Disseminação de Código Malicioso: firmware, o esconderijo ideal.

Ábner L. A. Pereira[1], Eloisa M. de M. Pereira[2], Juliana C. L. Paes[3], Rivaldo de S. Rodrigues[4], Taynara L. Costa[5]

1. Prof. / Orientador, Tecnólogo em Análise e Des. de Sistemas, Eixo Informação e Comunicação, IFPA – Breves
2. Estudante do Curso Técnico em Informática do IFPA – Breves; *eloh22mirandacn@gmail.com
3. Estudante do Curso Técnico em Informática do IFPA – Breves
4. Estudante do Curso Técnico em Informática do IFPA – Breves
5. Estudante do Curso Técnico em Informática do IFPA – Breves

Palavras Chave: *disseminação*, *firmware*, *malware*.

Introdução

No contexto atual, a falta de conhecimento entre os indivíduos de entidades educacionais sobre os riscos ao se manusear dispositivos removíveis, ajuda a propagar códigos maliciosos, fato que acaba acarretando perdas a estes usuários.

Atualmente a segurança de dispositivos USB (*Universal Serial Bus*) está cada vez mais se fragmentando, permitindo que códigos maliciosos se instalem no *firmware* (controlador que possui um conjunto de instruções usados para operar o *hardware*) dos dispositivos removíveis, não se limitando apenas às memórias *flash* (uma memória que possui como característica permitir a reprogramação de múltiplos endereços em uma só operação).

Como um *firmware* pode ser reprogramado, um código malicioso pode ser incluído, mas para que isso ocorra deve-se ter conhecimento da estrutura padrão deste, que ajuda a configurar os dispositivos, pois, não podem ser facilmente modificados pelos usuários, para que não venha comprometer seu bom funcionamento.

Embora saibamos que *malwares* estão presentes em nosso cotidiano, dependemos de *softwares* de proteção e até reformatação ocasional para manter os nossos dispositivos removíveis longe de se tornarem um transportador de "epidemia digitais". Mas, neste caso apresentado, acaba ficando difícil, pois esses males não residem na memória *flash* de dispositivos USB, mas no *firmware* – uma ROM (PROM, EPROM ou EEPROM), podendo permanecer escondidos.

Deste modo, este resumo vem contribuir com o objetivo de informar esta maneira de propagação de *malwares* para prevenir os indivíduos de entidades educacionais sobre como lidar com este problema.

Resultados e Discussão

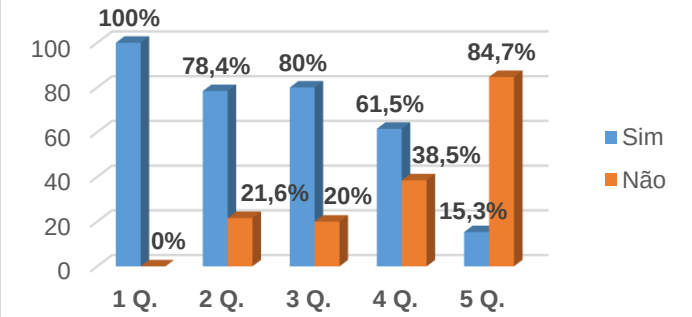
Para que os estudos viessem ter fundamentos durante o seu avanço foram realizadas pesquisas bibliográficas afim de aprofundar nosso conhecimento. Partindo disso, um questionário, com perguntas sobre possíveis fatores que levam à disseminação de códigos maliciosos (Tabela 1), foi elaborado e distribuído à comunidade do IFPA Campus Breves (funcionários e alunos).

Tabela 1. Perguntas realizadas através do questionário.

Nº	PERGUNTA
1	Você acha prático usar dispositivos USB?
2	Você tem a preocupação de saber se o lugar onde você conecta esse dispositivo removível é seguro?
3	Você sabe o que é código malicioso (vírus de computador)?
4	Você sabe como esses "vírus" se propagam?
5	Você sabe o que é *firmware*?

A partir do dados coletados foi possível realizar a criação de um gráfico que nos trouxe uma visualização macro do problema.

Gráfico 1. Nível de compreensão da comunidade do IFPA Campus Breves abstraído através do método utilizado.



Essa pesquisa comprovou que a maior parte dos entrevistados (84,7%) não sabe o que é *firmware*, uma vez que este é um assunto de interesse de todos que responderam ao questionário, pois, como mostra o gráfico 100% dos mesmos utilizam dispositivos removíveis. No entanto, 21,6% afirmaram não ter preocupação ao manusear seu dispositivo removível, isso reforça nosso intuito em alertar, de maneira geral, sobre como lidar com esta ameaça. Por fim, a porcentagem de pessoas que não conhecem como esses *malwares* se propagam (38,5%) nos chama a atenção, pois, entra em desacordo com os dados referentes à primeira pergunta do questionário. Então, porque você se preocupa com seus dispositivos removíveis se você não sabe como estes malwares se propagam e quais seus objetivos? Isso realça, ainda mais, à importância de cumprir nossa meta, alertar sobre a maneira de como os *malwares* estão se espalhando.

Conclusões

A partir do exposto é considerável dizer que os principais cuidados a serem tomados para proteger seu computador dos códigos maliciosos são ações simples realizados pelos próprios usuários, como: fazer *backups* periodicamente; nunca recuperar um *backup* ao perceber que ele contém dados não confiáveis; conectar os dispositivos somente em computadores seguros; e não conectar ao seu sistema dispositivos suspeitos.

Contudo, este trabalho contribuiu para o conhecimento dos indivíduos da entidade educacional IFPA Campus Breves, sobre códigos que podem se instalar em memórias específicas para estruturas padrões de dispositivos removíveis, causando danos. Além, de proporcionar, um conhecimento a mais sobre os estudos já realizados em nossa vida acadêmica.