Novembro de 2014

Estudo trimestral X-Force de inteligência contra ameaças 4º trimestre de 2014

Conheça mais profundamente os atuais riscos de segurança — de novas ameaças, que surgem com a Internet das Coisas, a fontes de infecções por malwares e botnets.

IBM

Índice

Visão geral executiva

Conforme o fim do ano se aproxima, a equipe de pesquisa e desenvolvimento do IBM® X-Force® observa de maneira mais aprofundada as tendências de segurança que modelam nosso mundo. Especificamente, este relatório examina como a Internet continua a conectar mais pessoas, lugares e coisas, resultando em uma nova gama de riscos de segurança.

Primeiro, voltemos nossa atenção à segurança na Internet das Coisas. A conectividade onipresente das "coisas" que enriquecem nossa vida, de termostatos a automóveis e dispositivos médicos, significa que o desenvolvimento de software está acontecendo ao mesmo tempo que a tecnologia de ponta desenvolvida pelos fabricantes de hardware. O segmento de mercado de segurança pode ajudar a orientar o desenvolvimento de práticas de segurança do software integrado praticamente desde sua concepção. Isso não apenas criaria uma nova era de programas de software seguros, como também impediria que um mundo de possíveis ameaças afetasse a Internet das Coisas.

Em um relatório de novembro de 2014, analistas estimaram que a Internet das Coisas representará 30 bilhões de "coisas" conectadas até 2020, partindo de 9,9 bilhões, em 2013. Essas "coisas" conectadas são, em grande parte, orientadas por sistemas inteligentes, todos coletando e transmitindo dados. Essa conectividade está mudando a maneira como vivemos e criando novas questões sobre privacidade pessoal, marketing e segurança na Internet à medida que as "coisas" são fabricadas e vendidas aos clientes.

Agentes maliciosos que pretendem assumir o controle de dados, identidades e senhas investigam e fazem uso de dispositivos conectados à Internet que não são desenvolvidos com segurança, fazendo deles alvos mais fáceis que PCs,

notebooks ou tablets. É vital agora, mais do que nunca, que as organizações e os funcionários que utilizam essa tecnologia emergente considerem os riscos de se conectarem à zona de segurança da empresa. Discutiremos posteriormente, neste relatório, os riscos e as proteções individuais disponíveis para auxiliar nessas áreas importantes.

Em seguida, focaremos os lugares. Mais especificamente, aqueles lugares da Internet que não são seguros. Utilizando nosso banco de dados de mais de 23 bilhões de URLs e endereços IP, observaremos quais são os países propensos à mais alta proporção de infecções por malwares e botnets e como esse cenário mudou nos últimos 14 meses.

Como em todas as edições do estudo trimestral IBM X-Force de inteligência contra ameaças, as pessoas são o aspecto mais importante. Enquanto analistas de segurança, esperamos que os *insights* sobre a proteção de coisas e lugares possam ser úteis para protegermos nossas próprias redes. Voltaremos em 2015 com uma revisão anual das tendências de segurança em 2014 e o que esperar para o próximo ano.

Protegendo o novo mundo da Internet das Coisas

De carros conectados a marca-passos programáveis, como podemos manter os dados sensíveis protegidos e seguros em um mundo de conectividade onipresente?

Seu próximo dispositivo móvel pode ser móvel de verdade: com rodas e um painel. Se tiver um marca-passo ou uma bomba de insulina modernos, além de você estar usando um dispositivo conectado à Internet, também estará o hospedando. A mais nova tendência é conectar qualquer coisa com poder de computação à Internet, incluindo veículos, dispositivos médicos implantáveis e medidores inteligentes de serviços públicos. Até mesmo objetos que tradicionalmente não eram computadorizados, como eletrodomésticos, escovas de dente, e xícaras estão sendo instrumentalizados e conectados.

Essa onda de instrumentação e conectividade se tornou conhecida como a Internet das Coisas (IoT). Assim como ocorre com outras categorias amplas de tecnologia, como a nuvem ou os dispositivos móveis, a IoT pode oferecer melhorias em termos de produtividade e qualidade de vida, mas também pode trazer consigo, durante sua ascensão, uma série de ameaças de segurança desconhecidas.
Durante os últimos anos, essa conectividade onipresente foi apresentada em conferências sobre segurança, como a Black Hat e a DEF CON. Em 2011, um pesquisador da área de segurança descobriu como hackear sua própria bomba de insulina apenas com o número de série.[5] Mais recentemente, dois pesquisadores apresentaram suas descobertas sobre a segurança de veículos conectados, inclusive uma demonstração transmitida em um *talk show* matutino nos EUA sobre como assumir o controle de dois modelos de carro.[6]

Como ocorre com a maioria dos monikers de conceitos tecnológicos emergentes, o termo "Internet das Coisas" é consideravelmente ambíguo. Então, o que compõe a IoT? Muitos de nós pensamos em recursos como automação de residências, como o Google Nest, uma rede de termostatos e detectores de fumaça conectados. Carros conectados também fazem parte da IoT. Mas, e quanto aos smartphones e tablets que oferecem acesso a essas "coisas"? Esses dispositivos também são "coisas"?

E quanto aos dispositivos de informática tradicionais, como mainframes, servidores, estações de trabalho e laptops? São "coisas" completamente desenvolvidas ou apenas computadores antigos? Eles não são tão novos assim e não parece certo relacioná-los a um termo de última geração, como IoT. Há também os sistemas de controle industrial e de Supervisory Control and Data Acquisition (SCADA). Alguns são tão antigos (muitos estão no subsolo das fábricas, enterrados desde a década de 50) que não possuem uma conectividade de IP inerente, mas estão conectados à Internet por meio de gateways de IP.

Claramente, "IoT" é um termo genérico que não tem praticamente significado nenhum para os profissionais de segurança: os dispositivos que compõem a IoT como um todo têm funções diferentes, expõem superfícies de ameaça bastante variadas e requerem estratégias de segurança específicas a cada categoria de dispositivo. Na IBM, criamos um modelo da IoT que é útil para entender as ameaças de segurança em vários pontos de fluxo de dados e transição de controle. Esse modelo foi generalizado para acomodar todas as categorias de "coisas", mas nem todas as "coisas" demandam todos os componentes do modelo.

Todas as "coisas" se conectam a uma rede local e, depois, a uma rede global que é geralmente a Internet. Isso se aplica aos computadores tradicionais e aos dispositivos de infraestrutura. Mainframes, servidores, desktops, laptops, roteadores e comutadores: todos se conectam a redes locais (embora os dispositivos do provedor de serviços possam estar conectados diretamente à Internet) e todas as redes, com exceção das redes governamentais sigilosas, são roteadas para a Internet. Os sistemas de controle industrial podem estar isolados.

