tecnologia, colaboração da indústria e política pública. O MAAWG utiliza a abrangência e a experiência dos seus membros globais para atacar o abuso das redes existentes e dos novos serviços emergentes. Com sede em São Francisco, Calif., o MAAWG é um fórum aberto voltado para as necessidades do mercado e apoiado pelas principais operadoras de rede e provedores de mensagens.

# # #

CONTACTO: Linda Marcus, APR de Astra Communications, +1-714-974-6356, lmarcus@astra.cc/

MAAWG - Diretoria: AOL; AT&T (NYSE: T); Cloudmark, Inc.; Comcast (Nasdaq: CMCSA); Cox Communications; France Telecom (NYSE e Euronext: FTE); Goodmail Systems; Openwave Systems (Nasdaq: OPWV); Time Warner Cable; Verizon Communications; e Yahoo! Inc.

MAAWG - Membros integrais: 1&1 Internet AG; Bizanga LTD; Constant Contact; e-Dialog; Eloqua Corporation; Experian CheetahMail; Genius.com; Internet Initiative Japan, (IIJ Nasdaq: IIJI); IronPort Systems; McAfee Inc.; MX Logic; NeuStar, Inc.; Outblaze LTD; Return Path, Inc.; Spamhaus; Sprint; e Symantec

Uma lista complete dos membros está disponível no http://www.maawg.org/about/roster.