5 previsões para a Internet das Coisas em 2018

Gabriel Dias (*)

A tecnologia conhecida como Internet das Coisas (IoT) está se tornando cada vez mais popular mundialmente. E no Brasil não é diferente. Em 2017, foi possível acompanhar a evolução das conexões entre máquinas, que passaram a ser adotadas em grandes empresas brasileiras, como bancos, operadoras de telefonia e, principalmente, varejistas

De acordo com a Agência Nacional de Telecomunicações (Anatel), o Brasil fechou o mês de outubro de 2017 com 14,8 milhões de conexões máquina a máquina (M2M), usadas em diversas aplicações. Isso representa um crescimento de 20,1% quando comparado com o mesmo período do ano anterior.

Segundo Gabriel Dias, PhD em IoT e líder de projetos da Semantix, empresa especialista em Big Data, Internet das Coisas, Inteligência Artificial e Análise de Dados, o ano de 2018 será especialmente relevante para o caminho de consolidação da tecnologia. O especialista listou cinco previsões que devem permear esse tipo de conexão nas suas mais diversas aplicações. Veja:

1.1. Soluções de IoT para área rural e indústria de base irão despontar no Brasil

O primeiro grande fator de impacto nas tendências do ano que vem é o Plano Nacional de IoT, elaborado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). O documento apontou que os setores rurais, sustentados pelo agronegócio, e as indústrias de base possuem uma alta capacidade de desenvolvimento, uma vez que são responsáveis por grande parte do PIB nacional. Podemos esperar programas de investimento do BNDES que incentivem novos negócios na área agrícola e nas indústrias de base.

1.2. Serviços baseados em IoT melhorarão a experiência do cliente

Com a chegada de novos dispositivos e serviços no mercado brasileiro, grandes empresas investirão no marketing para melhorar a experiência dos clientes do varejo. Por exemplo, ao chegar em um estabelecimento, o cliente poderá receber um alerta sobre a promoção de um produto que ele demonstrou interesse quando visitava a loja virtual.

1.3. As leis europeias deverão permitir a comercialização de dados IoT

Quase metade dos analistas de dados de empresas americanas dizem que já comercializam seus dados, enquanto que apenas 35% da França e 38% da Alemanha o fazem. Reconhecendo este atraso, a Comissão Europeia emitirá orientações para incentivar o uso de tecnologia avançada e estimular a economia de dados. Incentivado pelo avanço europeu, o Brasil deverá evoluir com o projeto de lei PL 5276/2016, que trata da comercialização de dados pessoais.

1.4. Os wearables ainda não serão adotados por todos

Em 2018, os dispositivos vestíveis – ou wearables – irão crescer. Mas ficarão ainda longe de uma adoção completa. De acordo com a consultoria Gartner, serão comercializados cerca de 347 milhões desses dispositivos em todo o mundo. Até 2021, esse número ultrapassar os 500 milhões. No entanto, a Forrester Research, através de um relatório publicado em Novembro, prevê que, diferente dos aparelhos celulares, os relógios inteligentes, o mais difundido dos wearables, ainda devem ficar restritos a um grupo restrito de pessoas. No Brasil, os valores dos smartwatches ainda são altos e as vendas ainda são modestas, mas já existem opções que começam a ficar mais comuns nos grandes centros urbanos.

1.5. A adoção de IoT baseada em blockchain aumentará 5%

O blockchain, tecnologia usada para processar as transações das criptomoedas, como o Bitcoin, ainda não está pronto para implantações em larga escala que exigem confiabilidade, estabilidade e integração com a infraestrutura tecnológica existente. Mas, ideias promissoras estão começando a surgir e a evolução das tecnologias impulsionarão a adoção de blockchain em 2018.

(*) É PhD em IoT e líder de projetos da Semantix.

Conheça 5 kits de ransomware como serviço (RaaS) e como são comercializados

Nos últimos meses, falamos sobre os kits de distribuição de Ransomware vendidos na Dark Web para quem quiser pagar. Esses pacotes RaaS (ransomware como serviço) permitem que pessoas com pouca habilidade técnica possam criar ataques com relativa facilidade

A Naked Security informou sobre a existência desses pacotes individuais e, em julho, lançamos um artigo sobre uma das campanhas mais produtivas de RaasS: a Filadélfia.

Este artigo analisa o problema a partir de cinco kits RaaS disponíveis. A pesquisa foi realizada por Dorka Palotay, uma pesquisadora de ameaças baseada no escritório da SophosLabs em Budapeste, Hungria.

Medir ataques de resgate de RaaS-based é difícil, pois os desenvolvedores são bons para cobrir seus rastros. Amostras recebidas pela SophosLabs mediram desde um único dígito até centenas. A questão que os pesquisadores agora lidam é como as vendas desses kits contribuem para os níveis globais de ransomware como um todo. Conheça abaixo alguns deles:

Filadelfia

A Filadélfia é um dos casos mais sofisticados e experientes no mercado. Há muitas opções e por US $ 389 é possível obter uma licença ilimitada completa.