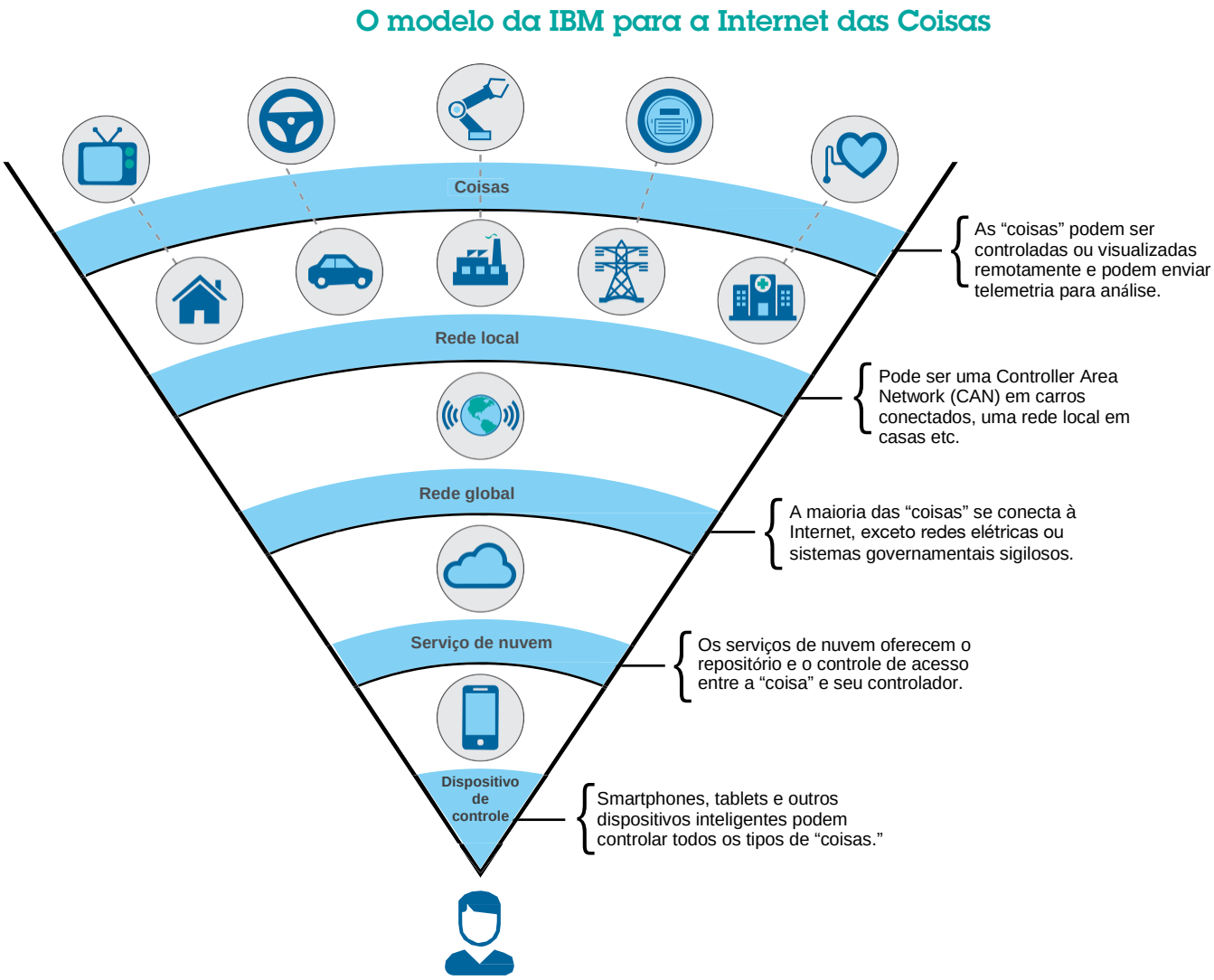

Gráfico 1. O modelo da IBM para a Internet das Coisas

Possivelmente, a característica que define uma “coisa” é a capacidade de visualizá-la e controlá-la remotamente, geralmente a partir de um dispositivo móvel inteligente. As “coisas” também podem enviar telemetria a um ponto de coleta e analítica central. Um serviço de nuvem geralmente oferece o repositório e o controle de acesso entre a “coisa” e seu controlador.

Vamos analisar algumas “coisas” e ver como elas se encaixam nesse modelo.

Automação de casas

Essa categoria pode incluir eletrodomésticos inteligentes, como refrigeradores que informam a temperatura ou a falta de brócolis, sistemas sonoros e de iluminação, televisões, termostatos e detectores de fumaça, sistemas de alarme, portas de garagem e até mesmo trancas de porta. Essas "coisas" se conectam à rede local da casa, que normalmente é sem fio, e a rede local geralmente se conecta à Internet por meio de um provedor de serviço, geralmente com cabos de fibra que chegam à residência ou com cabos de conexão banda larga. Os sistemas de segurança também podem ter uma conexão secundária, usando uma rede móvel. Provedores de serviço ou serviços públicos podem oferecer serviços de automação de lares, por exemplo, os serviços Digital Life da AT&T ou EnerLink.Net da Consumers Energy.[7] Como alternativa, entusiastas que fazem isso como hobby podem construir sua própria solução de automação doméstica e ignorar a camada da nuvem, optando, em vez disso, por conectar sua rede de área doméstica diretamente de um dispositivo móvel ou computador tradicional.

Veículos conectados

Para veículos conectados, a rede local pode ser a Controller Area Network (CAN), à qual as unidades de controle eletrônicas (ECUs) de freios, motor, janelas eletrônicas e outros componentes se conectam. A rede global é sua provedora móvel, enquanto o serviço de nuvem geralmente é a rede do fabricante automobilístico na qual o carro se identifica e você se autentica por meio de um aplicativo no celular.

Carros conectados têm uma série de recursos. Além da capacidade de fazer chamadas para assistência emergencial por meio de um sistema de diagnóstico baseado em assinatura, o carro pode relatar telemetria, como dados de velocidade, local e temperatura do motor. É possível monitorar seu veículo com um aplicativo no dispositivo móvel, dar partida remotamente, ajustar o clima da cabine para um ajuste perfeito de acordo com o clima e determinar a temperatura desejada. O fabricante ou parceiro de serviço poderá analisar a telemetria das ECUs para prever falhas e até mesmo agendar a manutenção, se o calendário de seu smartphone estiver sincronizado com o veículo.

