Internet of Toys: Despertar a Criatividade ou o Pesadelo de Segurança da Informação?

Christiane Borges Santos
Instituto Federal de Goiás – Campus Luziânia
Luziânia, Brasil
christiane.santos@ifg.edu.br

https://orcid.org/0000-0003-2003-135X

***Abstract*—Privacy and information security are always major challenges. Recently, the biggest cyber attacks have been triggered through vulnerabilities found in electro-electronic devices, and a potential target is connected toys. Dolls, teddy bears, baby monitors and strollers increasingly smart and connected to the Internet. What seemed like an innocent game can become a major headache for parents and guardians. And this is even more worrying now, in times of pandemic, when many are working in the home office format. This article aims to present Internet of Toys concepts, security and privacy requirements.**

***Resumo*— A privacidade e a segurança da informação são sempre grandes desafios. Recentemente, os maiores ataques cibernéticos foram disparados através de vulnerabilidades encontradas em dispositivos eletro-eletrônicos, e um alvo em potencial são os brinquedos conectados. Bonecas, ursos de pelúcia, babás eletrônicas e carrinhos cada vez mais inteligentes e conectados à Internet. O que parecia uma brincadeira inocente pode se tornar uma grande dor de cabeça para pais e responsáveis. E isso é algo ainda mais preocupante agora, em tempos de pandemia, em que muitos estão trabalhando no formato *homeoffice*. Este artigo tem como objetivo apresentar conceitos da *Internet of Toys* (IoToys), requisitos de segurança e privacidade, além de mostrar um breve estudo de caso sobre vulnerabilidades.**

***Palavras-chave — Internet of Toys*; Brinquedos Conectados; Brinquedos Inteligentes; Privacidade; Vulnerabilidade**

I. Introdução

Os brinquedos ajudam no desenvolvimento de habilidades e imaginação das crianças. Constroem autonomia, exploram, ensinam e reproduzem comportamentos. Brinquedos que gravam sons, imagens e interagem com uma criança não são novos.

Nos últimos anos, as empresas têm investido em brinquedos para que eles se tornem mais atrativos. Um exemplo disso são os *Smart Toys* (brinquedos inteligentes) e os *Connected Toys* (brinquedos conectados), visto que crianças e adolescentes estão cada vez mais envolvidos com as tecnologias e conectados a Internet.

Smart Toys são brinquedos que possuem componentes tecnológicos (câmera, microfone, acelerômetros, giroscópio, sensores, entre outros) e podem capturar como seus usuários interagem com eles, mas sem acesso a Internet. Os *Smart Toys* são os predecessores da *Internet of Toys* (IoToys)[1].

Connected Toys são brinquedos conectados à Internet, e como qualquer outro dispositivo conectado, podem interagir uns com os outros, capturar e registrar informações pessoais dos usuários para alimentar a inteligência do brinquedo. O objetivo da conexão com a Internet é o compartilhamento dos dados para análise, interação e personalização. Alguns brinquedos podem coletar informações das brincadeiras e reter na memória, para traçar a evolução e desempenho das crianças. Estes brinquedos são caracterizados como *Internet of Toys* [1].

Na *Internet of Toys*, uma variedade de brinquedos são capazes de interagir com crianças de forma inteligente, não apenas por meio de repetição simples de palavras, frases ou músicas em uma gravação, e sim de forma interativa. Por exemplo, utilizando tecnologias de sensores, câmeras, inteligência artificial e conectividade, é possível que estes brinquedos respondam ao que é falado pela criança, reproduzindo uma resposta individualizada e personalizada.

Com a crescente onda de dispositivos conectados, surgem preocupações relacionadas aos potenciais impactos e riscos dessas novas tecnologias, aspectos de privacidade e segurança, sobretudo em relação aos dados pessoais dos usuários que estão sendo coletados. E essa preocupação é maior ainda quando crianças e adolescentes são os usuários [2][3][4].