Os criadores do kit RaaS - Rainmakers Labs - gerenciam seus negócios da mesma forma que uma empresa de software legítimo vende seus produtos e serviços. Enquanto vende Filadélfia em mercados escondidos na Dark Web, ele também possui um vídeo de "introdução" no YouTube, explicando os detalhes do kit e como personalizar o ransomware, com uma variedade de opções de recursos.

Dentre os clientes desse pacote, está uma policial austríaca presa em abril por infectar uma empresa local. Nesse caso, o suposto hacker bloqueou os servidores da empresa e o banco de dados e exigiu US$ 400 para desbloqueá-los. A vítima se recusou, pois a empresa conseguiu recuperar os dados dos backups.

Stampado

Este foi o primeiro kit RaaS disponível da Rainmaker Labs, os criminosos começaram a vender o pacote no verão de 2016 pelo preço baixo de US$ 39.

Com base no Stampado, os desenvolvedores criaram o Filadélfia de forma muito mais sofisticada, incorporando muito da maquiagem de Stampado. O Stampado continua a ser vendido na rede, apesar da criação da Filadélfia.

Frozr Locker

Os kits FileFrozr são oferecidos pelo preço de 0,14 em bitcoins. No caso de ser infectados, os arquivos das vítimas são criptografados. Arquivos com cerca de 250 extensões diferentes serão criptografados. A página Frozr Locker observa que as pessoas devem adquirir uma licença para usar o construtor.

Os criadores também oferecem suporte on-line para os clientes solucionarem suas dúvidas e problemas.

Satan

Este serviço promete gerar uma amostra de trabalho em operação e deixa que você o baixe gratuitamente. Além disso, permite que o cliente estabeleça seu próprio preço e condições de pagamento, coleta o resgate em seu nome, fornece uma ferramenta

de descriptografia para as vítimas que pagam e o pagamento do 70% do produto via Bitcoin.

Seus criadores mantêm os 30% restantes da renda, então, se a vítima pagar um resgate no valor de 1 bitcoin, o cliente recebe 0,7 em bitcoin. Esta taxa se move, dependendo do número de infecções e pagamentos que o cliente pode acumular.

Ao criar uma amostra para enviar ao mundo, os clientes preenchem um formulário para criar o esquema de pagamento. Inclui uma caixa de captcha para se certificar de que você é quem você afirma ser.

RaasBerry

A SophosLabs o detectou pela primeira vez em julho de 2017. Foi anunciado na Dark Web e, como os outros, permite ao cliente personalizar seu ataque. Os pacotes são pré-compilados com um endereço de e-mail e o endereço de e-mail fornecido pelo cliente e o desenvolvedor promete não reduzir os lucros.

Os clientes podem escolher entre cinco pacotes diferentes, desde uma assinatura de comando e controle "Plastic" de um mês, até uma assinatura de três meses "bronze", e assim por diante.

Medidas defensivas – o que fazer?

Por enquanto, o melhor caminho para empresas e indivíduos contra essa ameaça é seguir algumas medidas defensivas contra os resgates:

- Faça uma cópia de segurança regularmente e mantenha uma cópia de backup recente fora do site. Existem dezenas de maneiras, além do ransomware, pelas quais os arquivos podem desaparecer como incêndios, inundação, roubo, um laptop descartado ou mesmo uma exclusão acidental. Criptografe seu backup e você não precisará se preocupar com ele caindo em mãos erradas.
- Não habilite macros em anexos recebidos por e-mail. A Microsoft desativou a execução automática de macros por padrão há muitos anos como medida de segurança. Muitas infecções de malware dependem da ativação de macros, então não faça isso!
- Tenha cuidado com anexos não solicitados. Os criminosos confiam no dilema de que você não deve abrir um documento até ter certeza de que é aquele que deseja, mas você não pode dizer se é o que deseja para abri-lo. Na dúvida, não abra.
- Faça todas as correções com frequência e antecedência. O malware que não entra pelas macros, geralmente depende de erros de segurança em aplicativos populares, incluindo o Office, seu navegador, Flash e muito mais. Quanto mais cedo você corrigir, menos espaços permanecerão abertos para os criminosos explorarem. Em casos como esses, os usuários querem ter certeza de que estão usando as versões mais atualizadas de PDF e Word.

News @TI

Aplicativo com previsão imediata de chuvas para agricultores

@Cientistas do Instituto Nacional de Pesquisas Espaciais (Inpe) estão desenvolvendo um aplicativo com a previsão do tempo e informações pluviométricas voltadas para a agricultura. Com base no SOS Chuva, ferramenta criada para divulgar a previsão imediata de tempestades para a população, o aplicativo "agrícola" vai mostrar onde está chovendo e armazenar dados sobre o volume de água em determinada região para que o agricultor possa acompanhar e identificar eventuais variações de produtividade. A expectativa dos pesquisadores é que a ferramenta contribua para a definição de estratégias para a chamada agrometeorologia de precisão – que analisa a variabilidade da produção a partir de fatores como fertilidade do solo e recursos hídrico. O aplicativo SOS Chuva pode ser baixado na App Store (iOS) e na Google Play Store (Android) (http://soschuva.cptec.inpe.br/soschuva).

