Tendências 2017

A SEGURANÇA ESTÁ REFÉM

ENJOY SAFER TECHNOLOGY™

CONTEÚDO

Introdução

Há vários anos, a equipe de investigação da ESET elabora o relatório de Tendências, no qual, a partir de uma retrospectiva dos acontecimentos recentes e mais relevantes em matéria de segurança informática, apresentamos os principais assuntos que serão relevantes para as empresas e usuários durante o próximo ano.

Introdução

Ao analisarmos o atual estado e a evolução da tecnologia na atualidade, há um aspecto que ressaltamos: há cada vez mais dispositivos, mais tecnologias e, portanto, um maior número de desafios para se manter a segurança da informação, seja qual for a sua esfera de aplicação.

Este cenário leva-nos à conclusão segundo a qual a segurança deve ser considerada em todos os níveis e, por esta razão, é que nosso documento de Tendências 2017 abrange diversos aspectos. Nos últimos anos, a infecção com códigos maliciosos tem se tornado cada vez mais preocupante e evidente entre os usuários por meio de uma tendência que vem se consolidando: o ransomware. **Este tipo de malware tem chamado a atenção de usuários de todo o mundo ao se deparar com sua informação ou seus sistemas feitos de refém por cibercriminosos.** No entanto, muito além desta proeminente tendência, acreditamos que é necessário falar sobre a segurança em termos mais amplos, já que o êxito do ransomware não deve nos fazer esquecer que existem problemas de segurança em outros âmbitos.

Em meio a todas essas questões, decidimos falar sobre como foi se transformando o panorama no tocante ao relato de vulnerabilidades. O fato de ano após ano o número de vulnerabilidades críticas relatadas não só não retroceder, mas permanecer constante (até mesmo com pequena tendência crescente), indica **a necessidade dos fabricantes e desenvolvedores se comprometerem mais fortemente com o desenvolvimento seguro de produtos e serviços informáticos.** Por outro lado, os ataques cada vez mais frequentes a grandes infraestruturas e serviços na Internet voltaram a levantar o debate acerca da importância de considerar a segurança nas infraestruturas críticas, um assunto que possui um capítulo especial neste relatório, considerando-se a sensibilidade do tema. Escolhemos igualmente atribuir um tratamento especial à salvaguarda da informação no setor da saúde. Ao longo desta seção, são apresentados os desafios deste setor, que manipula dados altamente sensíveis e críticos, razão pela qual se tornou um alvo para muitos criminosos.

De certa forma em relação com os pontos anteriores e a muitas das questões que desenvolvemos nas seções deste relatório, este quadro tem a ver com as legislações em matéria de segurança e tecnologia. Trata-se de um tema com várias implicações que será discutido em um capítulo à parte, porque ele é sem dúvida essencial e os governos de cada país devem assumir a sua importância. Entretanto, ao longo deste capítulo será possível observar que não é tão somente necessário que os governos levem adiante esta tarefa, mas que isso representa um desafio especial quando se tenta firmar acordos com o setor privado e com os indivíduos, em sua dupla natureza: usuários e cidadãos. Mas não somente essas questões mais gerais se apresentam como um desafio para o próximo ano, há igualmente problemas relacionados a questões mais "cotidianas", tais como as ameaças em dispositivos móveis ou na Internet das Coisas (IoT). Isto não é uma novidade; de fato, é algo de que temos falado desde 2012, quando teve início o crescimento da detecção de novas famílias para Android e, um ano mais tarde, apareceram os primeiros códigos maliciosos que afetavam Smart TVs e outros dispositivos inteligentes. No entanto, este ano, dada a proliferação do ransomware, descobrimos uma tendência que aparece no horizonte: o ransomwa-

A segurança deve ser considerada em todos os níveis e, por esta razão, é que nosso documento de Tendências 2017 abrange diversos aspectos.

re of things, o RoT, ou seja, a possibilidade que se abre para que os cibercriminosos **sequestrem um dispositivo e, em seguida, exijam o pagamento de um resgate para devolver o controle ao usuário.**

Em relação à evolução das ameaças em dispositivos móveis, os desafios em termos de segurança para o próximo ano são vários e os revisaremos ao longo da seção correspondente. Seria o modelo de distribuição de aplicativos realmente o mais adequado? **Como é possível garantir o desenvolvimento seguro de aplicativos no contexto de incorporação de outras tecnologias, tais como a realidade aumentada e a realidade virtual, nesses dispositivos cada vez mais poderosos?** Por que os controles de segurança não progridem com a mesma velocidade? Por outro lado, embora pudessem ser consideradas na categoria da Internet das Coisas, os consoles de videogames merecem um capítulo à parte. Esta indústria vem adquirindo cada vez mais relevância e abrange uma ampla variedade de usuários de equipamentos com alta capacidade de processamento à sua disposição, **o que os converte em um alvo muito atraente para os cibercriminosos.** E se somarmos a este quadro a tendência para a integração dos consoles com o ambiente dos equipamentos de escritório, se impõe a evidente necessidade de se falar sobre segurança com este público, uma vez que se apresentam novos vetores de ataque.

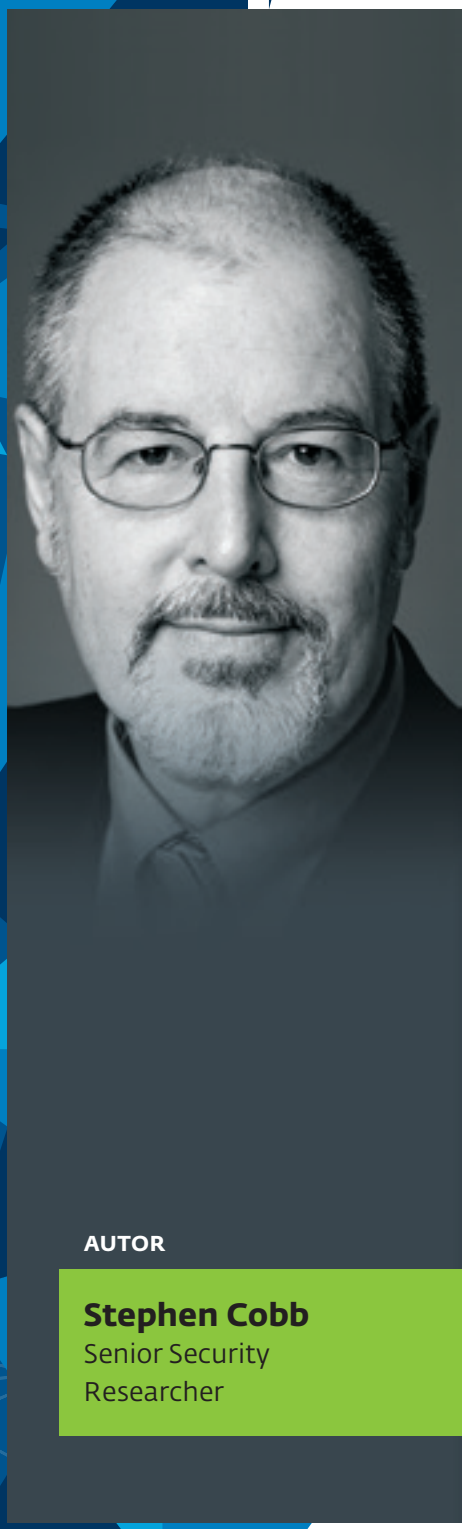
No que diz respeito à esfera empresarial, vale destacar que o aumento das soluções de processamento virtualizado tem atraído a atenção dos criminosos, os quais buscam violar a segurança deste tipo de infraestrutura. Portanto, é provável que assistamos a um crescimento deste tipo de ameaça, de onde vem a necessidade de começar a abordar estas questões como uma tendência de segurança à qual enfrentarão, com cada vez mais frequência, os administradores de sistemas. Entretanto, as tendências apresentadas neste relatório não têm somente a ver com os riscos e ameaças, mas é igualmente preciso destacar algo que está acontecendo na indústria da segurança. Trata-se de uma nova geração de ferramentas de proteção que baseiam a sua estratégia comercial em ignorar o desenvolvimento e a evolução das ferramentas de segurança em geral. Considerando-se a importância desta questão e para evitar confusões, nós nos propusemos a desmistificar e a esclarecer o que vem se constituindo como soluções de segurança da "próxima geração" ou "next-gen".

Há um ponto em comum entre todas essas seções e, de modo geral, em quase todas as questões relacionadas com a segurança da informação: trata-se, nada mais nada menos, que a educação e a conscientização dos usuários. A velocidade com que surgem novas tecnologias e os relatos de ataques, de famílias de malware ou de falhas de segurança **de impacto global fazem da segurança um desafio cada vez mais importante para as empresas, os governos e os usuários dos quatro cantos do planeta.** Ao mesmo tempo, é cada vez mais evidente a importância da educação e da conscientização em matéria de segurança, a fim de impedir que as ameaças continuem avançando. Ao longo da seção correlata, revisaremos os vários problemas associados a essa questão e veremos que a educação dos usuários não está acompanhando a velocidade com que surgem as novas tecnologias e as ameaças a elas associadas. Para nós é um prazer apresentar-lhes a publicação por nós preparada nos Laboratórios da ESET em nível global, para revelarmos os desafios em matéria de segurança que devem ser enfrentados em todos os níveis no ano de 2017. A nossa ideia é que todos possam desfrutar deste documento ou, caso convier, que sejam lidos aqueles assuntos relativamente aos quais haja mais interesse ou identificação em seu dia a dia enquanto usuários. Em suma, **o nosso objetivo é permitir que os usuários possam descobrir o que os aguarda em matéria de segurança, com o objetivo de estarem mais bem preparados para enfrentarem os desafios associados e,** assim, poderem estar mais protegidos.

Há um ponto em comum entre todas essas seções e, de modo geral, em quase todas as questões relacionadas com a segurança da informação: trata-se, nada mais nada menos, que a educação e a conscientização dos usuários.

RoT:
o Ransomware das Coisas

- Ameaças do passado e do futuro
- Como impedir o RoT



AUTOR

Stephen Cobb
Senior Security Researcher

1

RoT: o Ransomware das Coisas

De todas as tendências de 2016, a que achei mais preocupante foi a disposição de algumas pessoas em participar das três atividades a seguir em escala: usar sistemas de informação e arquivos de dados como reféns (por meio de ataques de ransomware); negar acesso a dados e sistemas (com ataques de negação de serviço distribuído ou DDoS); e infectar dispositivos que fazem parte da Internet das Coisas (IoT).

Infelizmente, acredito que estas tendências continuarão existindo em 2017 e é possível que, inclusive, se combinem à medida que evoluem. Um exemplo disso é o uso de dispositivos IoT infectados para extorquir sites comerciais ao ameaçar um ataque DDoS ou ao bloquear dispositivos IoT para cobrar um resgate, algo que eu gosto de chamar de "jackware".