Este artigo está definido da seguinte forma: a introdução discutiu o contexto e os conceitos básicos sobre *Smart Toys* e *Connected Toys*. A seção II apresentará os conceitos de *Internet of Toys* e requisitos para segurança dos dados. A seção III abordará problemas de privacidade e segurança na *Internet of Toys*, com alguns exemplos de vulnerabilidades reportadas, a seção IV trará um estudo de caso e a seção V trará as conclusões.

II. Internet of Toys e Requisitos de Segurança

Smart e *Connect Toys* normalmente são bem populares e aceitos por pais e responsáveis, pois são brinquedos que oferecem às crianças novas maneiras de brincar e aprender.

A *Internet of Toys* refere-se a uma tipologia bastante diversa de brinquedos, incluindo [1]:

- brinquedos baseados em reconhecimento de voz e/ou imagem;
- aplicativos habilitados para robôs, drones e outros brinquedos mecânicos;
- brinquedos para a vida (*toys-to-life*), que conectam bonecos de ação a videogames;
- jogos de quebra-cabeça e construção.

A maioria desses brinquedos se conectam sem fio a bancos de dados *online* para reconhecer vozes e imagens, identificando comandos, perguntas e solicitações das crianças. Essas interações são analisadas e geram uma resposta do dispositivo. Esses brinquedos são desenvolvidos com a finalidade de melhorar a qualidade das brincadeiras das crianças, proporcionando que elas criem novas experiências de brincadeiras colaborativas, desenvolvam alfabetização, aprendam uma nova linguagem, habilidades numéricas e sociais por exemplo.

No entanto, esses brinquedos também levantam preocupações sobre as potenciais ameaças à proteção de dados das crianças, que podem ser rastreados, registrados e analisados.

Em 2017, a Mozilla Foundation criou um guia sobre privacidade e segurança de brinquedos, aparelhos e produtos domésticos inteligentes conectados chamado *Privacidade não incluída, com o objetivo de auxiliar consumidores, pais e responsáveis antes de comprar um determinado produto. São considerados padrões mínimos de segurança que um brinquedo ou dispositivo conectado deve ter [5]:

- **Atualizações de Segurança:** é um tipo de atualização que normalmente corrige problemas relacionados à segurança de hardware e software. Dispositivos conectados à Internet devem oferecer suporte a atualizações por um período de tempo e de preferência, já vir ativado por padrão.
- **Criptografia:** é um recurso utilizado para enviar e receber dados de forma secreta, segura e rastreável. Dispositivos conectados a Internet devem criptografar a comunicação para que não sejam interceptadas ou modificadas em trânsito, e garantir que os dados também sejam protegidos enquanto estiverem armazenados.
- **Gerenciamento de Vulnerabilidades:** o fabricante deve possuir um sistema implementado para gerenciar vulnerabilidade nos dispositivos e mecanismos de contato para reportar erros.
- **Privacidade:** os dispositivos desenvolvidos devem conter informações de privacidade que se apliquem especificamente a eles.
- **Senhas Fortes:** senhas padrão devem ser redefinidas como parte inicial das configurações, principalmente se o dispositivo necessita de login para autenticação remota. Muitos ataques a dispositivos de Internet das Coisas (IoT – *Internet of Things*) exploraram senhas fracas ou padrão. Uma boa senha deve conter letras (maiúsculas e minúsculas), números e caracteres especiais. Deve ser fácil do usuário lembrar, difícil de um atacante quebrar.

Para esta análise, também são considerados se um dispositivo compartilha ou vende dados dos usuários, permite a exclusão de dados dos usuários ou se a empresa tem um histórico ruim de proteção dos dados de seus usuários.

