

Cada vez mais crackers buscam vulnerabilidades multiplataforma

Antone Gonsalves

Utilizando falhas já corrigidas por fornecedores, criminosos se aproveitam da negligência de usuários, que não atualizam seus softwares quando necessário

Cada vez mais crackers estão escolhendo como alvo as mesmas vulnerabilidade de aplicativos em Macs e Pcs com Windows, visando benefícios financeiros e para desenvolver malwares multiplataforma.

Essa tendência vem crescendo desde 2009, com documentos do Office. Outras multiplataformas, tecnologias de terceiros preferidas de hackers, incluem aplicativos como Java, Adobe PDF e Adobe Flash, afirmou a pesquisadora em segurança Methusela Cebrian Ferrer em um post no blog do Centro de Proteção contra Malware da companhia.

Escolhendo as mesmas falhas como alvo em aplicativos comumente utilizados por ambas as plataformas permite a crackers colher lucros duplos com um mesmo vírus. Essa tendência Ferrer chama de "economias de escala em vulnerabilidades multiplataforma". "Esse método de distribuição permite aos invasores aumentar sua capacidade em multiplataformas", disse.

Stephen Cobb, evangelista em segurança da ESET, disse que cibercriminosos têm tratado o desenvolvimento de malwares e métodos para infectar sistemas como um negócio por anos. "Podemos esperar para ver ainda mais a aplicação da lógica de negócios - tais como economias de escala, divisão de cálculos trabalhistas e de risco/recompensa - evoluindo nesse espaço", disse ele em entrevista por e-mail.

Entretanto, focando em vulnerabilidades que talvez já foram corrigidas por fornecedores, crackers contam com a negligência de usuários, que não atualizam seus softwares quando necessário.

Java

Por exemplo, pessoas são notoriamente lentas para instalar patches Java em PCs com Windows e Macs. Tanto que 60% das instalações do aplicativo nunca são atualizadas, segundo o fornecedor Rapid7. "Todos esses aplicativos não-atualizados no desktop, quaisquer que sejam, são alvos fáceis para ataques", afirmou Jamz Yaneza, gerente de pesquisas da Trend Micro.

A Microsoft apontou a última tendência enquanto investigava um malware chamado de Backdoor Olyx, identificado no ano passado. Desde então, variantes posteriores demonstraram a abordagem multiplataforma utilizadas por seus criadores.

Essas ameaças são tipicamente baixadas por vítimas ao clicarem em links maliciosos ou visitando sites corrompidos que distribuem o malware. Os Cavalos de Troia são também anexados em e-mails.

Por atacar vulnerabilidades conhecidas, a melhor forma de defesa ainda é manter seu software atualizado, instalando as últimas versões do sistema operacional e patches de segurança. "Essa prática deveria ser estendida a todos os dispositivos e plataformas, especialmente aqueles utilizados em redes corporativas", disse Ferrer.

As opções adicionais incluem desinstalar o Java. Enquanto a plataforma é muitas vezes necessária em servidores, sua importância tem diminuído em laptops e desktops que utilizam novas tecnologias web.

Para fazer o software mais seguro, usuários podem rodar aplicativos em configurações o mais seguras possível, de acordo com Wolfgang Kandek, chefe do escritório de tecnologia da Qualys. Ele notou, por exemplo, que usuários podem desativar o Javascript do Adobe Reader como uma maneira de reforçar a proteção do software.

Fonte: IDG Now. [Portal]. Disponível em:
<<http://idgnow.uol.com.br/internet/2012/08/01/cada-vez-mais-crackers-buscam-vulnerabilidades-multiplataforma/>>. Acesso em: 6 ago. 2012.

A utilização deste artigo é exclusiva para fins educacionais.