Ameaças do passado e do futuro

O uso indevido dos sistemas informáticos para extorquir dinheiro é quase tão antigo quanto a própria computação. Em 1985, um funcionário de TI de uma empresa de seguros americana programou uma bomba lógica que apagaria registros vitais se um dia ele fosse demitido. Isso aconteceu dois anos depois, quando a bomba foi ativada e gerou a primeira condenação por esse tipo de crime cibernético. Em 1989, foi observado um tipo de malware que usava a criptografia para sequestrar arquivos e pedir resgate, como relata David Harley. Em 2011, bloquear computadores para cobrar um resgate começou a "virar algo cada vez mais apelativo", assim como explica meu colega Cameron Camp.

Mas como esses elementos vão evoluir ou se combinar em 2017? Algumas pessoas têm chamado 2016 de "O ano do ransomware", mas receio que a futura manchete será: "O ano do jackware". **O jackware é um software malicioso que tenta assumir o controle de um dispositivo, cujo principal objetivo não é o processamento de dados, nem a comunicação digital.**

Um bom exemplo são os "carros conectados" – como muitos dos modelos mais recentes na atualidade. Esses automóveis executam muita comunicação e processamento de dados, mas seu principal objetivo é fazer com que você vá desde o ponto A até o ponto B. Sendo assim, **pense nos jackware como um tipo especializado de ransomware.** Com o ransomware comum, como o Locky e o CryptoLocker, o código malicioso criptografa os documentos do seu computador e exige o pagamento de um resgate para desbloqueá-los. **O objetivo do jackware é manter um carro bloqueado ou outro dispositivo até você realizar o pagamento.**

A cena de uma vítima de jackware pode ser a seguinte: em uma manhã fria de inverno, uso o aplicativo do carro no meu telefone para dar a partida (de longe) enquanto ainda estou dentro da minha cozinha, mas o carro não liga. Na hora, já recebo uma mensagem no telefone me dizendo que preciso enviar uma certa quantia em moeda digital para reativar meu veículo. **Felizmente, pelo que eu saiba, o jackware ainda é algo teórico** – uma informação muito relevante. Ele ainda não está acontecendo na prática. Infelizmente, confor-

Algumas pessoas têm chamado 2016 de "O ano do ransomware", mas receio que a futura manchete será: "O ano do jackware".

me já vimos no passado, devo admitir que **não tenho muita fé na capacidade que o mundo tem de deter o desenvolvimento e a implantação do jackware.** Já vimos que uma empresa automotiva pode vender mais de um milhão de veículos com vulnerabilidades que poderiam ser exploradas pelo jackware: esse foi o caso do Jeep da Fiat Chrysler que apareceu em todos os noticiários em 2015.

Tão grave quanto essas vulnerabilidades foi a aparente falta de planejamento da empresa para corrigir as vulnerabilidades do processo de design desses veículos. Uma coisa é vender um produto digital com "falhas" que serão descobertas posteriormente; na verdade, isso é quase inevitável. **Porém, outra coisa muito mais perigosa é vender produtos digitais sem contar com uma forma rápida e segura de dar um jeito nesses problemas.**

Embora a maioria das pesquisas e discussões sobre as "hacking de automóveis" sejam sobre questões técnicas do interior do veículo, é importante perceber **que boa parte da tecnologia IoT depende de um sistema de apoio que vai muito além do próprio aparelho.** Vimos isso em 2015 com a VTech, que atua na área da internet das coisas para crianças (IoCT). Uma falha de segurança no site da empresa expôs dados pessoais sobre os jovens, mostrando a todos quantas possibilidades de ataque são criadas por meio da IoT.

Também vimos esse problema de infraestrutura em 2016, quando algumas contas da Fitbit apresentaram problemas (que fique claro: os aparelhos Fitbit não sofreram uma invasão, e a Fitbit parece levar a privacidade muito a sério). Algumas falhas foram descobertas no aplicativo do BMW ConnectedDrive para a web – que conecta as BMWs à internet das coisas – também este ano. Por exemplo: é possível usar esse software para regular o aquecimento, as luzes e o sistema de alarme da sua casa de dentro de seu veículo. Pensar que os recursos e as configurações de um sistema automotivo de bordo possam ser administrados à distância **por meio de um portal que poderia ser invadido é no mínimo perturbador.** E continuamos ouvindo relatos sobre falta de segurança digital automotiva, como os casos da Mitsubishi com Wi-Fi, e os rádios que são invadidos e usados para roubar BMW, Audis eToyota.

Embora eu visse o jackware como uma evolução dos códigos maliciosos contra veículos, ficou claro que essa tendência pode ser ainda mais ampla e virar o **ransomware das coisas** (RoT). Uma história arrepiante de uma cidade finlandesa mostra um dos caminhos que isso pode tomar ataque DDoS interrompe o sistema de calefação da Finlândia em pleno inverno. Apesar desses relatos não conterem indícios de pedidos de resgate, **não é preciso ter uma imaginação muito fértil para imaginar qual será o próximo passo.** Quer que paremos de controlar o sistema de calefação? É só abrir a carteira!

Ficou claro que essa tendência pode ser ainda mais ampla e virar o ransomware das coisas (RoT).

Como impedir o RoT

Para evitar que a IoT vire o habitat natural do RoT, muito precisa acontecer em dois âmbitos diferentes da atividade humana. **O primeiro é o técnico,** no qual implementar a segurança em uma plataforma automotiva é um desafio considerável. As técnicas tradicionais de segurança– como filtragem, criptografia e autenticação – podem exigir um poder de processamento e largura de banda dispendiosos, adicionando uma sobrecarga aos sistemas (alguns dos quais precisam operar com uma latência muito baixa).

Técnicas de segurança como as air-gapping e a redundância podem aumentar o custo dos veículos de maneira significativa. E nós sabemos que o controle de custos centavo por centavo. O segundo âmbito é o políti-

co, **em que é necessário tomar medida**s para frear o RoT. Nossa perspectiva aqui não é das melhores, pois o mundo perdeu para o cibercrime até o momento.

Houve uma falha coletiva internacional em evitar que uma infraestrutura criminosa prosperasse no mundo digital, o que está ameaçando toda inovação imaginável na tecnologia digital, desde a telemedicina até os drones, dados de big data e carros autônomos. Por exemplo: como se mencionou na sessão "Desafios e implicações das legislações sobre cibersegurança" os políticos americanos mais preocupados não conseguiram aprovar uma legislação em 2016 que ajudaria a proteger a rede inteligente, apesar da proposta ter recebido um apoio de todos os partidos. **É claro que os termos "RoT" e "jackware" não foram criados para causar nenhum alarde. Eles simbolizam coisas que podem acabar existindo se não fizermos o suficiente para impedi-las de virar uma realidade em 2017.**

No entanto, **eu gostaria de concluir com algumas notícias positivas sobre o assunto.** Em primeiro lugar, diversas agências governamentais têm intensificado seus esforços para deixar a IoT mais segura.

Em 2016, foram publicados os artigos Princípios estratégicos para proteger a internet das coisas (PDF) do DHS (Departamento de Segurança Interna dos EUA) e a Publicação especial NIST 800-160 (PDF). O título completo desse segundo documento é "*Considerações sobre engenharia de sistemas de segurança para uma abordagem multidisciplinar na engenharia de sistemas de segurança confiáveis*". O NIST é o Instituto Nacional de Padrões e Tecnologias dos Estados Unidos e faz parte do Departamento de Comércio dos EUA. Ao longo dos anos, essa agência tem exercido uma influência positiva em muitos aspectos da segurança digital.

Em 2017, **tomara para que esses e outros esforços ao redor do mundo nos ajudem a melhorar a proteção da nossa vida digital contra quem opta por abusar da tecnologia para fins de extorsão.**

Por fim, os resultados de uma pesquisa do ESET aos consumidores – um tipo diferente de publicação – traz indícios de que talvez estejamos melhorando um pouco pelo menos com relação à conscientização pública do potencial problemático da IoT, assim como suas vantagens e benefícios de produtividade. Com o título "Nossa vida digital cada vez mais conectada" a pesquisa revelou que mais de 40% dos adultos americanos não acreditam que os dispositivos da IoT sejam seguros e protegidos. Além disso, mais da metade dos entrevistados declarou que desistiu de comprar um dispositivo de IoT por se preocupar com as questões de segurança e privacidade.

Será que a postura **dos consumidores e a orientação governamental** conseguirão fazer com que as **empresas deixem a IoT mais resistente** contra abusos? Talvez venhamos **a descobrir isso em 2017.**

Houve uma falha coletiva internacional em evitar que uma infraestrutura criminosa prosperasse no mundo digital.

A educação em segurança, uma responsabilidade a nível social

- Mudam as ameaças, mas a propagação é mantida
- Crime cibernético: uma atividade impiedosa e eficaz
- A educação não é apenas uma questão de idade
- O paradoxo atual: mais informação, menos sensação de segurança
- Pequenas mudanças fazem grandes diferenças
- A capacitação faz a diferença

AUTOR

Camilo Gutiérrez
Head of Awareness & Research

A educação em segurança, uma responsabilidade a nível social

Há uma ameaça já presente há muitos anos entre nós e que durante 2016 completou 25 anos da sua disseminação por meio de emails.

Milhões de usuários na rede se depararam com ela, mas embora muitos possam identificá-la, a realidade é que ainda há pessoas que podem ser envolvidas pelo golpe, algumas por inocência e por desconhecimento e outras por simples curiosidade acabam respondendo para ver o que vai acontecer e por fim se tornam vítimas.

Se ainda não sabem a que me refiro, vamos desvendar o mistério: **é o famoso "golpe nigeriano" ou "scam 419".** A origem deste tipo de fraude remonta ao século XIX, com cartas contendo oferta para a partilha de um vultuoso tesouro. Mas este golpe centenário, longe de desaparecer, **ganhou força com a evolução tecnológica e,** com o passar dos anos, surgiram múltiplas variantes que migraram para os sistemas de email.

Após tanto tempo, ainda continuamos vendo mensagens em redes sociais e páginas da web com o mesmo tipo de golpes, em que: "você é o visitante número 1.000.000", "você ganhou na loteria" ou "você foi escolhido para uma viagem dos sonhos", são apenas alguns dos pretextos. Entretanto, ainda que as ameaças cibernéticas tenham evoluído nos últimos anos e até falarmos de ataques direcionados, guerra cibernética e APT (Advanced Persistent Threat ou Ameaça Persistente Avançada), **por que ainda se continua vendo esse tipo de golpe?**

Mudam as ameaças, mas a propagação é mantida

Há apenas cinco anos, no nosso relatório Tendências para 2012, discutimos a crescente tendência para malware em dispositivos móveis, onde ameaças tais como as botnets (redes de computadores infectados por bots semelhantes) estavam no auge. Nos últimos anos, os riscos têm evoluído: começamos a falar sobre espionagem cibernética e de ataques direcionados, de ameaças à privacidade e dos desafios para a segurança nos novos dispositivos IoT (Internet das Coisas) e, **para 2017, acreditamos que o ransomware continuará aumentando o seu número de vítimas.**

No entanto, todos estes tipos de ameaças, que se transformaram com o tempo têm **um fator em comum: o usuário como um *gateway* ou porta de entrada**. Seja por meio de um email, um dispositivo USB deixado de propósito em um compartimento, uma mensagem em uma rede social ou uma senha fraca, **os atacantes continuam se beneficiando do comportamento inocente e, em muitos casos, irresponsável de usuários** para conseguirem possíveis meios de comprometer a segurança de um sistema.