Um um relatório técnico do Joint Research Centre (JRC) sistematizou os discursos públicos e percepções mais comuns de novembro de 2015 a dezembro de 2016, sobre os riscos e benefícios da *Internet of Toys*, como mostra a tabela 1 [6]:

TABELA I
DISCURSOS PÚBLICOS MAIS COMUNS SOBRE OS RISCOS E BENEFÍCIOS DA INTERNET OF TOYS [6]

Riscos da IoToys	**Benefícios da IoToys**
Segurança de dados Segurança do dispositivo Geolocalização para rastreamento de crianças Privacidade das crianças (coleta de dados e compartilhamento) Uso excessivo e equilíbrio na vida (sono, atividade física, socialização) Falta de jogos reais autênticos (importante para o desenvolvimento) Falta de interação pais e filhos (importante para o desenvolvimento) Jogos muito controlados ou artificiais, conduzidos por scripts e algoritmos Radiação eletromagnética (EMR)	Educacional (envolvente e individualizado para criança) Encoraja brincadeiras e interação com brinquedos de tempo de tela passivo Divertido, emocionante Pode ensinar programação/codificação Suporta jogos mais ativos Incentiva brincadeiras sociais Promove brincadeiras colaborativas com outras crianças Possibilidades de diagnóstico (identificar dificuldades de aprendizagem ou problemas médicos) Seguro e protegido (privacidade na Internet e segurança) Pode ser atualizado continuamente com novos conteúdos

De acordo com a tabela 1, é possivel perceber que existe uma preocupação pública com os riscos desses brinquedos conectados, mas muitos também acreditam que as informações geradas estão seguras e protegidas. Muitas pessoas não percebem os riscos reais da *Internet of Toys* e até consideram benefícios brincadeiras colaborativas com

outras crianças, desconsiderando que existem casos em que não é possível validar se o outro usuário que está interagindo com a criança realmente é outra criança. A atualização contínua de conteúdos também não é garantia que os dispositivos estão sendo atualizados para minimizar riscos e vulnerabilidades.

III. PRIVACIDADE E SEGURANÇA NA INTERNET OF TOYS

Tudo que está conectado à Internet está vulnerável. Dispositivos como celulares, computadores e tablets, que também são dispositivos que se conectam a Internet, normalmente têm-se tem uma preocupação maior quanto a utilização de senhas fortes e atualizações regulares de software por exemplo. Mas quanto se trata de brinquedos, essa preocupação não é uma rotina. Esses brinquedos possuem um alto custo e quem o comprou quer utilizar todos os recursos disponíveis, logo tem que estar ciente dos riscos envolvidos. Para isso, os fabricantes devem apresentar quais são os possíveis riscos aos usuários e garantir a ciência e o consentimento dos mesmos. Uma forma de conscientização por parte dos fabricantes por exemplo, seria alertar o usuário quanto ao uso de senhas fortes, atualização do produto e quais as informações realmente necessárias para a utilização do dispositivo.

Como os usuários desses brinquedos são em sua maioria crianças, estas estão em posição maior de vulnerabilidade em relação a um consumidor-padrão, pois ainda estão em fase de aprendizado e não têm a percepção dos riscos de compartilhar dados sensíveis, o que os tornam mais susceptíveis aos apelos dos fabricantes.

Em 2013, a *Federal Trade Commission*, agência de defesa do consumidor dos Estados Unidos, promoveu uma atualização da lei americana de proteção de dados das crianças na Internet, conhecida como COPPA (*Children's Online Privacy Protection Act*) para regular a coleta de dados de crianças menores de 13 anos, exigindo o consentimento verificável dos pais.

As alterações visam maior transparência, segurança e o consentimento na coleta e tratamento dos dados, evitando que esses fossem repassados a terceiros. Além disso, alerta os pais diretamente a respeito da obtenção dessas informações, permitindo que eles solicitem a exclusão desses dados a qualquer momento [4].

São considerados dados pessoais protegidos pela COPPA: nome completo da criança e dos responsáveis por ela, endereços eletrônicos como email, IP (*Internet Protocol*) e *cookies*, nomes de usuário, localização, arquivos de áudio e vídeo que contenham a imagem ou voz da criança, e outras informações coletadas que possam ser combinadas para gerar a identificação do usuário [4].