Sistemas de controle industrial e SCADA

Os sistemas de controle industrial e SCADA variam bastante de acordo com o segmento de mercado, a idade e o uso. Por exemplo: uma usina de processamento de cana de açúcar pode ter sistemas mais antigos que informam o status do maquinário e aceitam comandos de controle por meio de uma porta serial. O sistema é controlado com uma linha discada por um console do operador que pode ser segmentado do restante da rede de TI, sem conectividade com a Internet ou capacidade de controlar o sistema SCADA de fora da rede da fábrica. Em comparação, os sistemas de controle industriais mais recentes são criados com sistemas operacionais de propósito geral como base, como Windows e Linux, e são projetados para se conectarem a uma rede IP.

Medidores inteligentes

Os medidores inteligentes estão impulsionando a convergência da tecnologia operacional (como os dispositivos de controle industrial e SCADA discutidos anteriormente) e redes de TI tradicionais, porque a telemetria analisada é fornecida aos sistemas de faturamento e geralmente fica disponível aos clientes por meio de um portal da web. No futuro, os clientes terão a opção de escolher sua fonte de energia — talvez em uma microrrede composta por vizinhos que possuam painéis solares —, conectando-se à nuvem do provedor de energia com seus celulares.

Os clientes também poderão escolher colocar uma máquina lava-louças para funcionar às 2h, quando o painel de energia lhes informar que as tarifas de energia estão mais baratas, empregando a automação doméstica e um uso inteligente da energia. De forma ainda mais interessante, filtros poderão ser definidos para permitir que a lava-louças e o provedor de energia estabeleçam o momento de lavar a louça com base em custos de energia instantâneos.

Dispositivos médicos implantáveis

Dispositivos médicos implantáveis modernos oferecem telemetria a médicos, permitindo que eles monitorem o desempenho do dispositivo e o ajustem. Essa conectividade é fornecida por meio de frequência de rádio a dispositivos de controle especializados e tem alcance limitado. No entanto, a transformação na área da saúde está fazendo com que os pacientes tenham acesso a seus dados por meio de portais e todo o ecossistema de provedores de serviços de saúde e seguradoras tenha uma visão unificada das informações de saúde do paciente. Não é difícil imaginar um marca-passo que possa relatar seu próprio estado aos médicos, podendo estes, por sua vez, ajustar os dispositivos pela Internet, possivelmente com serviços sem fio durante um voo, salvando a vida de pacientes até mesmo durante um voo internacional.

As ameaças às “coisas” já são uma realidade

Pesquisadores modificaram o firmware na unidade telemática de um carro, permitindo acesso a todas as ECUs no veículo. Eles conseguiram desativar com êxito as funções de freio enquanto as rodas do carro giravam a 65 quilômetros por hora. A exploração foi conduzida inserindo um CD fabricado especialmente para isso, contendo arquivos MP3 que, embora estivessem sendo executados normalmente, exploravam uma extravasamento de buffer no software do reprodutor.[8]

O fabricante de um produto projetado para permitir o acesso remoto ao sistema de um prédio, incluin controles para os sistemas de HVAC e segurança, acesso administrativo sem senha e era utilizada para obter acesso não autorizado a pelo menos uma empresa, exibindo “a planta baixa do escritório, com campos de controle e feedback para cada escritório e loja.” O sistema é utilizado por mais de 16.000 organizações e é exposto à Internet sem um firewall para fazer a intervenção.[9]

Práticas criptográficas fracas não apenas deixaram a iluminação conectada à rede vulnerável a danos, como expuseram também as senhas para a rede Wi-Fi à qual estavam conectadas. Apesar de usar o Advanced Encryption Standard (AES), do National Institute of Standards and Technology (NIST) dos Estados Unidos, os dispositivos de iluminação se comunicam por uma rede em malha, usando uma chave pré-compartilhada que nunca muda. [10]

De que as “coisas” precisam

Em suma, embora as “coisas” possam ser diferentes e demandar diferentes controles de segurança (você gostaria de ter de passar um antivírus no seu marca-passo?), nosso modelo ajuda a definir os pontos de proteção e os tipos de controles de segurança que devem ser implementados em cada uma delas. Por exemplo, as “coisas” precisam de:

- **Um sistema operacional seguro com garantias de firmware confiáveis.** Isso inclui a capacidade de realizar atualizações pela rede cabeada ou sem fio em conexões não confiáveis.
- **Um identificador exclusivo.** Embora o IPv6 seja fundamental para identificar as “coisas” em redes, as “coisas” também precisam de uma assinatura a um banco de dados de identidade confiável. Como muitas “coisas” não interagem diretamente com os usuários, como em computadores tradicionais, o con ceito de autenticação tradicional não se aplica (e cred enciais administrativas codificadas permanentemente[11] não s ã o uma solução aceitável). Ainda mais quando as “coisas” interagem em um ambiente machine to machine (M2M), como uma C AN automotiva, é necessário que elas possam confiar interas nas outras
- **Autenticação e controle de acesso fortes.** Quando os usuários acessam ou controlam os dados das “coisas”, geralmente por meio de um serviço de nuvem no dispositivo móvel do usuário, é crucial confirmar se o usuário é quem ele diz ser. Você não gostaria que um ladrão pudesse desbloquear e dar partida em seu carro com um simples nome de usuário e senha, especialmente se considerarmos a recente explosão de credenciais comprometidas[12] e o fato de que a maioria dos usuários escolhe senhas simples. Na verdade, pesquisas mostram que “123456” e “senha” ainda são as duas senhas mais comuns encontradas na Internet.[13]
- **Proteção à privacidade dos dados.** Os dados que fluem das “coisas” ou para elas, e que podem ser armazenados nas “coisas” ou em seus dispositivos de controle, geralmente são sensíveis. Os motoristas podem conectar seus celulares ao sistema de informação e entretenimento do veículo, que tem acesso a informações de contato e possivelmente a email e mensagens de texto. Com os pagamentos móveis começando a aparecer em novos celulares, é possível que as informações de cartão de crédito possam ser acessadas pelo veículo. Credenciais de acesso a sistemas de automação de casas e controles industriais também poderão ser expostas se não forem protegidas adequadamente. Geralmente, a solução para a questão da privacidade é a criptografia de dados e de transmissão
- **Uma forte segurança do aplicativo.** As vulnerabilidades surgem por causa dos erros em programas de software. Os fabricantes de hardware geralmente não são especialistas em desenvolvimento de software, inclusive de aplicativos da web que possam ser instalados na “coisa” ou que existam como portais na nuvem e aplicativos móveis. Dentro da comunidade de software, as vulnerabilidades de segurança são várias e geralmente catastróficas, como mostrado pela recente vulnerabilidade Heartbleed OpenSSL[14] e pela vulnerabilidade ainda mais recente, Bash Shellshock.[15] Os fabricantes das “coisas” têm novas ideias para produtos todos os dias e podem se precipitar em colocar seus produtos no mercado, sem implementar um ciclo de vida de desenvolvimento de segurança ou conduzir testes funcionais e de segurança criteriosos.