Infelizmente, em 2017 e nos anos subsequentes, essas práticas continuarão sendo aproveitadas pelos ataques. A realidade é que, embora possa haver vulnerabilidades em dispositivos ou aplicativos que permitem a um invasor assumir o controle de um sistema, **o modo mais fácil de fazê-lo é enganando usuários.** Por que passar horas no desenvolvimento de um exploit, quando através de um simples email é possível conseguir o mesmo tipo de acesso aos

Por que um ladrão se esforçaria para cavar um túnel a fim de entrar em uma casa, se basta bater à porta?

sistemas? Ou, sob outra perspectiva: Por que um ladrão se esforçaria para cavar um túnel a fim de entrar em uma casa, se basta bater à porta?

Crime cibernético: uma atividade impiedosa e eficaz

Para 2017, é difícil negar que continuaremos observando a evolução das famílias de códigos maliciosos, que o **ransomware continuará o seu infame reinado como a ameaça mais disseminada, assim como seria inocente ignorar que em breve veremos mais ameaças contra dispositivos IoT.** O crime cibernético chegou a ser classificado como uma atividade impiedosa, em que até setores como a saúde são ameaçados e infraestruturas como os caixas eletrônicos encontram-se em risco latente a nível global.

Além disso, durante 2016, tornou-se claro como os cibercriminosos de hoje vêm armados não tão somente com diferentes tipos de softwares maliciosos e técnicas de Engenharia Social, mas igualmente com os "planos de negócios" **para extorquir as suas vítimas e obterem algum tipo de vantagem econômica.**

Estamos diante da necessidade de deixarmos de falar genericamente quando se trata de riscos de segurança. **É necessário que os usuários, quer seja no âmbito corporativo ou na esfera pessoal, reconheçam os ataques passíveis de afetá-los.** Desde um golpe por email até um sequestro de informações, tudo deve ser concebido como factível, sendo necessário tomar as medidas cabíveis de conscientização e tecnológicas para evitá-los.

A educação não é apenas uma questão de idade

O mundo digital está habitado por dois tipos de seres: o**s nativos e os imigrantes digitais.** Os primeiros incorporaram o uso da tecnologia na maioria dos aspectos da sua vida diária desde a primeira idade; em contrapartida, os segundos empregam-na para resolver muitas das suas atividades diárias, embora tenham sido obrigados a se adaptarem e a acostumarem-se para fazê-lo.

Seria de se esperar que os nativos digitais estivessem menos vulneráveis a esse tipo de golpe. No entanto, neste ano, um estudo do BBB Institute evidenciou que **os jovens entre 25 e 34 anos são mais vulneráveis a scams,** ao passo que outros estudos mostram que os mais jovens são aqueles com o comportamento mais arriscado ao navegarem na Internet, tais como se conectar a redes Wi-Fi não protegidas, ligar dispositivos USB entregues por terceiros, sem as devidas precauções, bem como a reduzida utilização de soluções de segurança.

Por outro lado, enquanto os imigrantes digitais podem ser mais cautelosos ao empregarem a tecnologia, notamos que muitas vezes eles podem ser vítimas de ataques ou ter comportamentos inseguros. Geralmente, é devido ao **desconhecimento das características dos recursos em matérias de segurança disponíveis nos diferentes dispositivos,** bem como à falta de informação acerca do alcance das ameaças eletrônicas e dos cuidados correlatos a serem tomados.Ao final das contas, pouco importa a idade. **A necessidade de todos os usuários disporem de conhecimentos sobre as ameaças, acerca do modo de atuação destas últimas e no tocante a quais dispositivos** são aqueles em que os usuários devem focar as suas atenções para se protegerem.

O paradoxo atual: mais informação, menos sensação de segurança

Sem dúvida, há quase quatro anos, após as revelações de Snowden, **a sensação**

É necessário que os usuários, quer seja no âmbito corporativo ou na esfera pessoal, reconheçam os ataques passíveis de afetá-los.

de segurança em relação à informação é cada vez menor. O paradoxo é que **atualmente há mais informações sobre o que acontece com ela.**

Sentir-se monitorado é uma preocupação para muitos usuários e, justamente, uma das mais importantes lições aprendidas com as revelações de Snowden é a seguinte: caso alguém seja autorizado a agir secretamente e se a esta pessoa for atribuído um orçamento substancial, não pode supor que, por melhor que seja a pessoa, **ela irá fazer a coisa certa, da maneira correta e sem consequências prejudiciais.**

Contudo, **não se trata de cair na paranoia ou de pensar em não usufruir de qualquer conexão à Internet.** Um desafio importante a ser enfrentado é **a necessidade de se capacitar e conhecer os meios de se proteger na rede,** de se saber qual tipo de informação é passível de publicação na rede e quais medidas de proteção permitirão garantir a segurança e a privacidade das informações.

Pequenas mudanças fazem grandes diferenças

Na ESET, acreditamos firmemente que a segurança não se reduz tão somente a uma solução tecnológica, considerando que **nela há igualmente um componente humano que deve ser protegido.** Muito embora os esforços de sensibilização e de conscientização em matéria de segurança informática já sejam uma realidade em muitas esferas da vida moderna, há muitos usuários que ainda não têm capacitação adequada neste âmbito. Enquanto muitos reconhecem as ameaças aos computadores, isso ainda **não ocorre no tocante a dispositivos móveis e ainda menos em relação aos dispositivos IoT.**

De acordo com levantamentos realizados pela ESET, apenas **30% dos usuários adotaram uma solução de segurança em seus dispositivos móveis[1],** ainda que mais de **80% reconheçam que os usuários são aqueles sobre os quais recai a maior parcela de responsabilidade** quando ocorrem fraudes e golpes, em razão de não tomarem consciência ou estarem informados acerca dos diferentes crimes.

No transcorrer dos próximos anos, veremos como as ameaças começam a se propagar para atingir todo tipo de dispositivo conectado à Internet e que manipulam informações sensíveis. Assim sendo, **é necessário pensar na segurança a todo momento e em qualquer contexto,** desde quando se trata de um dispositivo de uso pessoal com conexão Wi-Fi, até infraestruturas críticas, conectadas remotamente através da Internet. É indiscutível que todas as tecnologias estão mudando rapidamente e que cada vez mais modos de infecção podem ser facilmente explorados por cibercriminosos, desde que os usuários não sejam capacitados para tratar estas questões. Por isso, não se pode permitir que o avanço da tecnologia se volte contra o próprio usuário.

Em 2017, as tendências em matéria de proteção devem acompanhar a progressão dos incidentes de segurança identificados e, por esta razão, a capacitação é essencial. Se os usuários reconhecerem que o uso de uma senha como medida única possa representar um risco de vazamento de informações, eles saberão que a adoção de um mecanismo de dupla autenticação, acrescentando uma camada adicional de segurança, vai fazer a diferença a seu favor. Deste modo, além de reconhecer as ameaças, **o desafio reside na capacitação para o uso de ferramentas de segurança capazes de manterem protegidas as suas informações.** Caso contrário, o

Não se pode permitir que o avanço da tecnologia se volte contra o próprio usuário.

1- Pesquisa realizada pela ESET América Latina com a comunidade online durante agosto de 2016.

crescimento de ameaças e ataques continuará sendo uma constante. Da mesma forma, a melhor maneira de garantir a confidencialidade da informação consiste em fazer uso das tecnologias de criptografia em todas as modalidades de comunicação. Ao mesmo tempo, quando se fala de ransomware, a melhor maneira de assegurar-se contra a perda definitiva de informações reside em manter um backup adequado dos dados mais sensíveis.Entretanto, a adoção destas tecnologias ao longo do próximo ano parte do reconhecimento das ameaças e a base fundamental para isso é dispor de usuários capacitados e capazes de decidir sobre qual é o melhor modo de se proteger.

A capacitação faz a diferença

Para todos que atuam no mundo da segurança informática, **não há melhor máxima que aquela segundo a qual o elo mais fraco da cadeia é o usuário final.**

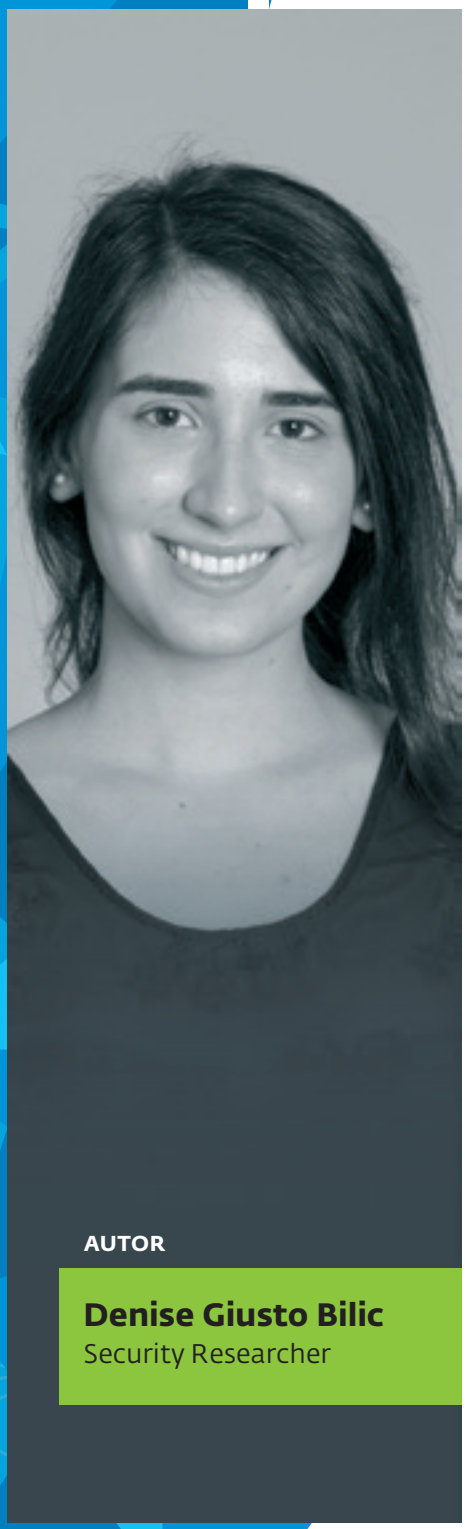
Tendo em vista que desde 2015 foi feita a advertência de haver cada vez mais e mais tecnologia da informação para se defender e levando-se em conta que, mesmo assim, o número de pessoas capacitadas para garantir esta proteção é perigosamente reduzido, **é imprescindível ver na capacitação um fator-chave para se fazer a diferença.** Embora todo o processo de capacitação e treinamento de novos profissionais da área de segurança não seja algo imediato, **nos próximos anos, o foco deve ser orientado para a conscientização dos usuários** acerca dos cuidados básicos na Internet, porque **nela está a massa crítica da qual se aproveitam os criminosos para obterem os seus ganhos.** Assim sendo, o grande desafio daqueles que responsabilizamos pela segurança consiste em convertê-los na linha de frente da defesa das informações: a capacitação e o treinamento como ferramenta para ensinar os usuários acerca das ameaças atuais e como elas se propagam é o que pode fazer a diferença no futuro para reduzir o impacto do crime cibernético. Não se pode esquecer que a segurança é algo transversal, não sendo atribuição exclusiva daqueles que trabalham com tecnologia: atualmente, é tão crítica uma informação manipulada por um jornalista quanto aquela processada por um executivo, tornando-se, inclusive, mais sensível quando se trata de profissionais da saúde e dos prontuários de pacientes diariamente manipulados.