No Brasil, em 2018 foi aprovada a LGPD (Lei Geral de Proteção de Dados Pessoais), Lei nº 13.709, de 14 de agosto de 2018, que passou a ter vigência em agosto de 2020. A LGPD estabelece regras para o uso, coleta, armazenamento e compartilhamento de dados dos usuários por empresas públicas e privadas. O principal objetivo é garantir mais segurança, privacidade e transparência no uso de informações pessoais. Com a nova legislação, o usuário terá o direito de consultar gratuitamente quais dos seus dados as empresas têm, como armazenam e até pedir a retirada deles do sistema. Além disso, a LGPD define que dados sobre crianças e adolescentes precisam seguir o princípio do melhor interesse (Artigo 14 da Seção III - Do Tratamento de Dados Pessoais de Crianças e de Adolescentes) e devem ter seus direitos e necessidades tratados com a máxima prioridade pelo Estado, pela sociedade e pela família, pois são consideradas pessoas em desenvolvimento [7][8].

Segundo a LGPD, para o tratamento de dados pessoais de crianças e adolescentes, é preciso o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal. A exceção fica quando a coleta for necessária para a sua proteção, para contatar os pais ou o responsável legal. Esses dados são utilizados uma única vez, não são armazenados e em nenhum caso poderão ser repassados a terceiro sem o consentimento específico [7].

Para se adequarem as Leis de Proteção de Dados vigentes em diversos países, alguns fabricantes já adotam a *privacy by default*, por exemplo deixando por padrão a geolocalização dos dispositivos desligada. Ao habilitar o GPS, o site ou aplicativo obrigatoriamente avisa o usuário dos riscos, em uma linguagem clara e acessível. E brinquedos que se conectam a Internet para transmitir para algum servidor, alertam no exato momento de uso os dados que estão sendo coletados.

Muitas empresas fabricantes de brinquedos – quando implementam senha – as vezes adicionam um código de acesso, normalmente uma sequencia numérica simples, mas não deixam claro que os usuários deverão alterar este código imediatamente após a ativação. Também não mostram a importância de se manter o brinquedo atualizado para vulnerabilidades de segurança.

Existe ainda riscos de que os brinquedos conectados através de tecnologias sem fio possam se transformar em um espião da criança, enviando dados sem o consentimento e até mesmo conhecimento dos pais. Ou mesmo que estranhos no mesmo raio de cobertura dos dispositivos se conectem a eles e conversem com as crianças. Além disso, alguns brinquedos ainda têm GPS (*Global Positioning System*), que também podem revelar a localização dos usuários, mesmo que sejam crianças.

Infelizmente, é comum na *Internet of Toys* que os usuários aceitem termos e condições de uso e acesso com abordagem abusiva, de forma não transparente para que o brinquedo fique ativo. Muitas empresas também compartilham os dados pessoais coletados com terceiros, que são usados para marketing direcionado. Alguns brinquedos até incentivam que as crianças divulguem informações pessoais para uma maior personalização. Sem contar as propagandas ocultas e subliminares. Um dos grandes problemas com a coleta dos dados pessoais dos usuários é em relação a falta de transparência que trata da coleta, tratamento e armazenamento destas informações. O usuário não tem noção de quem tem acesso e o quão seguro estas informações estão [9].

Muitas vezes, a interação do brinquedo com a criança é baseada em algoritmos e tecnologias de inteligência artificial, que precisam ser transparentes, assim como o desenvolvimento tecnológico deve estar de acordo com os preceitos legais de proteção a crianças e adolescentes, considerando sua vulnerabilidade e condição peculiar de pessoa em desenvolvimento. E o monitoramento dos pais por meio desses brinquedos também deve ser pensado, para que

não constitua uma verdadeira invasão à privacidade das crianças [2][3].