O modelo da IBM para a IoT ainda é um trabalho em andamento, uma vez que a IoT, como um todo, ainda está evoluindo. O risco — e também a oportunidade — coexistem justamente nesse nicho.

Esse é o início da revolução das "coisas" e, assim como com os dispositivos móveis, os fabricantes e desenvolvedores das "coisas" podem ajudar a concretizar a necessidade de integrar a segurança desde o início, em vez de aperfeiçoá-la de maneira genérica e retroativa. No entanto, diferentemente do mercado de dispositivos móveis, que é isolado a poucos fabricantes de hardware e a uma quantidade ainda menor de sistemas operacionais móveis, o mercado de fabricação da IoT é muito mais amplo. Muitos fabricantes das "coisas" da IoT são novos e de pequeno porte e, portanto, não possuem fundos ou recursos para incluir a segurança no orçamento e nos planejamentos de design e desenvolvimento. Além da escassez de recursos, existem ainda os desafios residuais a seguir.

- O mercado de software tradicional não teve um bom desempenho na criação de códigos seguros. O fato de a *SQL injection* ainda ser um grande problema é uma triste indicação de que não progredimos de maneira suficiente no treinamento de desenvolvedores, ou do segmento de mercado como um todo, em codificação segura e no teste de aplicativos em desenvolvimento e produção.
- Os fabricantes de hardware, que normalmente constroem as "coisas", em geral não são bons em desenvolvimento de software. E, como mencionado, muitas empresas de software não escrevem códigos seguros muito habilmente.
- A implementação e a configuração de sistemas, programas de software e "coisas" ficam a cargo do usuário final; e nas empresas, do departamento de TI. Os clientes nem sempre pensam sobre segurança e, mesmo quando pensam, pode não ser fácil encontrar ou entender as configurações de segurança em dispositivos da IoT. Além disso, alguns aplicativos exigem configurações muito abertas (e não seguras) para que funcionem. Embora as "coisas" geralmente sejam bens de consumo, elas podem evoluir e se tornar "coisas" corporativas, assim como ocorreu com a tecnologia móvel. A maioria dos departamentos de TI, no entanto, não é responsável por gerenciar a segurança física dessas "coisas". Isso pode indicar uma mudança futura geral em como todos os aspectos da segurança são gerenciados dentro da empresa.
- Muitas "coisas" acabam por exigir endereços IPv6, trazendo com isso uma série de ameaças à segurança. O IPv6 não é bem entendido por muitos sistemas e administradores de rede, muito menos por usuários domésticos que possam ter de configurar um modem a cabo para IPv6. Para proteger uma tecnologia, é preciso primeiro se tornar um especialista em como ela funciona. Poderíamos dedicar toda uma edição do estudo trimestral X-Force de inteligência contra ameaças à segurança de IPv6, incluindo o potencial de utilizá-lo para ataques avançados de *distributed denial of service* (DDoS), túneis em firewalls e ocultação de tecnologias de detecção de invasão e anomalia. Essas, porém, são apenas as ameaças que conhecemos.
- As "coisas" dependem de um conjunto de protocolos amplamente variados, como MQTT, XMPP, DDS, AMQP, Zigbee e Z-Wave, bem como de alguns remanescentes industriais, como o Modbus e DNP3, e novos protocolos automotivos, como os protocolos de comunicação *vehicle to vehicle* (V2V) e *infrastructure to vehicle* (I2V). Cada um deles tem seus próprios desafios de segurança.

Para ajudar a lidar com os desafios de segurança da IoT, o IBM X-Force recomenda que os fabricantes:

- sigam as dez práticas principais do Open Web Application Security Project (OWASP) Para IoT;[16]
- criem uma prática de design e desenvolvimento segura;
- realizem testes de penetração regulares nos produtos;
- sigam as orientações do segmento de mercado, como as do IBM Automotive Security Point of View.[17]

Os tecnologistas também podem ajudar a melhorar a segurança, adotando a IoT com um olhar crítico. Você pode ser um dos primeiros a adotá-la sem ser uma vítima. Compre um novo dispositivo interessante, mas não o coloque em produção cegamente. Teste os produtos quanto à segurança em um ambiente de simulação; depois, trabalhe com os fornecedores para ajudá-los a entender quaisquer falhas e corrigi-las. Se os fornecedores não tiverem uma atitude ativa, siga as orientações de divulgação de vulnerabilidade responsáveis, como aquelas publicadas pelo CERT[18] ou pela equipe X-Force.[19] Trabalhando juntos, podemos todos ajudar a garantir que a IoT se torne um lugar mais seguro e protegido.

A reputação conta: as fontes de malware e botnet

Diretamente de nosso seguro banco de dados sobre reputação de IP, saiba quais países são os principais ofensores quando se trata de infecções por malware e botnet.

Os pesquisadores da IBM X-Force monitoram continuamente sites que contêm malwares e armazenam informações em nosso banco de dados sobre reputação de IP, que os clientes da IBM usam para ajudar a proteger suas redes. Esses sites podem ter sido criados com o propósito de hospedar malware ou podem ser sites legítimos que foram comprometidos e infectados. Nosso banco de dados também contém endereços IP conhecidos por serem usados por serviços de "anonimização", geralmente utilizados para o envio de spam.

Com as recentes divulgações de vulnerabilidades disseminadas, como Heartbleed e Shellshock, a X-Force queria estabelecer uma linha de base das fontes de malwares distribuídos em massa. Nesta seção do relatório, observamos os países em que links maliciosos são hospedados com mais frequência, com base em nossa pesquisa, bem como a distribuição geográfica de servidores de comando e controle (C&C) de botnets. Também comparamos a situação atual aos dados de 14 meses atrás.