Para alcançar este objetivo, é imperativa a participação ativa dos governos e das empresas. Chegamos a um ponto em que, no âmbito da capacitação e do treinamento, tornou-se imprescindível tratar de modo formal as questões de segurança e que as empresas não deixem essas questões apenas no campo da mera sugestão, induzida no momento da contratação do colaborador, mas, ao contrário, **que elas sejam tratadas ininterruptamente, de modo contínuo e constante**. O usuário final deve se sentir **como parte de toda a cadeia de segurança,** cabendo-lhe entender, em primeira instância, que existem ameaças, mas que também existem os mecanismos necessários para desfrutar da tecnologia de forma segura.

Não se pode esquecer que a segurança é algo transversal, não sendo atribuição exclusiva daqueles que trabalham com tecnologia.

A realidade (aumentada) do malware móvel

- Superando os limites da percepção
- Aplicativos vulneráveis com API não tão seguras
- Android, um sistema inseguro?
- Apps maliciosos em lojas oficiais
- Facilidade de atualização
- Plataformas móveis sob ataque



AUTOR

Denise Giusto Bilic
Security Researcher

3

A realidade (aumentada) do malware móvel

Inicialmente, esperava-se que os dispositivos móveis evoluíssem para se tornarem computadores de mão tão capazes quanto qualquer desktop. É claro que hoje os nossos smartphones e tablets transcenderam esta finalidade, criando novas formas de interação tecnológica antes inimagináveis.

Neste contexto de revolução sócio-tecnológica, **aquilo que existe de mais avançado em termos de realidade virtual incorpora novos riscos no tocante à segurança, afetando não somente a informação digital, mas o próprio bem-estar físico do usuário.** Enquanto determinados aplicativos concentrem dados cada vez mais sensíveis, os **malware ou software maliciosos voltados para dispositivos móveis estão se expandindo e se tornando cada vez mais complexos,** elevando a importância do desenvolvimento seguro. Tendo em vista o grande número de vítimas potenciais, as lojas oficiais de aplicativos são abatidas diante **das novas campanhas de códigos maliciosos que se multiplicam no mercado.** Seria este o cenário que nos espera no que diz respeito às tendências em termos de segurança em dispositivos móveis? No transcorrer desta seção, analisaremos quais são as tendências desses riscos no futuro próximo.

Superando os limites da percepção

Antes do surgimento do Pokémon GO, nunca antes a realidade aumentada havia sido experimentada por tantas pessoas fora da comunidade de aficionados, colocando assim esta tecnologia na dianteira no que se refere às tendências para dispositivos móveis. Simultaneamente, **é cada vez mais comum ver pessoas usando dispositivos de realidade virtual** graças a projetos como o Google Cardboard, os quais serviram para divulgar o conceito junto ao público em geral e torná-lo mais acessível. O enorme sucesso dos aplicativos como o Pokémon GO se torna inevitavelmente atraente para os cibercriminosos que procuram injetar códigos maliciosos em futuros aplicativos de realidade aumentada, espalhando as suas criações através de servidores maliciosos, em sites comprometidos, lojas virtuais não oficiais e, inclusive, até mesmo oficiais.

No momento de produção deste artigo, foi possível ver o primeiro uso público do Father.IO: um aplicativo para dispositivos móveis que combina realidade aumentada e virtual em um jogo colaborativo de guerra, configurando-se aparentemente em um grande sucesso para o próximo ano. **Os usuários deverão ter muito cuidado para evitar malware que tentam se passar por aplicativos genuínos,** *software* de instalação ou manuais de usuário. Estas novas tecnologias combinadas com aplicativos de uso cotidiano apresentam riscos de segurança anteriormente não levados em conta, suplementarmente a outros perigos que mencionamos em nosso relatório Tendências 2016, tais como a propagação de malware e problemas de vulnerabilidade. À medida que a pessoa, enquanto entidade física, se transforma em uma variável do jogo, **não devemos tão somente nos preocupar com a proteção dos dados nos dispositivos, mas igualmente com a inte-**

Enquanto determinados aplicativos concentrem dados cada vez mais sensíveis, os malware ou software maliciosos voltados para dispositivos móveis estão se expandindo e se tornando cada vez mais complexos, elevando a importância do desenvolvimento seguro.

gridade do jogador. A sensatez – ou a sua falta – desempenhará um papel crucial na segurança física. Temos assistido a casos de pessoas que tentam capturar Pokémon enquanto dirigem, em áreas de propriedade privada, zonas altamente inseguras ou em condições de tamanho envolvimento e compenetração na realidade aumentada que se esquecem de observar se algum veículo se aproxima em cruzamentos.

A confluência de desconhecidos no mesmo lugar também representa riscos, por não sabermos a quem estamos nos expondo. Este aspecto pode ter sido uma das questões mais controversas em torno do surgimento do Pokémon GO, pois várias pessoas se feriram em discussões em ginásios Pokémon ou ao tentar iniciar batalhas com estranhos. Como se trata de *apps* que podem colocar em perigo a vida dos seus usuários, **conceber um modelo de segurança de modo inerente ao processo de desenvolvimento será um fator incontornável na criação de novos aplicativos.** Afinal, se não forem considerados os aspectos físicos da usabilidade, **o que se pode esperar em relação a falhas de segurança mais técnicas e talvez menos visíveis para os usuários e desenvolvedores?**

Aplicativos vulneráveis com API não tão seguras

Se existe algo que marcou o desenvolvimento de software até o momento, **isso seria o modo como considerações sobre a segurança são adiadas até as fases finais do projeto ou até mesmo deixadas absolutamente de lado.** Salvo alguns poucos aplicativos que devem cumprir e seguir padrões em termos de segurança, **poucos desenvolvedores se preocupam em realizar controles detalhados de *pentesting*** em seus produtos antes de disponibilizá-los ao público. À medida em que os dispositivos móveis se apresentam como construtores de relações humanas que ultrapassam o espaço digital, quer seja em jogos, na prática de esportes ou na busca por relacionamentos afetivos, **a segurança se torna um fator crítico** no processo de desenvolvimento para evitar projetos com falhas de segurança. Por exemplo, pesquisadores descobriram recentemente que o app Tinder fornecia – no momento da redação deste Artigo – a geolocalização exata da pessoa sempre que havia uma partida. Outro exemplo notável foi o caso da Nissan Leaf, quando se descobriu que seria possível ter acesso a alguns comandos não críticos do veículo através de vulnerabilidades na API fornecida pela empresa para desenvolvimentos em dispositivos móveis.

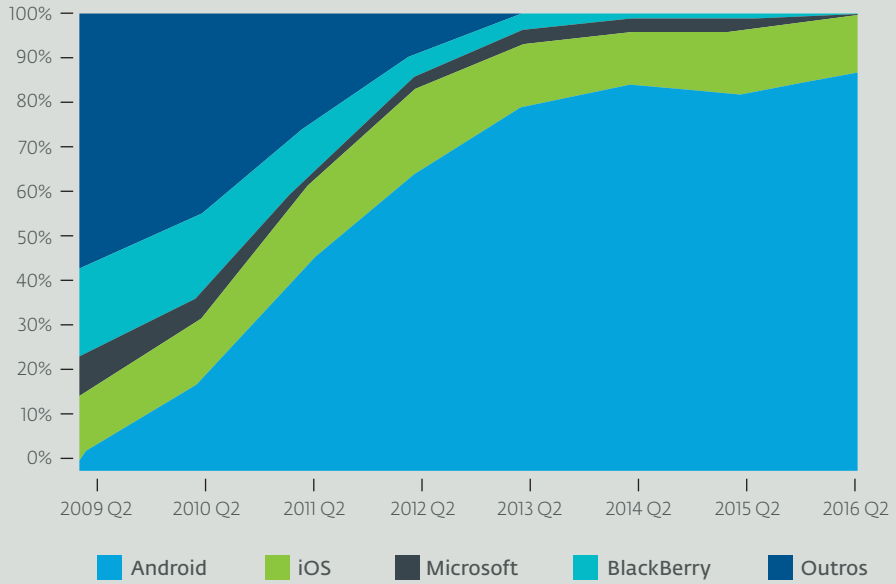
As bibliotecas de anúncios publicitários também desempenham um papel importante em matéria de segurança. Esses espaços são amplamente utilizados por desenvolvedores em plataformas nas quais os usuários normalmente não estão habitualmente dispostos a pagar para obterem a funcionalidade que as suas criações disponibilizam. Normalmente, encontramos pelo menos uma delas por aplicativo e muitas vezes contendo API inseguras que poderiam ser exploradas para se instalar um malware ou roubar informações. Além destes erros involuntários no processo de desenvolvimento, **há igualmente aquelas criações maliciosas cuja propagação é por vezes favorecida pelas políticas pouco restritivas** presentes em determinados repertórios de aplicativos, os quais involuntariamente abrigam cibercriminosos sob o manto da confiabilidade das lojas virtuais oficiais.

Android, um sistema inseguro?

Em 2007, **o surgimento do iOS revolucionou a indústria dos dispositivos móveis, forçando os consumidores a repensarem o papel dos dispositivos tecnológicos** no dia a dia. Naquele tempo, pouco se debatia acerca do papel da Segurança da Informação nas inovações tecnológicas e o seu eventual impacto na proteção de dados.

Se não forem considerados os aspectos físicos da usabilidade, o que se pode esperar em relação a falhas de segurança mais técnicas e talvez menos visíveis para os usuários e desenvolvedores?

Market Share dos diferentes OS



Fonte: Statista

A expansão do Android para outros dispositivos o converte em um potencial vetor para ataques em múltiplas plataformas.

Cerca de um ano após a apresentação do iOS, um novo sistema operacional apareceu como possível concorrente: **Android, desenvolvido pelo Google.** Com um sistema open source, um mercado de aplicativos menos restritivo, a possibilidade de se adaptar a diferentes marcas e com grande flexibilidade na personalização, o Android rapidamente aumentou a sua participação no mercado.