Em 2015, a Mattel em parceria com a empresa US Toy Talk lançou a Hello Barbie (Figura 1), anunciada como a primeira "boneca interativa" do mundo, capaz de ouvir a criança e respondê-la por voz. Ela se conectava a Internet utilizando tecnologia Wi-Fi (Wireless Fidelity) e as conversas gravadas poderiam ser ouvidas posteriormente pelos pais. Para interpretar e responder as perguntas das crianças, o conteúdo era enviado para a Toy Talk, que processava as informações antes de responder com respostas em linguagem natural [10].

Foi verificado que, quando conectada ao Wi-Fi, a boneca ficava vulnerável a atacantes, permitindo-lhes acesso fácil às informações do sistema da boneca, informações da conta, arquivos de áudio armazenados e acesso direto ao microfone. A partir dessas informações, também podia ser possível assumir a rede Wi-Fi onde a boneca estava conectada e, a partir daí, obter acesso a outros dispositivos conectados à Internet e informações pessoais, potencialmente sem conhecimento dos envolvidos.

Fig. 1. Boneca Hello Barbie [10]

Em 2017 a Agencia de Telecomunicações da Alemanha, alertou sobre possíveis falhas de privacidade na boneca falante Cayla (Figura 2), fabricada pela empresa Genesis Toys e ordenou aos pais que destruíssem ou desabilitassem esta "boneca inteligente" porque o brinquedo poderia ser utilizado para espionar crianças ilegalmente. Foram apontados problemas de segurança, como o fato de uma pessoa que esteja utilizando a mesma rede poder se conectar ao brinquedo e falar com a criança por meio dele. Atacantes poderiam utilizar esse recurso como forma de ter fácil acesso à criança ou ao adolescente, sem a intermediação ou vigilância dos pais [11].

Fig. 2. Boneca My Friend Cayla [11]

Um dos droids mais famosos do universo Star Wars, o BB-8 desenvolvido pela Orbotix também requer atenção dos usuários. Para emparelhar o Sphero BB-8 (Figura 3) com um dispositivo, existe um aplicativo que conecta utilizando tecnologia *Bluetooth* mas não requer um PIN (Personal Identification Number). Isso significa que qualquer pessoa no raio de alcance pode instalar e executar o aplicativo do brinquedo e sequestrá-lo. Mas o maior problema são as atualizações de firmware do dispositivo. A atualização é feita através de uma conexão HTTP (HyperText Transfer Protocol) ao invés de uma conexão segura HTTPS (Hyper Text Transfer Protocol Secure). Como não há autenticação SSL, um atacante pode sequestrar a conexão e instalar seu próprio firmware. Este software pode então reportar de volta as informações do BB-8 ao atacante ou alterar os controles. Mas o Sphero BB-8 não transmite nenhuma informação útil [12].

Fig. 3. Sphero BB-8 [12]

Robôs de codificação para crianças são legais mas deve-se verificar as permissões dadas ao aplicativo utilizado para controlar esses robôs, que pode solicitar acesso a câmera, microfone e localização. Os kits de robótica Jimu da Ubtech (Figura 4) é um produto que pode potencialmente coletar muitos dados sobre as crianças mas não deixa claro como usam, protegem ou não protegem esses dados coletados a partir das permissões dadas. A política de privacidade para este produto se aplica apenas ao site, não ao dispositivo ou aplicativo Jimu [5].

Fig. 4. Kits de Robótica Jimu da Ubtech – Meebot 2.0 [5]

Pulseiras inteligentes como a Fitbit Ace 2 (Figura 5) surgem como incentivo para que crianças façam exercícios físicos. Pais e responsáveis podem rastrear as atividades das crianças (inclusive o sono), aprovar conexões com amigos, estabelecer metas e recompensas por atividades e estimular a competição entre outras crianças. Uma questão a ser levantada é sobre o nível de vigilância digital na vida da criança. Outro ponto é que o Google, uma empresa que gosta

de ter o máximo possível de dados sobre pessoas, está em processo de compra do Fitbit [5].

Fig. 5. Fitbit Ace 2 [5]

Uma das grandes dificuldades para minimizar os riscos e vulnerabilidades na *Internet of Toys* é que a maioria dos dispositivos possuem arquitetura proprietária, tanto de hardware quanto de software.