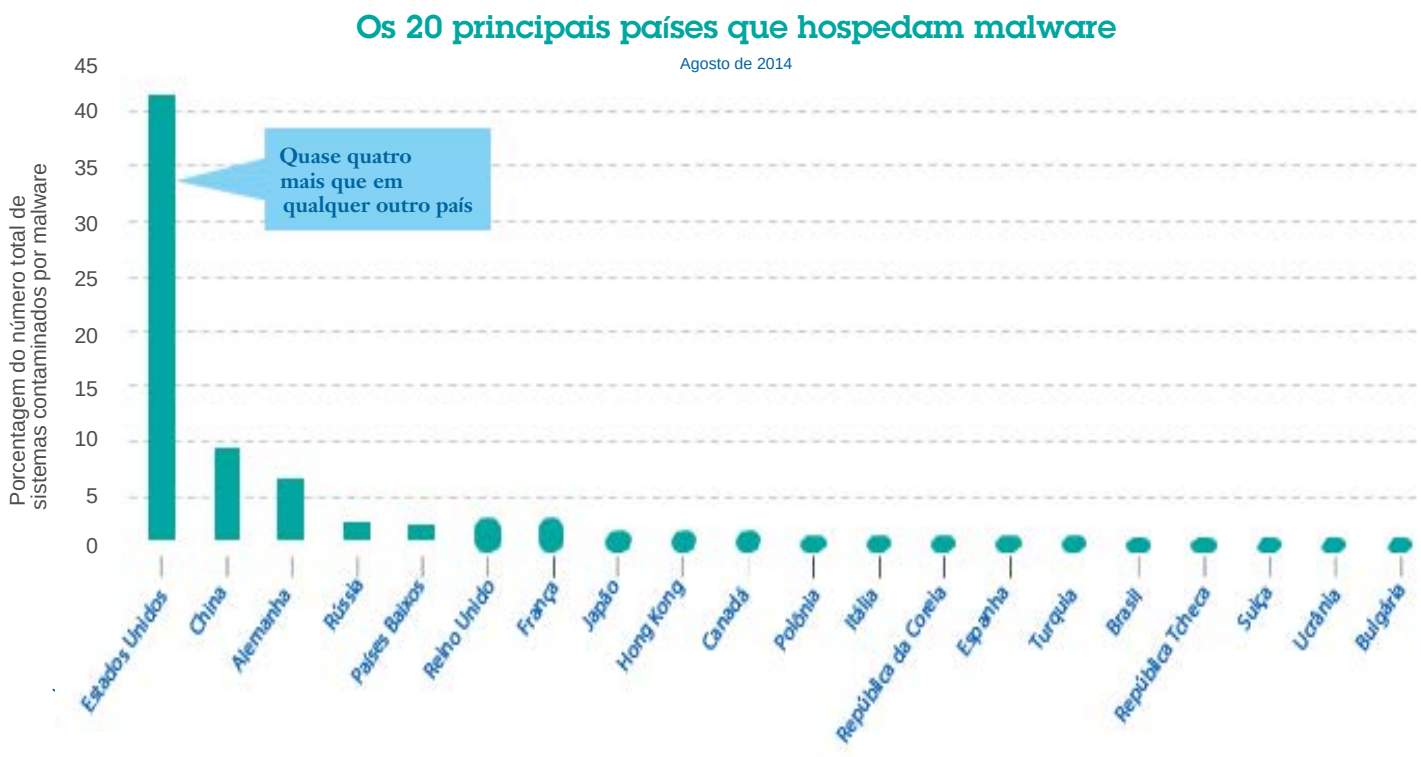

Figure 1. The top 20 malware-hosting countries in August 2014

Em relação aos principais países que hospedam malwares, a Figura 1 mostra que:

- Os Estados Unidos predominam no cenário, hospedando quase 43% de todos os links maliciosos.
- A China tem a segunda maior concentração de links maliciosos, com cerca de 11%. (Curiosamente, essa quantidade quase dobrou em relação ao ano anterior.)
- A Alemanha caiu do segundo para o terceiro lugar, agora hospedando 8,3%, uma redução dos 9,8% há 14 meses.
- Os próximos três países, ocupando as posições de quatro a sete, não sofreram alteração desde 2013. Todos eles hospedam quantidades semelhantes de links maliciosos: a Rússia, a Holanda, o Reino Unido e a França hospedam entre 3,6% e 3,3% dos malwares.

Ao observar a distribuição geográfica dos servidores de C&C de botnets, o quadro é semelhante. A figura 2 mostra que

- Os Estados Unidos hospedam mais servidores de C&C que qualquer outro país, com um quarto do número total de sistemas contaminados. Há 14 meses, no entanto, os EUA hospedavam 4% a mais do que atualmente.
- O país com o segundo maior número de servidores de C&C é a Rússia, com cerca de 9%.