Até o final de 2009, os usuários de dispositivos móveis começaram a se dividir em campos antagônicos de acordo com a sua preferência por cada sistema, adotando um ou outro. Foi quando surgiram **os primeiros questionamentos sobre o eventual papel negativo destes recursos, tão apreciados no Android, no momento da abordagem da sua segurança.** Hoje, talvez estejamos vendo os resultados dessa aposta. Para o segundo trimestre de 2016, este sistema estava presente em 86,2% dos equipamentos em uso. **A abundância de usuários envolvidos o torna um alvo preferencial para ataques.** Sua expansão para outros dispositivos, tais como tablets inteligentes, televisores, *wearables* e automóveis, o converte em um vetor potencial para ataques em múltiplas plataformas, em um cenário complexo onde simultaneamente ganham vida novos sistemas de automação residencial. Existem várias causas que propiciariam ataques em múltiplas plataformas. Em primeiro lugar, a interconectividade entre dispositivos que permite a fácil propagação de ameaças e ataques por meio de técnicas de Engenharia Social. Além disso, componentes comuns em toda a estrutura do sistema operacional que podem permanecer sem a devida e contínua atualização pelos diferentes fabricantes. Finalmente, são cada vez mais comuns os frameworks de desenvolvimento que permitem exportar rapidamente executáveis para diferentes dispositivos e periféricos, os quais poderiam propagar as falhas de segurança nos diferentes terminais. **Na Internet das Coisas (IoT) não é difícil imaginar futuramente mais ataques desse tipo.**

Apps maliciosos em lojas oficiais

É corriqueiro ultimamente o **surgimento de aplicativos maliciosos nos repositórios oficiais do iOS e do Android,** uma tendência que em princípio seria aparentemente

extraordinária, mas, infelizmente, consolidou-se com o passar do tempo. Esta tendência envolveu até mesmo a App Store da Apple, teoricamente mais restritiva do que a Play Store do Android. Ao passo que no tocante à publicação de aplicativos, **existem numerosos fatores que favorecem a existência de códigos maliciosos na loja de aplicativos do Google.** Não somente o maior número de vítimas potenciais faz do Android um alvo favorito para os cibercriminosos, **mas igualmente a velocidade de publicação da Play Store** é outro agravante que contribui para torná-la um ambiente de predileção para a propagação de muitos ataques ameaçadores. Com o Android, qualquer desenvolvedor pode criar uma conta com **um único pagamento de 25 dólares, fazer o upload de um aplicativo e tê-lo publicado no prazo de 24 horas.** Em contrapartida, **no iOS o custo de adesão é superior a 99 dólares por ano e o período de espera até a publicação pode se estender por semanas.** Assim sendo, embora sejam realizados aperfeiçoamentos no Bouncer (módulo Google para análise automática e detecção de malware) e seja fortalecida a análise manual do código, a enorme quantidade de novos aplicativos criados diariamente e a rapidez com que são disponibilizados no mercado complicam a devida e minuciosa análise de cada um.

Podemos assim imaginar que, para futuramente reduzir os casos de software malicioso na sua *app store*, o **Google deverá modificar alguma dessas variáveis** – ou ambas – para assim dedicar mais recursos à análise intensiva de um número reduzido de aplicativos ou prolongar o período de análise, minando a velocidade de publicação. Uma das muitas estratégias que o Google pode utilizar para reduzir o número de aplicativos candidatos para publicação é **aumentar o valor da assinatura para desenvolvedores.** A verdade é que, apesar das políticas referentes à publicação na Play Store continuarem as mesmas e não haja implementação de qualquer destas ações corretivas, **podemos esperar uma maior quantidade de malware em lojas oficiais no ano de 2017,** à medida que realizadores de ataques consolidem este novo *modus operandi* e encontrem novos mecanismos para escapar da detecção.

Com relação a este último ponto, devemos dizer que **existem muitas técnicas que complicam a detecção de códigos maliciosos para dispositivos móveis:** bombas-relógio, código dinâmico executado através de reflexão, wrappers, criptografados, *strings* ofuscadas, scripts em outras linguagens de programação para a atuação remota do código malicioso, novas formas de C&C, anti-emulação, *rootkits*... Mas, acima de tudo, os cibercriminosos apostam e continuarão apostando na Engenharia Social, esperando atentamente o lançamento oficial de aplicativos populares para distribuírem versões falsificadas destes últimos, tal como aconteceu recentemente com o Pokémon GO, Prisma ou o Dubsmash. A rapidez com que estes aplicativos maliciosos conseguem obter centenas e até milhares de downloads é motivo de preocupação para os usuários destas plataformas. **O que aconteceria se os cibercriminosos decidissem massificar a complexidade das suas criações?** A diferença no nível de entendimento dos usuários do sistema acerca da instalação de aplicativos também desempenha papel contraproducente quando se trata de Android. **A facilidade com que alguém pode alterar um APK** obtido em uma loja oficial para nele inserir um código malicioso e depois propagá-lo através de sites ou mercados fraudulentos, **associada à facilidade com que os usuários instalam arquivos de fontes desconhecidas resultam em um índice maior de detecções** (e, na pior das hipóteses, na infecção), em comparação com outros sistemas para dispositivos móveis.

Apesar das políticas referentes à publicação na Play Store continuarem as mesmas, podemos esperar uma maior quantidade de malware em lojas oficiais no ano de 2017.

Facilidade de atualização

Ao longo dos anos, foram várias as investigações que se desdobraram em pareceres favoráveis à opinião, segundo a qual, a

característica Open Source do Android implicaria irremediavelmente em um maior número de vulnerabilidades e, consequentemente, em um aumento na frequência dos ataques. **No entanto, 2016 foi o primeiro ano em que o Android aparentemente terminaria com maior número de vulnerabilidades publicadas que o iOS.** No entanto, **a forma com que os patches de segurança são implantados continua deixando inseguros os usuários do Android,** criando uma grande janela de tempo entre o momento em que a vulnerabilidade é detectada e tempo de reação dos diferentes fabricantes e operadoras de telefonia, para a disponibilização de aperfeiçoamentos de segurança nas diferentes versões do sistema. Isso quando eles decidem fazê-lo...

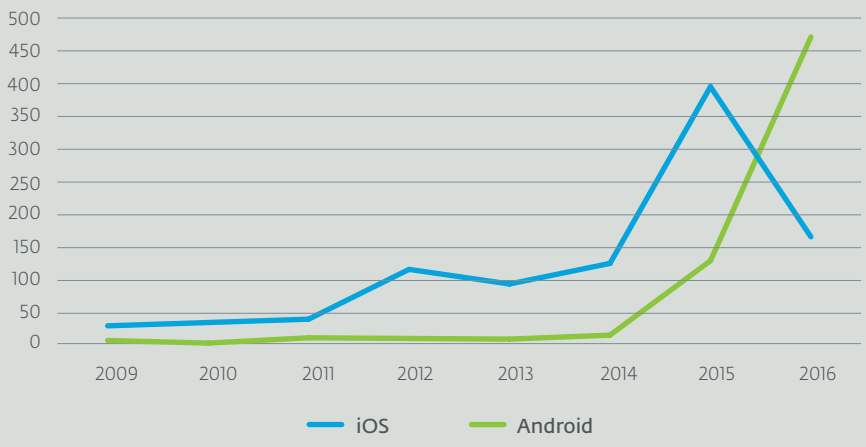
Para o restante de 2016 e no próximo ano, o plano de atualizações proposto pelo Google para o Android 7.0 Nougat em dispositivos Nexus inclui patches na forma de correções de segurança mensais, além de atualizações trimestrais de funcionalidade e correções de bugs. Entretanto, **obteve-se pouco progresso neste ano no sentido de se alcançar um consenso para a rápida liberação de *patches*.** Pelo contrário, as lutas de poder pelo controle do mercado de dispositivos móveis têm atrasado a resolução do conflito. Por sua parte, a Samsung, fabricante líder em dispositivos com Android, recusa-se a ceder o controle do SO dos seus equipamentos para o Google. Enquanto isso, o Google volta-se para fabricantes mais dóceis que concorram com a Samsung e levem-na a reduzir a sua participação no mercado. Existem alguns indicadores de que o Google tenha idealizado um novo plano para solucionar este problema. Até então, uma das opções que se apresenta para os usuários de dispositivos móveis com Android, preocupados em poder contar com os patches de segurança mais recentes, **consistiria em adquirir aparelhos Nexus,** rebatizados pelo Google com o nome Pixel por Google–, **para assim terem certeza de obter as atualizações o mais rapidamente possível e diretamente da fonte.**

A forma com que os patches de segurança são implantados continua deixando inseguros os usuários do Android.

Plataformas móveis sob ataque

Desde 2012, **o número de detecções de ameaças contra o universo dos dispositivos móveis continua crescendo e podemos projetar este crescimento para o próximo ano.** Trata-se de um reflexo estatístico que demonstra a grande importância atribuída pelos cibercriminosos a esses aparelhos que se tornam cada vez mais pes-

Quantidade anual de vulnerabilidades no Android e iOS desde 2009



Observação: As vulnerabilidades de 2016 foram contabilizadas até 14 de novembro.

Fonte: www.cvedetails.com

soais. Além das questões levantadas nesta seção, **é importante notar que os usuários da Apple não devem se deixar levar por uma falsa sensação de segurança.** De acordo com os dados dos nossos produtos, em termos mundiais, **as detecções para iOS ainda representam menos de 1% se comparadas às detecções para Android.** Entretanto, as detecções para este OS aumentam de modo exponencial: **no que se refere a 2016, até agora já foram detectadas mais de cinco vezes a quantidade de detecções para iOS correspondentes a todo o ano de 2015** e podemos esperar que esta maior exposição continue em 2017. Suplementarmente a este quadro, as vulnerabilidades graves permanecem à espreita. Recentemente, a Apple liberou patches de segurança para um conjunto de vulnerabilidades de "0-day" que possibilitavam aos cibercriminosos controlarem por completo o equipamento, com vistas à espionagem da vida privada.

O crescimento do malware para dispositivos móveis é uma realidade inegável, que previamos já há alguns anos e, atualmente, é algo que se consolida diante dos nossos olhos. **Durante o ano de 2015, o número de novas variantes de códigos maliciosos criados para Android foi de em média 200 variantes mensais; em 2016, este número aumentou para 300 novas variantes mensais (para iOS número é de 2 mensais).** Não é uma surpresa que este aumento continue ocorrendo durante o próximo ano, **com uma média de 400 novas variantes mensais de software maliciosos para dispositivos móveis com Android, até o final de 2017.** Isso nos dá uma noção não somente da quantidade de códigos maliciosos, mas igualmente da velocidade com que essas campanhas maliciosas evoluem. No próximo ano, veremos mais ransomware, mais aplicativos falsos, códigos maliciosos mais complexos e muito mais golpes voltados para dispositivos móveis, via WhatsApp e aplicativos de redes sociais. Enquanto, por sua vez, os usuários passam a entender o perigo ao qual estão submetidos ao instalarem aplicativos de fontes não confiáveis, os cibercriminosos apostam em novas campanhas de Engenharia Social, realizadas em mercados oficiais, e podemos esperar ver muitos mais desses casos no transcorrer dos próximos meses. Quais medidas tomarão o Google e a Apple para conter esta situação? Isso é o que deveremos notar durante o próximo ano. Acompanhando o aumento no volume de novas variantes de códigos maliciosos, **uma grande preocupação para os usuários de dispositivos móveis serão as vulnerabilidades não apenas do sistema operacional, mas igualmente dos aplicativos utilizados.** Como esses aplicativos concentram dados que podem colocar em perigo a integridade física dos seus membros, será um desafio para os seus criadores a pronta adoção de processos de desenvolvimento seguro para assegurar a minimização do risco de exposição, por exemplo, API incorretamente concebida.