No final de 2019, a empresa chinesa Elephant Robotics criou o MarsCat (Figura 6), o primeiro gato de estimação biônico do mundo, com o objetivo de ser um robô doméstico e um animal de estimação robótico. O MarsCat imita o comportamento autônomo de gatos reais através da inteligência artificial e cada dispositivo é único, do corpo à personalidade. Sua personalidade mudará de acordo com as interações do usuário.

O projeto utiliza Raspberry Pi e pode ser programado a partir de um SDK (*Software Development Kit*) de código aberto, que facilitará a alteração do código e acesso a APIs (*Application Programming Interface*) para controlar câmera, microfone, sensores e servos, conectados ao microcontrolador ATMega2560. Além de ser possível a programação visual através do Scratch [13].

Fig. 6. MarsCat: um gato biônico, um robô doméstico *open source* [13]

O Arduino, plataforma de prototipagem eletrônica de hardware livre, é uma boa alternativa para a criação de brinquedos inteligentes e conectados, através da utilizaçao de sensores de *shields*. Além disso, existem vários kits Arduino no mercado de baixo custo, e que permite um controle total do projeto.

Um exemplo de kit é o Otto (Figura 7), um robô humanóide bípede do tipo DIY (*do-it-yourself*) com Arduino. A proposta é que os usuários aprendam a conexão lógica entre componentes mecânicos, design, eletrônica e código. Ele utiliza peças impressas em impressora 3D, sensores, Arduino e pode ser programado em multiplas linguagens, inclusive linguagem em blocos como o Scratch [14].

Fig. 7. Robo Otto [14]

IV. Estudo de Caso

A *Internet of Toys* é uma realidade e está cada vez mais Então, formar o criticismo com relação a segurança de dados se torna cada vez mais necessário.

Foi feita uma análise de riscos de dois brinquedos adquiridos: o drone DJI Tello e o carro Buggy Wi-Fi da BeeWi. Além disso, foram feitas pesquisas na ferramenta Shodan [15] para mostrar o risco de se utilizar dispositivos de imagem e vídeo em configurações padrão.

O drone DJI Tello (Figura 8) fabricado pela Ryze Tech, combina o processador Intel com tecnologia de voo com recursos de inteligência artificial desenvolvida pela DJI. Um dos grandes diferenciais é que ele é compatível com o Scratch, desenvolvido pelo MIT (*Massachusetts Institute of Technology*), permitindo que usuários (incluindo crianças) possam programar padrões de voos e sequências de manobras.

O drone não tem memória interna e não suporta a cartão de memória, todas as fotos e os vídeos são transmitidos ao vivo em HD e gravados no smartphone. Por padrão, o drone cria uma rede Wi-Fi sem senha e, mesmo que tenha sido definida uma senha, é possível resetar para configuração padrão apenas apertando o botão de ligar por 5 segundos. Ele é passivel à ataques de desautenticação, com isso um atacante no raio de alcance poderia derrubar a conexão original e controlar o drone.

Existe uma comunidade ativa em torno de "hackear" os protocolos de vídeo usados pelo Tello. Uma ferramenta de código aberto utilizada para analise de protocolos e informações da rede é o Wireshark. É possível conectar na rede e coletar as informações trocadas entre o drone e o dispositivo que está sendo utilizado para controlar o drone. Por exemplo, um atacante pode facilmente visualizar *streaming* de vídeo sendo enviado do drone para o dispositivo de controle [16].

A preocupação sobre a exploração de dados pelo governo chinês é grande, pois a DJI tem sede na China. Em 2017, as Forças Armadas dos EUA (Estados Unidos da América) até mesmo proibiram o uso de drones dessa empresa para fins militares [5].

Além disso, atualmente existe um *framework exploit* chamado DroneSploit, que é dedicado ao *hacking* de drones, principalmente drones comerciais conectados em redes Wi-Fi.

