Análise sobre vulnerabilidades dos periféricos de entrada disponíveis para o público brasileiro

Guilherme Machado Leal da Silva , Emerson Ribeiro de Mello

Instituto Federal de Santa Catarina (IFSC)
Campus São José, São José, SC, Brasil

guii.leal@outlook.com, mello@ifsc.edu.br

Abstract. *Mousejack is a class of vulnerabilities that affects wireless devices such as mouses and keyboards that made use of proprietary communication protocolos instead of Bluetooth standard. This work aims to check if best seller wireless devices by Brazilian electronic commerce are still vulnerable.*

1. Introdução

A comunicação entre dispositivos de entrada sem fio como mouses, teclados ou passadores de apresentação e o computador pode ser feita por meio de receptores (*dongles*) conectados na porta USB do computador ou ainda por meio de conexões Bluetooth [Bluetooth 2003], que dispensa o uso de *dongles*, uma vez que todos os *laptops* modernos possuem uma interface Bluetooth por padrão. Para os dispositivos que não fazem uso do Bluetooth, cada fabricante implementa um protocolo de comunicação proprietário, que em alguns casos, faz uso de mecanismos criptográficos para garantir a confidencialidade e integridade das informações trocadas entre dispositivo sem fio e o seu receptor.

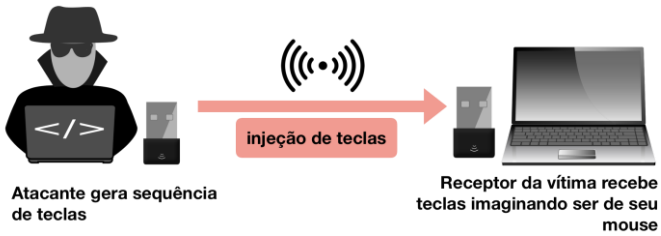

Figura 1. Personificação do dispositivo autêntico para injeção de comandos

Em [Newlin 2016] foi apresentado um conjunto de vulnerabilidades em dispositivos de entrada sem fio que implementam protocolos proprietários ao invés do Bluetooth. Os autores constataram que a maioria dos dispositivos vendidos na época estavam vulneráveis e era possível realizar ataques de **captura de tráfego**, quando se identifica os comandos enviados pelo dispositivo sem fio ao transmissor que está conectado no computador da vítima; **reenvio de comandos** (*replay attack*), quando o atacante retransmite um comando que originalmente foi criado pelo dispositivo sem fio da vítima; **injeção**, quando o atacante injeta comandos no receptor da vítima (Veja Figura 1).

A única forma de corrigir essas vulnerabilidades seria por meio de uma atualização de *firmware*. O fabricante Logitech, motivada pelo trabalho de [Newlin 2016], lançou em 2017 uma atualização de *firmware* para seus dispositivos [Logitech. 2017].

Nesse trabalho pretende-se investigar se mesmo após 2 anos desde a publicação do trabalho de [Newlin 2016], ainda existem dispositivos vulneráveis sendo comercializados para o público brasileiro.

2. Proposta

Para a concepção da amostra a ser analisada, buscou-se pelos dispositivos mais vendidos pelos principais *sites* de comércio eletrônico que são usados pelo público brasileiro. A lista de *sites* mais acessados por brasileiros foi obtida por meio do serviço de *ranking* Alexa [Amazon.com, Inc 2018]. Buscou-se ainda garantir que na amostra houvesse uma diversidade de marcas.

Para todos os dispositivos da amostra foi verificado se estavam vulneráveis aos ataques de captura, injeção e reenvio de comandos. Para realização dos experimentos foi feito uso do transmissor CrazyRadio PA[1], dos *softwares* originais do trabalho de [Newlin 2016], das variações destes feitas por Phikshun e Infamy[2], e também as feitas por Ck[3]. Os resultados dos experimentos são apresentados na Tabela 1.

Tabela 1. Modelos selecionados e resultados

Dispositivos			Ataques		
Marca	**Modelo**	**Tipo**	**Captura**	**Injeção**	**Reenvio**
C3 tech	AP-400	passador de *slides*	Não	Não	Não
Dell	KM-636	mouse & teclado	**Sim**	Não	Não
HP	Z-3700	mouse	Não	Não	Não
Logitech	M-170	mouse	**Sim**	**Sim**	**Sim**
Logitech	M-510	mouse	**Sim**	Não	**Sim**
Logitech	R-400	passador de *slides*	**Sim**	**Sim**	**Sim**
Logitech	K400+	teclado	**Sim**	Não	**Sim**
Leadership	Class	mouse	Não	Não	Não
Multilaser	MO-251	mouse	Não	Não	Não
Multilaser	MO-264	mouse	Não	Não	Não
MaxPrint	6012254	mouse	Não	Não	Não
Microsoft	1850	mouse	**Sim**	Não	Não

3. Considerações finais

Mesmo após 2 anos desde a publicação do trabalho de [Newlin 2016], alguns fabricantes ainda comercializam dispositivos vulneráveis. Apesar da Logitech ter lançado uma correção de *firmware*, constatou-se que essa nova versão não está presente nos dispositivos que foram adquiridos em junho de 2018. Notou-se que muitos dispositivos implementam criptografia, porém não validam a autenticidade das partes envolvidas.

Referências

Amazon.com, Inc (2018). Alexa, top sites in brazil. `https://www.alexa.com/topsites/countries/BR`.

Bluetooth, S. (2003). Bluetooth specification.

Logitech. (2017). Logitech response to research findings. `https://community.logitech.com/s/question/0D531000058b3B7CAI/logitech-response-to-research-findings`.

Newlin, M. (2016). Injecting keystrokes into wireless mice. *Bastille*.

[1] `https://www.bitcraze.io/crazyradio-pa`
[2] `https://github.com/insecurityofthings/jackit`
[3] `https://github.com/iamckn/mousejack_transmit`