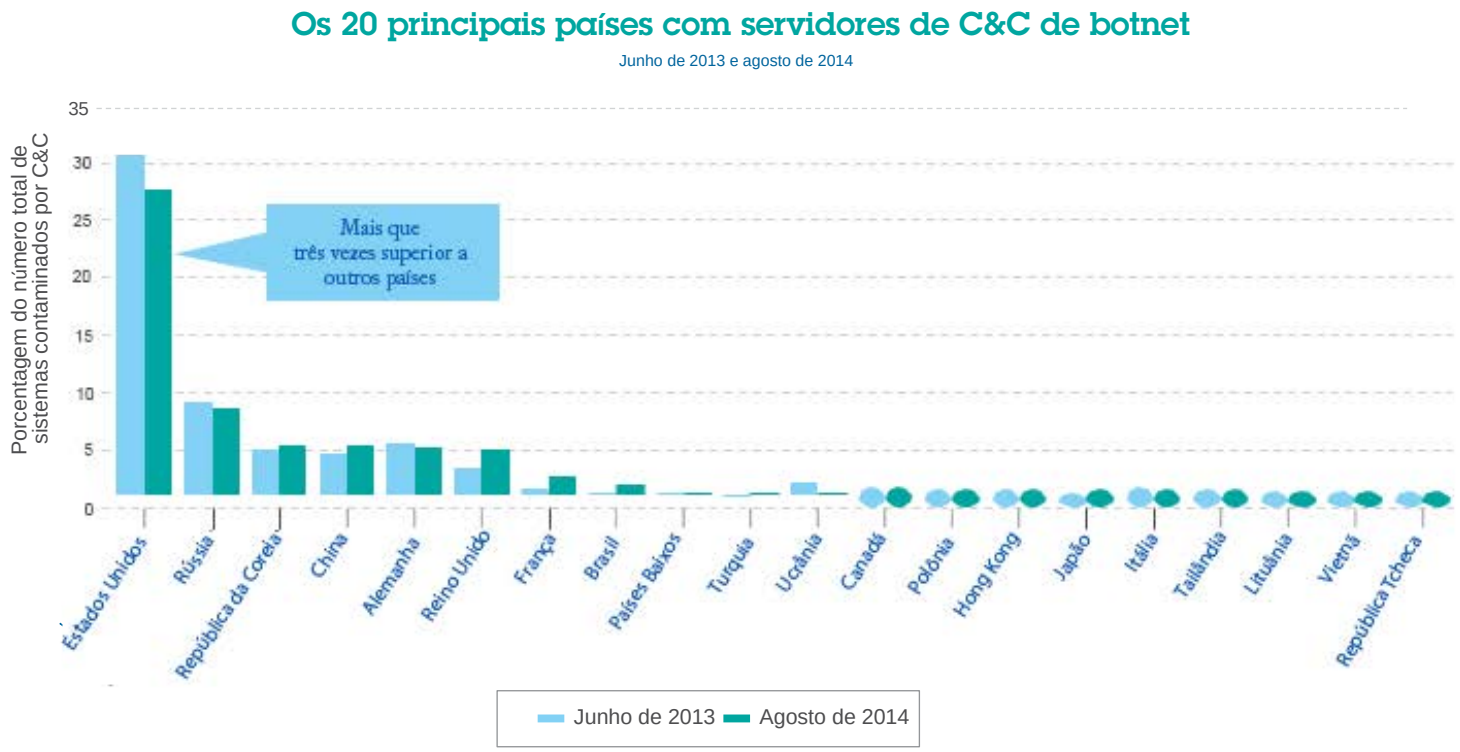

Figura 2. Os 20 principais países com servidores de C&C de botnet em junho de 2013, em comparação a agosto de 2014

- A República da Coreia, a China, a Alemanha e o Reino Unido estão próximos, hospedando entre 7,2% e 6% dos servidores de C&C.

Conforme analisamos nas Figuras 1 e 2, não é de se surpreender que os países com os maiores números de usuários de tecnologia e provedores de serviços apareçam em uma posição mais alta nos rankings. Consequentemente, decidimos normalizar os números com base na proporção de endereços IP como uma porcentagem do total de sistemas que pudessem ter endereços IP no país correspondente.

A Figura 3 mostra que, com dados normalizados, os EUA saem dos 20 principais países que hospedam malware e caem para o número 25. Hong Kong, Lituânia e Bulgária agora aparecem

Figure 3. Malware contamination as a percentage of the total number of systems in a country, August 2014

nas três principais posições. Embora a Lituânia não esteja na liderança na porcentagem de sistemas contaminados por malware, a Figura 4 mostra que ela está na liderança nas contaminações de servidores de C&C.

Ao normalizarmos os dados para as contaminações de servidores de C&C, a Figura 4 mostra que os EUA saem dos 20 principais países em relação aos servidores de C&C e caem para o número 28. Dessa vez, a Rússia passou apenas do segundo para o terceiro lugar. A Lituânia aparece em primeiro com uma grande margem; Bielorrússia, Eslováquia, Ucrânia, Turquia, Tailândia, Hong Kong, Hungria, República Tcheca e Polônia aparecem acima da média, o que corresponde a uma quantia ligeiramente inferior a dois sistemas contaminados por milhão.

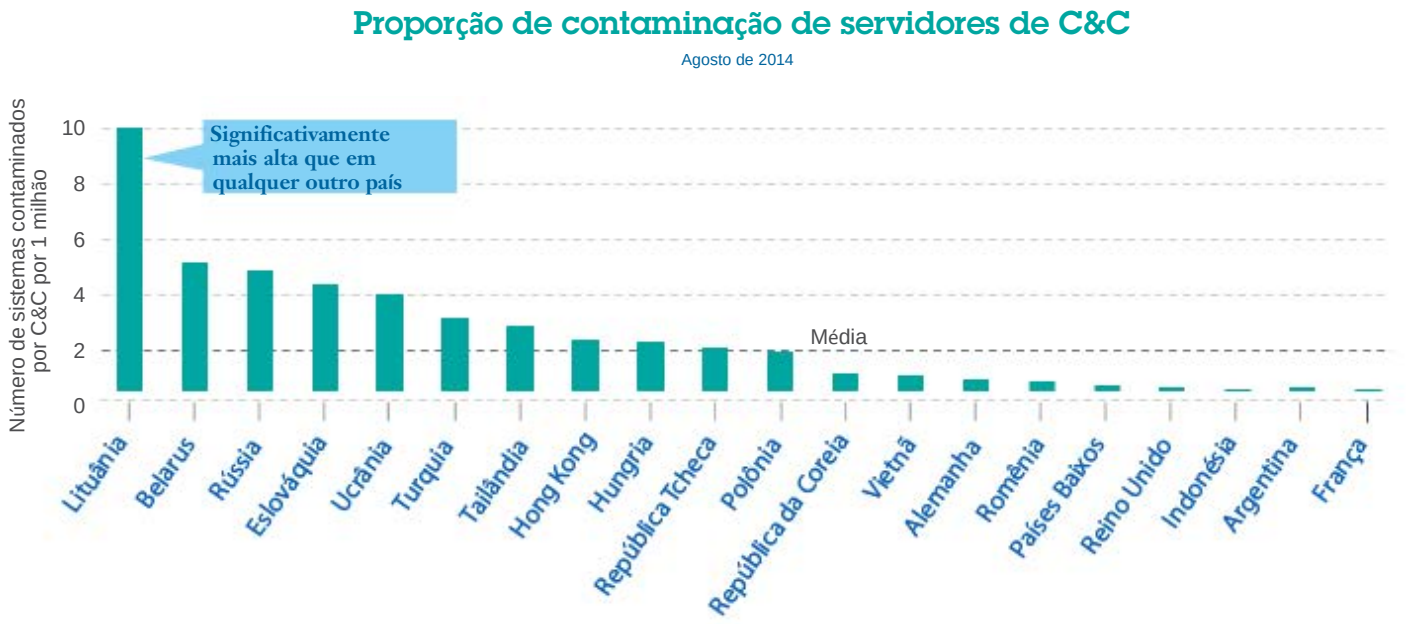

Figura 4. Contaminação de servidores de C&C como uma porcentagem do número total de sistemas no país, agosto de 2014

Comparando dados de 2013 e 2014, quase todos os países reduziram seu número total de contaminações de servidores de C&C, exceto a Lituânia, que, além de estar na principal posição em 2014, permaneceu nessa posição aumentando sua proporção de sistemas contaminados em cerca de um sistema por milhão. A Eslováquia permaneceu na mesma posição ano após ano, enquanto a Indonésia subiu de lugar. Curiosamente, a Ucrânia foi o país que mais reduziu sua proporção de contaminação, em quase cinco sistemas por milhão.