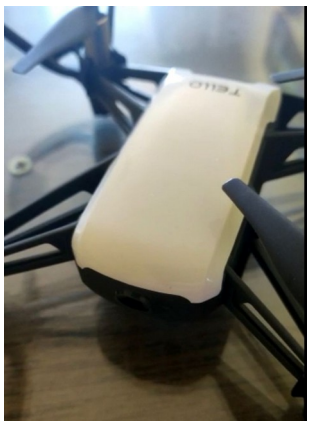

Fig. 8. Drone DJI Tello [Arquivo Pessoal]

O Carro Buggy Wi-Fi da BeeWi (Figura 9) utiliza a tecnologia Wi-Fi IEEE 802.11b/g para se conectar aos dispositivos. A bateria dura até 20 minuto e possui câmera VGA que permite gravar vídeos e tirar fotos.

Ao ligar o brinquedo, ele cria um ponto de acesso e os dispositivos conectam nele através de uma rede com SSID (Service Set Identifier) *BeeWi BWZ200 1322*, que são as informações do modelo do brinquedo e os 4 últimos dígitos representam o endereço MAC (Media Access Control) dele.

Quando selecionada a rede, ele se conecta automaticamente, sem nenhuma senha. Qualquer pessoa em seu raio de alcance (30 metros) pode instalar e executar o aplicativo do brinquedo e sequestrá-lo. Ele cria um servidor WEB HTTP onde é possível acessar e visualizar as imagens capturadas. Atualmente, não possui aplicativo para dispositivos iOS e o aplicativo para Android está desatualizado.

Fig. 9. Carro Buggy Wi-Fi da BeeWi [Arquivo Pessoal]

Uma ferramenta que apesar de assustadora não é ilegal é o Shodan, um mecanismo de busca projetado especificamente para dispositivos IoT. O serviço coleta apenas dados que já estavam disponíveis para o público, e exibe metadados de vários dispositivos IoT conectados e transmitindo dados online, como por exemplo: servidores, impressoras, webcams, sinais de trânsito, câmeras de segurança, geladeiras, televisores e até mesmo brinquedos [15].

Por exemplo, utilizando o seguinte filtro:

port:554 has_screenshot:true country:"BR"

é possível visualisar câmeras instaladas em lugares que vão desde estacionamentos a ruas, estoques de lojas e até mesmo interior de residências, incluindo quartos de crianças, que estão utilizando o protocolo *Real Time Streaming Protocol* (RTSP) na porta 554 do protocolo TCP (*Transmission Control Protocol*). A Figura 10 mostra a quantidade de dispositivos conectados no Brasil no dia 03 de dezembro de 2020.

Fig. 10. Resultados de busca de câmeras no Shodan

Um dado preocupante é que entre os dispositivos encontrados foi possível encontrar produtos da marca Hipcam (que inclusive fabrica babás eletrônicas e possui geolocalização) e dispositivos de monitoramento H.264 DVR (*Digital Video Recorder*). E parte destes dispositivos apontavam para ambientes internos.

V. CONCLUSÃO

É inegável que os brinquedos conectados são uma realidade, mas também uma preocupação, que depende de diversos fatores.

Antes de comprar qualquer tipo de brinquedos conectados à Internet, os pais devem pesquisar cuidadosamente e avaliar estes dispositivos, como funcionam, se implementam ou não configurações de segurança e privacidade antes de levá-los para suas casas, para não colocar as crianças em risco. Deve-se considerar se existe uma política de atualização de software e firmware e como é o histórico de tratamento de vulnerabilidades. Outro ponto importante é assumir que dispositivos conectados podem ser vulneráveis, logo desabilitar serviços desnecessários, alterar senhas padrão e mantê-los sempre atualizados.

Dispositivos *open source* podem oferecer um nível de segurança melhor pois muitas vezes possuem uma comunidade colaborativa, as falhas são reportadas e corrigidas mais facilmente e existem ferramentas e sistemas operacionais Linux que são voltados para a privacidade dos dados. É possível um maior controle da concepção a criação dos dispositivos.