Por enquanto, **os recentes lançamentos do** iOS 10 e do Android 7.0 Nougat **apresentam algumas notáveis melhorias no nível de proteção do dispositivo móvel,** especialmente no que se refere ao último sistema. Em relação ao Google, começamos a vislumbrar esforços para a unificação de alguns aspectos de segurança, por meio de diferentes modelos de celulares e tablets disponíveis no mercado. Além disso, a empresa continuará confiando no seu agressivo programa de *bug hunting* como meio de descobrir vulnerabilidades. Outra característica marcante do Android 7.0 Nougat consiste em ele ter introduzido vários aprimoramentos na manipulação de licenças e aplicativos que dificultarão a instalação de malware nos dispositivos e limitarão o controle exercido por estes aplicativos, em uma clara tentativa de se contrapor ao aumento dos ransomware para dispositivo móveis, um dos principais desafios existentes em termos de proteção e segurança de dispositivos deste gênero.

Durante o ano de 2016, o número de novas variantes de códigos maliciosos criados para Android foi de em média 300 mensais.

Em relação ao Google, começamos a vislumbrar esforços para a unificação de alguns aspectos de segurança.

Vulnerabilidades: os índices diminuíram, mas realmente estamos mais seguros?

- É reduzido o número de relatos, mas o risco diminui?
- Desenvolvimento seguro do software
- O protagonismo das múltiplas vulnerabilidades e o seu papel na conscientização
- Às vezes, um bom ataque é a melhor defesa
- Conclusão

AUTOR

Lucas Paus
Security Researcher

4

Vulnerabilidades: os índices diminuíram, mas realmente estamos mais seguros?

A globalização tecnológica e os múltiplos dispositivos, atualmente utilizados e interconectados de modo natural, aumentaram sensivelmente os vetores de ataque à disposição dos criminosos cibernéticos. Justamente por este motivo, a exploração de vulnerabilidades continua a ser uma das principais preocupações em relação a incidentes de segurança em empresas dos quatro cantos do planeta.

Atravessando as barreiras de segurança em diferentes plataformas, é possível para os criminosos encontrarem e explorarem falhas de programação que possibilitarão várias ações, incluindo desde o roubo de informações ou a propagação de malware sem a necessidade de intervenção por parte do usuário, até a queda do sistema ou a interrupção do serviço.

A este contexto de auge tecnológico e de vulnerabilidades, são incorporados novos desafios de segurança, referentes não tão somente à informação digital, mas ao acesso a infraestruturas críticas, automóveis inteligentes, IoT, indústrias 4.0 e até mesmo ao gerenciamento de cidades inteligentes. Enquanto as aplicações ou sistemas operacionais se concentram em ser mais funcionais e competitivos no mercado, **surge a necessidade de fortalecer a importância do desenvolvimento seguro,** em conjunto com a periodicidade de auditorias voltadas para a segurança.

Durante 2016, acompanhamos o estabelecimento de alianças estratégicas entre a Microsoft e a Canonical, com o objetivo de integrar ferramentas do Ubuntu (Linux) ao Windows 10, as quais poderiam se tornar um novo vetor de ataque em múltiplas plataformas, tais como o são, em muitos casos, as vulnerabilidades presentes no Java ou em navegadores da Web. **Serão esses novos cenários que elevarão a importância de se encontrar e de se mitigar de forma imediata as vulnerabilidades? Teria sido reduzido o número de vulnerabilidades encontradas? Como poderemos assegurar com maior certeza a segurança da informação, tanto ao nível privado quanto em âmbito corporativo?**

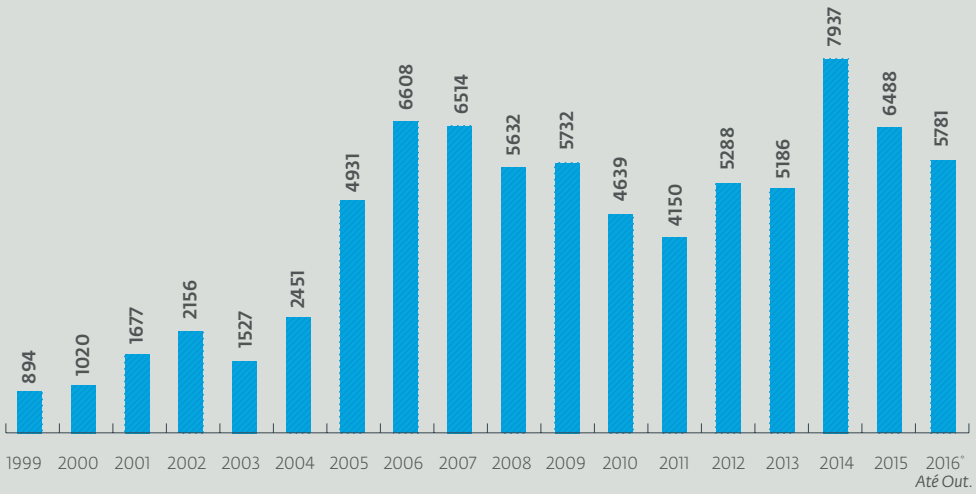
Ao longo desta seção, buscaremos responder a estas questões, além de observarmos o contexto futuro que nos espera, no tocante às vulnerabilidades.

É reduzido o número de relatos, mas o risco diminui?

Paradoxalmente, apesar do advento de novas tecnologias, **a quantidade total de todo tipo de vulnerabilidades, relatadas anualmente, tem diminuído nos últimos anos.** Deste modo, é possível observar que, apesar do número de novos vetores em ação, **a quantidade de CVE relatada está diminuindo nos últimos dois anos, após ter atingido uma alta histórica em 2014.**

De fato, **até o final do terceiro trimestre de 2014, haviam sido publicadas 5405**

FIG. 1 | Vulnerabilidades publicadas por ano



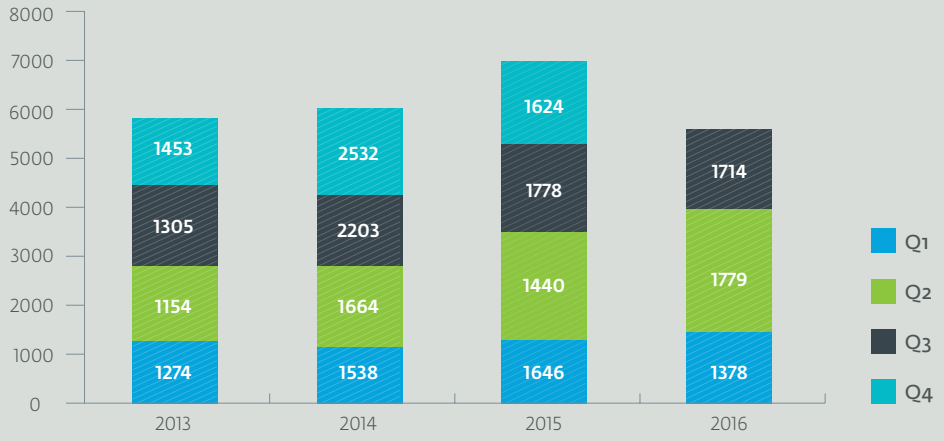
Fonte: National Vulnerability Database

vulnerabilidades, enquanto no mesmo período de 2015 o número caiu para 4864. (Fig 2). Agora que encerramos o terceiro trimestre de 2016 (momento em que se redige este artigo) o número alcança 5781, **(Fig 1),** quase a mesma quantidade que no ano passado.

Isto significa que há um aumento brusco no número total de vulnerabilidades publicadas. Seguindo essa lógica e devido ao fato de o desenvolvimento seguro continuar a ganhar terreno, em 2017 não se espera um aumento abrupto na quantidade de vulnerabilidades reportadas. Contudo, para além do otimismo que possa gerar essa redução na quantidade de vulnerabilidades publicadas, esse dado ganha outro significado quando se observa quantas dessas vulnerabilidades são considerados "críticas", **(Fig 3)**, isto é, aquelas que têm impacto maior na segurança do usuário.

Ao final do terceiro trimestre de 2016, a quantidade de vulnerabilidades críticas relatadas corresponde a 40% do total, uma proporção maior do que foi observado em todos os anos anteriores.

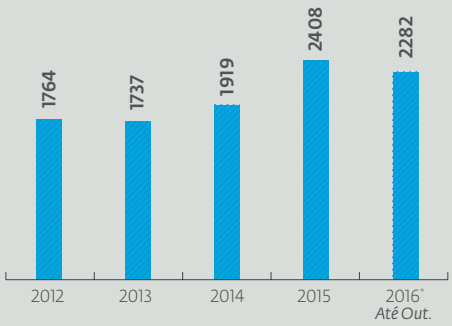
FIG. 2 | Vulnerabilidades publicadas por trimestre



Fonte: National Vulnerability Database

Paradoxalmente, apesar do advento de novas tecnologias, a quantidade total de todo tipo de vulnerabilidades, relatadas anualmente, tem diminuído nos últimos anos.

FIG. 3 | Número de vulnerabilidades críticas relatadas por ano



Fonte: National Vulnerability Database

Por conseguinte, a redução global no número de falhas reportadas não é sinal de tranquilidade, pois os relatos de vulnerabilidades críticas nos últimos anos apresentaram crescimento. Entretanto, para além das quantidades de vulnerabilidades encontradas, não se pode deixar à parte o fato de a sua exploração não ser diretamente proporcional à quantidade de CVE reportadas. **O risco de uma vulnerabilidade ser explorada está ligado a várias questões, tais como o uso massivo do aplicativo ou do protocolo vulnerável, a dificuldade da sua exploração e a criticidade das informações armazenadas.**

Por exemplo, a CVE-2016-2060 é uma vulnerabilidade crítica que afeta **milhões de dispositivos com Android,** permitindo que determinados aplicativos obtenham privilégios e possam acessar informações privativas do usuário.

Quanto aos protocolos, no caso do OpenSSL, encontramos a DROWN, uma vulnerabilidade crítica publicada em 2016 e cujo impacto estimado pode chegar a afetar a **25% dos domínios mais visitados na Internet** e até mesmo um terço de todos os servidores da Web. Isto mostra nitidamente como duas CVE podem ter grande impacto, afetando desde usuários domésticos até empresas.

Desenvolvimento seguro do software

Quando vemos a redução no número de vulnerabilidades relatadas, parte deste êxito pode ser associado aos novos paradigmas em matéria de desenvolvimento de sistemas. Um dos grandes desafios colocados anualmente a partir da segurança em informática é o modo de segurança que se aplica em novos projetos.