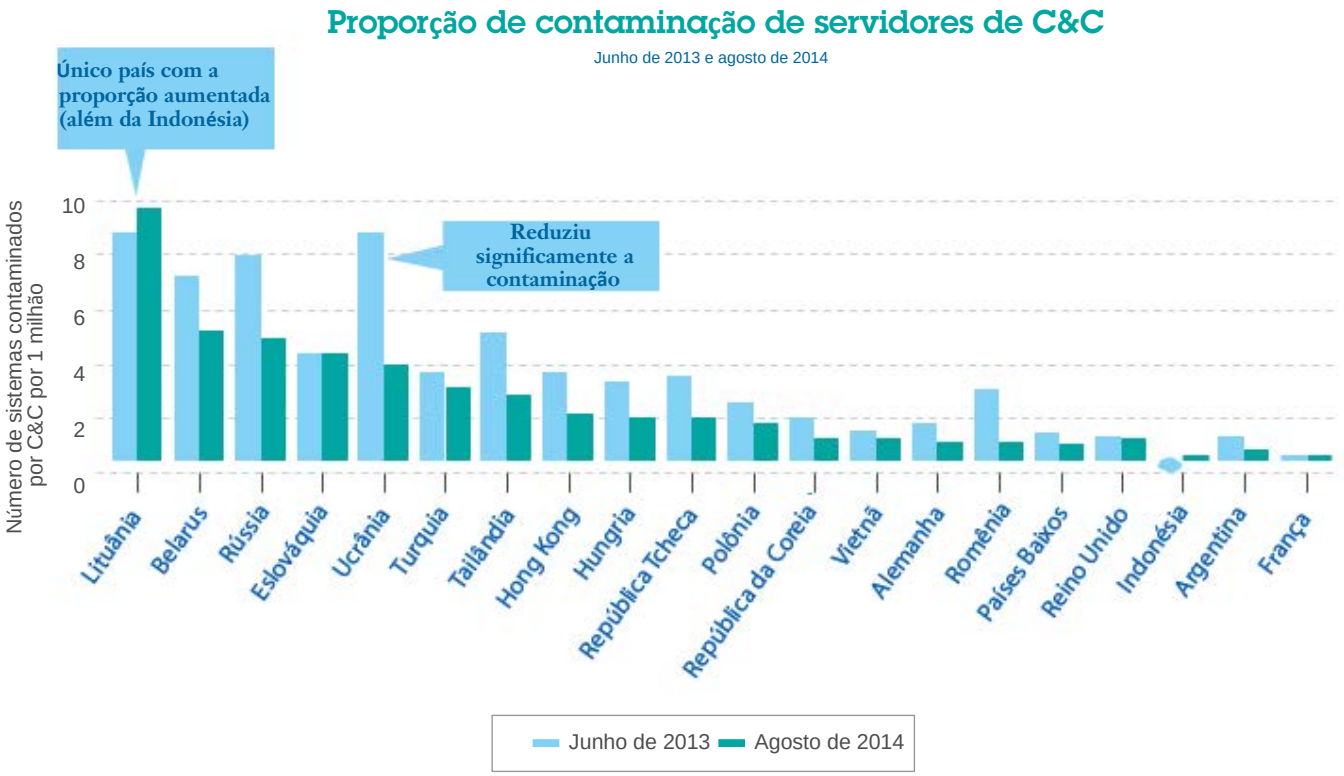

Figura 5. Contaminação de servidores de C&C em junho de 2013, em comparação a agosto de 2014

Observações conclusivas

É interessante ver que a Lituânia predomina no cenário, o que se assemelha a como a Bielorrússia é líder mundial em sua proporção de infecção por spambot (para mais informações sobre infecções por spambot, consulte o estudo trimestral IBM X-Force de inteligência contra ameaças, 2º. Trimestre de 2014).
O conflito militar no leste da Ucrânia pode ser um dos motivos pelos quais esse país agora hospeda somente 0,7% de todos os malwares, enquanto que há 14 meses, 1,4% de todos os links maliciosos podiam ser encontrados em servidores ucranianos. Conflitos miliares tendem a perturbar a apreensão de criminosos. Além disso, uma vez que quase todos os países reduziram seu número total de contaminações de servidores de C&C, os operadores de botnets podem estar distribuindo as infecções a um número maior de países, a fim de se proteger de qualquer ação local contra essas infecções.

Por fim, ao observar os países que hospedam malware e têm servidores de C&C contaminados, os países do Leste Europeu parecem predominar em ambas as listas. Será interessante ver se isso é permanente ou se essa distribuição mudará da mesma forma que ocorreu com os principais países que enviam spam (para mais informações sobre as tendências de spam, consulte o documento estudo semestral de tendências e riscos IBM X-Force, 2º. Semestre de 2013).

Sobre o X-Force

As ameaças avançadas estão em toda parte. Ajude a minimizar riscos com *insights* dos especialistas da IBM.

A equipe de pesquisa e desenvolvimento IBM X-Force estuda e monitora as tendências mais recentes em ameaças, incluindo vulnerabilidades, explorações, ataques ativos, vírus e outros malwares, spams, phishing e conteúdo malicioso da web. Além de aconselhar os clientes e o público em geral sobre as ameaças críticas e emergentes, a IBM X-Force também oferece conteúdo de segurança a fim de ajudar a proteger os clientes IBM dessas ameaças.