Se o brinquedo envia dados para um servidor remoto, se o usuário não é capaz de controlar as ações do brinquedo, se o brinquedo possui sensores, câmeras, microfone, acelerômetros, giroscópio, possui configurações simples demais e pede informações pessoais, deve-se desconfiar.

Para os desenvolvedores, a segurança deve ser nativa e não opcional, considerando todos os elementos do protótipo como hardware, firmware, sistema operacional, aplicativos, armazenamento dos dados. Deve-se procurar utilizar criptografia e autenticação forte e não utilizar protocolos que já estão em desuso ou obsoletos.

Fabricantes devem considerar requisitos de segurança desde o início do projeto, levando em consideração a análise de riscos e respostas a incidentes. A LGPD por exemplo prevê no Artigo 46 que devem-se adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Sem contar que os dados pessoais de crianças e adolescentes devem ser tratados em seu melhor interesse.

AGRADECIMENTOS

Agradecimentos a toda a organização da Latinoware e Latin.Science e ao Instituto Federal de Goiás, em especial ao Laboratório Metabotix.

REFERÊNCIAS

[1] Donell Holloway & Lelia Green (2016). *The Internet of toys, Communication Research and Practice*, 2:4, 506-519, DOI: 10.1080/22041451.2016.1266124

[2] CARVALHO, Diógenes Faria de; OLIVEIRA, Thaynara de Souza. *A categoria jurídica de 'consumidor-criança' e sua hipervulnerabilidade no mercado de consumo brasileiro.* Revista Luso-Brasileira de Direito do Consumo, vol. V, n. 17, mar. 2015, p. 224

[3] LEAL, Livia Teixeira. *Internet of toys: os brinquedos conectados à internet e o direito da criança e do adolescente*. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, vol. 12, p. 175-187, abr./jun. 2017.

[4] COPPA – *Children's Online Privacy Protection Act*. Disponível em: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule Acessado em Novembro, 2020.

[5] *Privacidade não incluída*. Disponível em: https://foundation.mozilla.org/pt/privacynotincluded/ Acessado em: Novembro, 2020

[6] JRC Technical Reports. *Kaleidoscope on the Internet of Toys - Safety, security, privacy and societal insights*. Disponível em: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf Acessado em: Novembro, 2020

[7] *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Lei nº 13.709, de Agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm Acessado em: Novembro, 2020

[8] BORELLI, Alessandra. *É PRA JÁ! A proteção de dados de crianças e adolescentes não pode esperar.* Opice Blum Academy. Publicado em Julho de 2020.

[9] *The Internet of Toys: stimulating creativity or a security nightmare?* Disponível em: https://www.kemplittle.com/blog/the-internet-of-toys-a-leap-forward-in-stimulating-childrens-creativity-or-a-privacy-and-security-nightmare/ Acessado em: Novembro, 2020.

[10] *Hackers can hijack Wi-Fi Hello Barbie to spy on your children*. Disponível em: https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children Acessado em: Novembro, 2020

[11] *German parents told to destroy doll that can spy on children*. Disponível em: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children Acessado em: Novembro, 2020

[12] *Hack Turns BB-8 Star Wars Toy to Dark Side*. Disponível em: https://www.tomsguide.com/us/bb8-toy-hack,news-22115.html Acessado em: Novembro, 2020

[13] *MarsCat: A Bionic Cat, a Home Robot.* Disponível em: https://www.kickstarter.com/projects/1655380003/marscat-a-bionic-cat-a-home-robot Acessado em: Novembro, 2020

[14] *Build your own robot.* Disponível em: https://www.ottodiy.com/ Acessado em: Novembro, 2020

[16] Shodan. Disponível em: https://www.shodan.io/. Acessado em Novembro, 2020.

[13] H*ello, Tello - Hacking Drones With Go.* Disponível em: https://www.hackster.io/deadprogram/hello-tello-hacking-drones-with-go-5a6a50 Acessado em: Novembro, 2020