Anteriormente, vimos com frequência a atribuição de prioridade à inovação, em detrimento da segurança da informação. Impulsionados ou constrangidos pela exigência constante de novidades no mercado de tecnologia, o fato de relegar a segundo plano a segurança da informação nos desenvolvimentos é uma prática de risco, não somente do ponto de vista da proteção de dados, mas igualmente no que tange à continuidade do negócio, pois **um incidente de larga escala poderia ter enorme impacto na imagem corporativa.**

Contudo, este é um paradigma que se está tentando mudar e **a nova tendência nos leva a crer que, gradualmente, os desenvolvedores estarão cada vez mais sendo acompanhados de especialistas em segurança e em criptografia, desde as fases iniciais.** Assim sendo, na medida em que continuem evoluindo essas boas práticas no ciclo de vida do software (SDLF -Systems Development Life Cycle), podemos esperar que a quantidade de CVE não apresente grande aumento, o que reduzirá a possibilidade de exploração de vulnerabilidades nos diferentes sistemas desenvolvidos.

Todos estes aperfeiçoamentos no SDLF tornam-se ainda mais necessários se considerarmos cenários já conhecidos e que têm crescido nos últimos anos, tais como o número de aplicativos e serviços baseados nas nuvens ou a sua futura migração, o isomorfismo, os aplicativos de Big Data ou as interfaces de Desenvolvimento de Aplicativos (API). Todas

A redução global no número de falhas reportadas não é sinal de tranquilidade, pois os relatos de vulnerabilidades críticas nos últimos anos apresentaram crescimento.

elas devem contar com as devidas validações de entrada e garantir codificações de saída, mediante a adoção de práticas criptográficas, além de tratamento adequado de logs, memória, erros e arquivos.

Para consolidar a melhoria ao longo de todo ciclo, **o desafio para 2017 estará voltado para o aperfeiçoamento da gestão das vulnerabilidades encontradas.** Assim sendo, tanto para os fabricantes e desenvolvedores quanto para os usuários, o desafio não residirá tão somente em se tomar medidas de controle para evitar a exploração das vulnerabilidades, mas igualmente em se realizar um relatório e um gerenciamento satisfatórios das mesmas.

Desta forma, prevê-se que a implantação de um ciclo de desenvolvimento seguro, a partir da consolidação de um padrão de projeto voltado para a segurança, começará a gerar sinergias entre as áreas de segurança e de desenvolvimento, **a qual nos aproximará da criação de sistemas mais robustos, eficientes e rentáveis.**

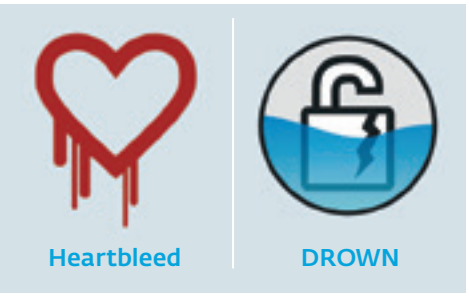
O protagonismo das múltiplas vulnerabilidades e o seu papel na conscientização

Por parte dos usuários, **ultimamente, algumas das vulnerabilidades críticas não passaram despercebidas.** Por mais de três décadas, as empresas de antivírus e pesquisadores em segurança foram designando com nomes vários códigos maliciosos que tiveram grande impacto. Podemos destacar como exemplos os antigos worms Morris ou Sasser, o vírus Melissa e alguns mais atuais, como os ransomware CTB-Locker e Locky.

Este tipo de prática deu um passo adiante **e desde 2014 começou-se igualmente a batizar algumas vulnerabilidades críticas.** Um exemplo claro foi a CVE-2014-0160, muito mais conhecida como Heartbleed, uma vulnerabilidade infame que não somente ganhou nome, mas também um logotipo.

Naturalmente, **os nomes procuram gerar uma caracterização das ameaças, tentando estabelecer-lhes um ponto de referência ou a compreensão acerca do seu funcionamento. Além disso, em termos de sensibilização junto aos vários departamentos de TI, este tipo de batismo de vulnerabilidades é mais eficaz quando busca, a partir da identificação da referida vulnerabilidade, levar à adoção das medidas necessárias para mitigá-la.**

Durante 2015, destacaram-se nomes como FREAK (CVE-2015-0204) e Logjam (CVE-2015-4000) e, em 2016, deparamo-nos com o Badlock (CVE-2016-2118), afetando o Samba, HTTPoxy (CVE-2016-5387), ainda que tenha sido detectada pela primeira vez há 15 anos, e DROWN, que afetou a protocolos TLS/SSL. Com certeza, no próximo ano continuará este "batismo" de vulnerabilidades **e espera-se que, para além dos efeitos de marketing e promoção, as referidas denominações consigam aumentar os esforços em termos de sensibilização e conscientização dos usuários,** a fim de que sejam tomadas as medidas necessárias para mitigar o impacto que essas vulnerabilidades possam ter em seus sistemas.



Às vezes, um bom ataque é a melhor defesa

A questão da vulnerabilidade tem sido igualmente uma preocupação para os principais serviços e empresas do mundo

Tanto para os fabricantes e desenvolvedores quanto para os usuários, o desafio não residirá tão somente em se tomar medidas de controle para evitar a exploração das vulnerabilidades, mas igualmente em se realizar um relatório e um gerenciamento satisfatórios das mesmas.

da tecnologia. **Anos atrás, as empresas haviam assumido uma postura bem ofensiva com respeito à gestão de segurança e de vulnerabilidades,** principalmente, gerando políticas e controles para lhe dar respaldo.

Recentemente, eles foram benéficos em várias auditorias ou testes de penetração que ganharam muito espaço, principalmente em ambientes corporativos onde, com frequência, devem ser periodicamente realizados com base em normas regulamentares e em medidas de sensibilização e conscientização.

Entretanto, grandes empresas e órgãos governamentais estão se apoiando em uma tendência que se aproxima do que poderia ser um verdadeiro ataque. **Ela envolve basicamente a contratação de especialistas em segurança privados, visando a realização de testes de penetração com remuneração em função dos resultados,** o que tem sido denominado **Vulnerability Reward Program ou Bug Bounty Program.** Empresas líderes como Facebook, Google ou Yahoo!, entre muitas outras, já formalizaram com muita ênfase esse tipo de atividade, em que estão acompanhadas por outras entidades, tais como o Departamento de Defesa dos Estados Unidos.

Para desenvolvedores de aplicativos e fabricantes de dispositivos IoT, **tais programas podem trazer-lhes melhorias em seus produtos mais rapidamente,** tendo em vista que, normalmente, os testes são realizados por um número maior de pesquisadores, as vulnerabilidades são relatadas imediatamente e, como os tempos em que os testes são realizados podem ser significativamente mais extensos, explorações mais profundas podem ocorrer. Assim sendo, tanto essas causas como outras, relacionados ao orçamento e à motivação dos especialistas envolvidos, continuarão futuramente reforçando esta tendência.

Conclusão

Atualmente, mais preocupados com incidentes de segurança, tais como vazamento de informações ou acesso indevido a dados sensíveis, as empresas **não melhoraram substancialmente as suas práticas de gestão da segurança.** Por conseguinte, **os principais desafios para o mundo corporativo em 2017 estão associados ao foco na concentração de esforços na gestão da tecnologia,** complementando-o com uma necessária conscientização dos seus colaboradores acerca destes riscos, além da capacidade de poderem cumprir as normas impostas pelas autoridades regulamentadoras do negócio.

A tudo isto acrescenta-se a necessidade de aprofundar a cultura de resiliência, deixando os especialistas em segurança com o principal papel para intervirem como facilitadores nas áreas de TI, na correção de erros de código e na mitigação de impactos. Assim, **a gestão deve ter foco na implementação adequada das políticas de segurança e em planos que possibilitem a continuidade do negócio,** incluindo uma comunicação adequada dos incidentes para manter os usuários informados.

Por parte dos desenvolvedores, espera-se que continuem sustentando o paradigma do desenvolvimento seguro e, a partir de uma maior conscientização dos usuários acerca dos riscos das vulnerabilidades, não causaria espanto se houvesse um aumento na demanda por uma melhor proteção dos dados pessoais que as empresas manipulam. Se isso acontecer, o desenvolvimento seguro poderá ser um diferencial competitivo na indústria de tecnologia e, no futuro, se tornaria um incentivo para os desenvolvedores.

Além disso, novos códigos maliciosos começaram a se valer das vulnerabilidades para se propagar, pois uma vítima despro-

A questão da vulnerabilidade tem sido igualmente uma preocupação para os principais serviços e empresas do mundo da tecnologia.

tegida, simplesmente ao acessar um link, pode ver como a informação dos seus dispositivos é criptografada, tal como acontece com algumas variantes do ransomware CryptoWall 3.0. De modo semelhante, **os exploit kit continuarão sendo utilizados mais frequentemente na propagação de malware e, inclusive, em ataques ainda mais direcionados, tais como os APT** que invadem sites violados ou são especialmente gerados com tal finalidade.

Com muita frequência, as vulnerabilidades de software são difíceis de se prever, por conseguinte, reduzir os seus riscos é fundamental para se levar adiante planos de conscientização sobre boas práticas e a sua boa gestão. O uso dos famosos o-days ainda deixa expostos os sistemas, todavia, a indústria de antivírus também percebeu essa tendência e, por essa razão, existem soluções em segurança com heurística avançada, as quais possuem tecnologia capaz de detectar tais ações e bloqueá-las.

Desta forma, tanto as soluções de segurança, quanto o gerenciamento de atualizações e de vulnerabilidades continuarão a ganhar destaque na mitigação deste tipo de problema, visando minimizar ou eliminar as brechas para exposição ou vazamento de informações no transcorrer dos próximos anos.

Os principais desafios para o mundo corporativo em 2017 estão associados ao foco na concentração de esforços na gestão da tecnologia, complementando-o com uma necessária conscientização dos seus colaboradores.

Software de segurança “next-gen”: mitos e marketing

- A era dos dinossauros
- A teoria da evolução
- A seleção natural e não natural
- Avaliação do produto completo
- No cenozoico

AUTOR

David Harley
Senior Research Fellow

5

Software de segurança "next-gen": mitos e marketing

A era dos dinossauros

Há uma concepção do atual mercado da segurança informática que ultimamente está aparecendo com muita frequência nos meios de comunicação. Existem dois tipos diferentes de tecnologia de detecção de malware: uma de **"primeira geração" ou "tradicional"** (às vezes, inclusive, a chamam de tecnologia "fóssil" ou "da época dos dinossauros"), **que segundo dizem, é baseada invariavelmente na detecção da "seguinte ou último geração" (next-gen),** que utilizam métodos de detecção sem assinaturas. **Com certeza, esta concepção se vê muito mais favorecida pelas empresas que comercializam "soluções next-gen"; no entanto, não reflete a realidade.**

A teoria da evolução

Em primeiro lugar, quero discordar com o termo "primeira geração". Um pacote moderno de segurança não pode mais ser agregado às primeiras tecnologias de "camada única", como os scanners de assinaturas estáticas, a detecção de mudanças e as vacinas. Seria como considerar que o Microsoft Word está no mesmo grupo do *ed* ou do *edlin.* Apesar de terem uma finalidade fundamental em comum com essas aplicações já obsoletas (como a detecção e/ou o bloqueio de softwares mal-intencionados ou a criação e o processamento de textos), essas novas tecnologias têm uma gama muito maior de funcionalidades. Um processador de texto moderno incorpora elementos que eram considerados puramente domínios de editoração eletrônica, planilhas e bancos de dados há algumas décadas.