Colaboração da IBM Security

A IBM Security representa várias marcas que oferecem um amplo espectro de competências em segurança:

- A equipe de pesquisa e desenvolvimento IBM X-Force descobre, analisa, monitora e registra uma ampla variedade de ameaças de segurança a computadores, vulnerabilidades, além das tendências e dos métodos mais recentes utilizados por invasores. Outros grupos da IBM utilizam esses dados ricos para desenvolver técnicas de proteção para nossos clientes. A família de produtos IBM Security Trusteer®[20] oferece uma plataforma holística de prevenção de crimes cibernéticos em endpoints que ajuda a proteger as organizações contra fraudes financeiras e violações de dados.
- Centenas de organizações e dezenas de milhões de usuários finais dependem desses produtos da IBM Security para proteger seus aplicativos da web, computadores e dispositivos móveis de ameaças online (tais como malwares avançados e ataques de phishing).
- A equipe de segurança de conteúdo da IBM X-Force busca e categoriza a web por meio de rastreamento (*crawling*), descobertas independentes e feeds fornecidos pelo serviço IBM Managed Security Services.
- O serviço IBM Managed Security Services é responsável por monitorar explorações relacionadas a endpoints, servidores (inclusive servidores da web) e infraestrutura de rede em geral. A equipe monitora explorações feitas na web ou por meio de outros vetores, como emails e mensagens instantâneas.
- O serviço IBM Professional Security Services oferece avaliação de segurança em toda a empresa, design e implementação para ajudar a criar soluções eficazes de segurança de informações.
- A QRadar® Security Intelligence Platform oferece uma solução integrada de *security intelligence and event management* (SIEM), gerenciamento de log, gerenciamento de configuração, avaliação de vulnerabilidade e detecção de anomalia. Ela fornece um painel unificado e *insights* em tempo real sobre os riscos de segurança e conformidade de pessoas, dados, aplicativos e infraestrutura.
- O IBM Security AppScan® permite que as organizações avaliem a segurança de aplicativos da web e móveis, fortaleçam o gerenciamento de programas de segurança de aplicativos e estejam em conformidade regulatória com a identificação de vulnerabilidades e geração de relatórios que tenham recomendações inteligentes para facilitar as correções. O serviço IBM Hosted Application Security Management é uma solução baseada em nuvem para testar aplicativos da web dinamicamente com o uso do AppScan em ambientes de pré-produção e produção.

Colaboradores

A produção do estudo trimestral IBM X-Force de inteligência contra ameaças é feita em colaboração com toda a IBM. Gostaríamos de agradecer às pessoas a seguir pela atenção e contribuição para a publicação deste estudo.

Colaborador	Cargo
Chris Poulin	Research Strategist, IBM X-Force
Doug Franklin	Research Technologist, IBM X-Force Advanced Research
Dr. Jens Thamm	Database Manager, IBM X-Force Content Security
Leslie Horacek	Manager, IBM X-Force Threat Response
Marc Noske	Database Administrator, IBM X-Force Content Security
Michael Hamelin	Lead Security Architect, IBM X-Force
Pamela Cobb	Worldwide Market Segment Manager, IBM X-Force, Threat Portfolio
Ralf Iffert	Manager, IBM X-Force Content Security

Para mais informações

Para saber mais sobre a IBM X-Force, acesse: **ibm.com**/security/xforce/

[1] IDC, “Worldwide and Regional Internet of Things 2014–2020 Forecast Update by Technology Split”, Doc # 252330, Data da publicação: novembro de 2014. http://www.idc.com/getdoc.jsp?containerId=252330

[2] Brandon Griggs, “Connected TVs, fridge help launch global cyberattack”, *CNN*, 17 de janeiro 2014. http://www.cnn.com/2014/01/17/tech/gaming- gadgets/attack-appliances-fridge

[3] “CES 2014: Toothbrush ‘tells you how well you brush’”, *BBC News*, 6 de janeiro de 2014. http://www.bbc.co.uk/news/technology-25621422

[4] Ellis Hamburger, “Vessyl is the smart cup that knows exactly what you’re drinking”, *The Verge*, 12 de junho de 2014. http://www.theverge.com/2014/6/12/ 5801106/vessyl-smart-cup-that-knows-exactly-what-youre-drinking

[5] Dan Kaplan, “Black Hat: Insulin pumps can be hacked”, *SC Magazine*, 4 de agosto de 2011. http://www.scmagazine.com/black-hat-insulin-pumps- can-be-hacked/article/209106/

[6] Steve Henn, “With Smarter Cars, The Doors Are Open To Hacking Dangers”, *NPR*, 30 de julho de 2013. http://www.npr.org/blogs/alltechconsidered/2013/07/30/206800198/Smarter-Cars-Open-New-Doors-To-Smarter-Thieves

[7] “Online Energy Monitoring”, *Consumers Energy*, acessado em 8 de outubro de 2014. http://www.consumersenergy.com/content.aspx?id=1696

[8] Robert Vamosi, “Hard-coded Credentials Still Haunt Many Legacy IoT Products”, *Forbes*, 13 de agosto de 2014. http://www.forbes.com/sites/ robertvamosi/2014/08/13/hard-coded-credentials-still-haunt-many- legacy-iot-products/

[9] “Experimental Security Analysis of a Modern Automobile”, *2010 IEEE Symposium on Security and Privacy*. http://www.autosec.org/pubs/ cars-oakland2010.pdf

[10] Dan Goodin, “Intruders hack industrial heating system using backdoor posted”, *Ars Technica*, 13 de dezembro de 2012. http://arstechnica.com/ security/2012/12/intruders-hack-industrial-control-system-using- backdoor-exploit/

[11] Dan Goodin, “Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords”, *Ars Technica*, 7 de julho de 2014. http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/

[12] Danny Yadron, “Russian Hackers Steal 1.2 Billion Usernames and Passwords, Security Firm Says”, *Wall Street Journal*, 5 de agosto de 2014. http://blogs.wsj.com/digits/2014/08/05/security-firm-russian-hackers- amassed-1-2-billion-web-credentials/

[13] “‘Password’ unseated by ‘123456’ on SplashData’s annual ‘Worst Passwords’ list”, *SplashData*, acessado em 21 de outubro de 2014. http://splashdata.com/press/ worstpasswords2013.htm

[14] John Lucassen, “Are Vendors Doing What Is Needed to Mitigate Security Vulnerabilities?” *Blog IBM Security Intelligence*, 30 de junho de 2014. http://xforce.iss.net/xforce/xfdb/92322

[15] Seth Hanford, “Common Vulnerability Scoring System, V3 Development Update”, *FIRST*, junho de 2014. http://xforce.iss.net/xforce/xfdb/96153

[16] OWASP Internet of Things Top 10 Project. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[17] IBM Institute of Business Value, “Transforming the automotive industry: A globally integrated enterprise point of view”, 5 de setembro de 2014. http:// public.dhe.ibm.com/common/ssi/ecm/en/gbe03619usen/GBE03619USEN.PDF

[18] “Vulnerability Disclosure Policy”, CERT. Acessado em 8 de outubro de 2014. http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm

[19] IBM, “IBM Internet Security Systems X-Force Research and Development Team Vulnerability Guidelines”, dezembro de 2008. http://www-935.ibm.com/services/us/iss/xforce/vulnerability-guidelines.pdf

[20] Trusteer, Ltd. foi adquirida pela IBM em setembro de 2013.

Recicle

IBM
Corporation
Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América,
novembro de 2014

WGL03062-BRPT-00