CVM confirma: a Niobium Coin (NBC) é um ativo não financeiro

@A área técnica da Comissão de Valores Mobiliários (CVM), autarquia federal que regulamenta o mercado de capitais, tomou uma decisão fundamental neste início de ano. O departamento concluiu que a Niobium Coin (NBC) não é um valor mobiliário. Com isso, a moeda virtual, que servirá como moeda de referência e como meio de troca para as transações com criptomoedas realizadas na Bolsa de Moedas Virtuais Empresariais de São Paulo (Bomesp), não será considerada um ativo financeiro e não está sujeita à fiscalização da CVM. Como um ativo, a Niobium Coin pode ser equiparada ao ouro ou ao diamante. A Niobium Coin é uma commodity digital. "A decisão é inédita no sistema financeiro brasileiro e abre um campo enorme para os ICOs", diz Fernando Barrueco, diretor da Bomesp e responsável jurídico da Fundação Niobium. Segundo a CVM, as moedas virtuais serão consideradas valores mobiliários quando tiverem características de investimento. Por exemplo, quando pagarem juros ou dividendos aos seus investidores, ou quando permitirem a participação na gestão da empresa, por meio de votos (http://bomesp.org/).

Cinco passos para ter uma vida digital mais segura

Ao mesmo tempo em que a navegação na Internet está cada vez mais facilitada e difundida na sociedade, as ameaças e os ataques virtuais não param de crescer. Os cibercriminosos, pessoas que cometem crimes virtuais, parecem estar sempre um passo à frente das autoridades.

Além disso, os usuários não estão fazendo sua parte para terem uma vida digital mais segura: pesquisa da Kaspersky Lab, especialista em antivírus, divulgada em 2017, aponta que 51% das pessoas entrevistadas afirmaram usar métodos inseguros para lembrar senhas, enquanto 22% já revelaram dados confidenciais por acidente. Sendo assim, confira cinco passos para se prevenir da ação dos criminosos na web:

Fortaleça suas senhas: seja do banco, e-mail ou redes sociais, o furto de senhas sempre foi o objetivo principal dos criminosos virtuais. Para não ser mais uma vítima, é preciso ter uma combinação forte que dificulte a ação dos bandidos. O ideal é utilizar a criatividade e fugir de informações óbvias, como datas de aniversários e sequências numéricas simples (como 123456). A recomendação é usar, pelo menos, 16 caracteres no código – além de manter uma senha para cada site. Também é importante incluir entre as boas práticas a troca periódica de senhas e a utilização de cofres de senha como lastpass ou 1password.

Atenção ao tipo de informação compartilhada nas redes sociais: a grande maioria dos usuários disponibiliza em seus perfis dados pessoais que podem facilitar a aplicação de ataques de engenharia social, termo utilizado para descrever situações onde alguém faz uso da persuasão, abusando da ingenuidade e confiança do usuário, para obter informações sigilosas. Recomenda-se diminuir a quantidade de informações compartilhadas, sobretudo check-in/check-out, números de documentos, endereços e telefones. Além disso, é importante limitar sempre a visualização do conteúdo apenas para amigos.

Cuidado com redes públicas: o avanço dos dispositivos móveis fez explodir a rede Wi-Fi. A internet sem fio está praticamente em todo o lugar, inclusive por meio de redes públicas em pontos turísticos e lugares com grande fluxo de pessoas. Porém, elas são mais vulneráveis, o que faz um ataque ser mais propenso. A recomendação é nunca utilizar redes sem fio de terceiros. Caso não tenha outra alternativa, antes de enviar informações pessoais ao usar redes públicas, gratuitas ou compartilhadas, certifique-se de que o ambiente online está protegido com o ícone do cadeado ao lado da barra de navegação. Uma alternativa é utilizar uma rede virtual privada (VPN), garantindo a segurança dos seus dados.

Confira as solicitações de acesso de aplicativos e serviços: aplicativos e serviços gratuitos na Internet utilizam seus dados pessoais para comercializarem publicidade personalizada de acordo com hábitos e comportamentos. Se você deseja limitar isso, é preciso conferir as permissões e os termos de uso antes de realizar o download do app.

Preste atenção nos e-mails: os e-mails ainda são a principal arma dos cibercriminosos para roubar informações e senhas. A tática mais frequente é o phishing, que atrai a atenção do usuário e o estimula a clicar em links e aplicações. Desconfie de mensagens duvidosas que receber, mesmo que o remetente seja uma pessoa de confiança – afinal, elas também podem ter sido vítimas de ataques virtuais.

(Fonte:Rafael Abdo é gerente de segurança da informação da Locaweb).