A origem do ilusório

Um pacote de segurança antimalware moderno não é tão abrangente nos elementos de programação que incorpora. No entanto, ele inclui camadas de proteção genérica que vão muito além das assinaturas (até mesmo as genéricas). Houve uma evolução nas diferentes gerações dos produtos, absorvendo tecnologias que não existiam quando os primeiros mecanismos de segurança foram lançados.

Descrever os recém-chegados ao mercado como se apenas eles fossem a next-gen, indo além da tecnologia primitiva e específica das assinaturas, é algo errôneo e enganoso.

Assinaturas? Que assinaturas?

Hoje em dia, mesmo os modernos scanners comerciais antimalware de camada única **vão muito além da procura de amostras específicas e assinaturas estáticas simples.** A detecção de famílias específicas conhecidas de hash do malware foi ampliada com a inclusão de elementos de whitelisting, análise comportamental, bloqueio de comportamentos e detecção de mudanças (por exemplo), que já foram consideradas tecnologias puramente "genéricas".

Não que eu recomende, em geral, que as pessoas devam confiar totalmente em um scanner de camada única, como aqueles que muitas vezes são oferecidos de graça por empresas tradicionais. **Elas também deveriam usar outras "camadas"** de proteção, seja por meio de um pacote de segurança de nível comercial ou ao replicar as funcionalidades das múltiplas camadas de um pacote durante a utilização de componentes extraídos a partir de diversas

Descrever os recém-chegados ao mercado como se apenas eles fossem a next-gen, indo além da tecnologia primitiva e específica das assinaturas, é algo errôneo e enganoso.

fontes, incluindo um scanner antimalware de camada única. No entanto, a última abordagem requer um nível de compreensão das ameaças e dasde tecnologias de ameaças e de segurança que a maioria dos indivíduos não tem. Nesse ponto, nem todas as organizações têm acesso a um profissional com esse tipo de experiência, o que as deixa à possível mercê do marketing disfarçado de assessoria técnica.

Um retorno ao básico

Embora alguns produtos "next-gen" mantenham o funcionamento real de sua tecnologia a sete chaves, disponibilizando produtos antimalware atuais que parecem ter código aberto, **fica claro que as distinções entre os produtos fossilizados e os itens da "next-gen" são muitas vezes uma questão de nomenclatura, não de tecnologia.** Eu não acredito que os elementos da "next-gen" tenham evoluído muito além dessas abordagens básicas para acabar com malware, definidas há muito tempo por Fred Cohen (cuja introducción y definición do termo "vírus de computador" alavancaram a indústria antimalware em 1984), em comparação com as soluções "tradicionais":

- A identificação e o bloqueio de comportamentos mal-intencionados.
- A detecção de mudanças inesperadas e inadequadas.
- A detecção de padrões que indicam a presença de malware conhecidos ou desconhecidos.

Naturalmente, as formas de implementar essas abordagens vêm avançando muitíssimo, mas esse progresso não é uma propriedade exclusiva dos produtos recém-lançados. O que geralmente vemos descrito como indicadores de compromisso, por exemplo, também poderia ser descrito como assinaturas (bem fracas). Mais de um fornecedor não foi capaz de diferenciar de forma convincente o uso de antimalware tradicionais na análise do comportamento e do bloqueio, entre a sua própria utilização de (por exemplo) análise/monitoramento/bloqueio de comportamento, análise de tráfego (e assim por diante), e o uso das mesmas tecnologias por antimalware de grandes empresas. Em vez disso, **eles optaram por promover uma visão ilusória de tecnologia fóssil e impregnaram suas campanhas de marketing com uma imensidão de palavras tecnológicas de efeito.**

Bem-vindos à máquina

Considere, por exemplo, os repetidos elogios feitos para a "análise comportamental" e para a ML (aprendizagem automática) "pura" como tecnologias que separam a próxima geração da primeira. No mundo real, a aprendizagem automática não é exclusiva de um setor do mercado. O progresso em áreas como as redes neurais e o processamento paralelo são tão úteis na segurança atual quanto em outras áreas da computação. Por exemplo: sem algum grau de automação no processo de classificação de amostras, não poderíamos nem mesmo começar a lidar com a avalanche diária de milhares de amostras de ameaças que devem ser examinadas para gerar uma detecção precisa.

No entanto, o uso de termos como ML pura na estratégia de marketing da Next Gen é retórico, não tecnológico. **Isso significa não apenas que a ML de alguma forma fornece sozinha uma detecção melhor que qualquer outra tecnologia, mas também que ela é eficaz a ponto de não haver a necessidade de supervisão humana.**

De fato, **apesar das abordagens de ML serem muito bem conhecidas e utilizadas na indústria de antimalware tradicionais, elas têm seus prós e contras como qualquer outra abordagem.** Algo igualmente **importante é que os criadores de malware muitas vezes têm tanta consciência sobre a ML quanto os fornecedores**

Fica claro que as distinções entre os produtos fossilizados e os itens da "next-gen" são muitas vezes uma questão de nomenclatura, não de tecnologia.

de segurança que detectam malware e dedicam muito tempo para encontrar maneiras de contorná-los, como é o caso de outras tecnologias antimalware.

A análise do comportamento

Da mesma forma, **quando os fabricantes dos produtos da "next-gen" falam sobre a análise comportamental como sua descoberta exclusiva, eles talvez estejam mal-informados.** O termo "análise comportamental" e as tecnologias que utilizam essa abordagem foram usados em antimalware tradicionais por décadas. **Na verdade, praticamente todo o método de detecção que vai além das assinaturas estáticas pode ser definido como uma análise comportamental.**

A seleção natural e não natural

O jornalista Kevin Townsend me perguntou recentemente:

> *Existe alguma maneira da indústria poder ajudar o usuário a comparar e escolher entre a primeira [...] e a segunda geração [...] para a detecção de software malicioso?*

Deixando de lado a classificação totalmente equivocada de primeira e segunda geração, sim, é claro que há. Na verdade, algumas das empresas que se intitulam como de segunda geração e afirmam que sua tecnologia é muito avançada para a realização de testes **acabaram abrindo ainda mais essa possibilidade em suas próprias tentativas de comparar a eficácia de seus produtos com a dos fornecedores da primeira geração.** Por exemplo: pelo menos um fornecedor da "next-gen" passou a usar amostras de malware em suas próprias demonstrações públicas. Se diferentes gerações de produtos não podem ser comparadas em um ambiente independente de testes, como essas demonstrações poderiam garantir a precisão em um exercício de relações públicas?

Outro argumento enganoso de marketing dos fornecedores de produtos "next-gen" é afirmar que "os produtos da primeira geração não detectam malware sem arquivos na memória" (algo que fazemos há décadas). Um exemplo bastante equivocado usou uma pesquisa mal desenvolvida com base em solicitações pela liberdade de informação para "comprovar" o "lamentável fracasso" dos antimalware tradicionais sem tentar fazer uma distinção entre os ataques e os ataques bem-sucedidos.

Testes e pseudotestes

É muito comum que o VirusTotal (VT) seja mal utilizado, deturpando os relatórios como se ele e os serviços similares fossem adequados para o uso como um "mecanismo múltiplo para serviços de testes de AV", o que não é o caso. Nas palavras do próprio VT

> *O VirusTotal não deve ser usado para gerar métricas comparativas entre diferentes produtos de antivírus. Os mecanismos de antivírus podem ser ferramentas sofisticadas que têm características adicionais de detecção que, por sua vez, podem não funcionar dentro do ambiente de verificação do VirusTotal. Sendo assim, os resultados da verificação do VT não servem para serem utilizados para a comparação da eficácia dos produtos antivírus.*

Podemos dizer que o VT é usado para "testar" um **arquivo** expondo-o a um lote de mecanismos de detecção de malware. No entanto, ele não usa toda a gama de tecnologias de detecção incorporadas a esses produtos e, assim, não testa nem determina a eficácia do **produto** com precisão.

Um fornecedor de itens da "next-gen" mencionou ter sido capaz de detectar uma amostra específica de ransomware um mês antes dela ser submetida ao VirusTotal. No entanto, pelo menos um fabricante grande/tradicional já havia detectado o mesmo hash um mês antes do anúncio da detecção pelo representante da "next-gen". É simples-

No entanto, o uso de termos como ML pura na estratégia de marketing da Next Gen é retórico, não tecnológico.

mente impossível medir a eficácia de um produto a partir de relatórios do VirusTotal, porque o VT não é um testador e os seus relatórios refletem apenas uma parte das funcionalidades dos produtos que ele utiliza.

Do contrário, não haveria a necessidade de entidades avaliadoras de renome como a Virus Bulletin, a SE Labs, a AV-Comparatives ea AV-Test, que dedicam muito esforço para realizarem seus testes com a maior precisão e abrangência possíveis.

Rumo à cooperação

Uma das reviravoltas mais drásticas de 2016 ocorreu quando o VirusTotal alterou os seus termos de compromisso dificultando que as empresas **da "next-gen" pudessem se beneficiar do acesso a amostras submetidas por empresas da 1ª geração ao VirusTotal sem precisarem contribuir com o VT.** Como o blog do VirusTotal publicou:

> ***... agora, todas as empresas de verificação serão obrigadas a integrarem o seu verificador de detecção à interface pública do VT a fim de serem elegíveis para receberem os resultados de antivírus como parte dos serviços da API do VirusTotal.*** *Além disso, os novos verificadores que venham a ser integrados à comunidade terão que comprovar a certificação e/ou as análises independentes de testadores de segurança de acordo com as melhores práticas da AntiMalware Testing Standards Organization (AMTSO).*

Enquanto muitos fornecedores da "next-gen" responderam inicialmente com frases como *"Não é justo"*, *"Os dinossauros estão querendo acabar conosco"* e *"Como não usamos assinaturas, não precisamos do VT e não estamos nem aí"*, parece que vários grandes nomes se prepararam depois para atender a essas exigências, juntando-se à AMTSO e ficando disponíveis para a realização de testes independentes (e, aliás, testes reais, não pseudotestes com o VirusTotal). Como os fornecedores da "next-gen" já demonstraram uma tendência de declarar que seus produtos não poderiam ser testados, principalmente por grupos "tendenciosos" representados pela AMTSO, isso pode indicar a possibilidade empolgante de que **não são todos os clientes que confiam somente no marketing ao tomarem decisões de compra.**

Compartilhamento e compartilhamento semelhante

Por que os fornecedores da "next-gen" decidiram agora que realmente precisam trabalhar com o VirusTotal? **Bem, o VT compartilha as amostras recebidas com os fornecedores e fornece uma API que pode ser usada para verificar os arquivos de forma automática em todos os mecanismos utilizados por ele.** Isso possibilita não apenas que os fornecedores acessem um conjunto de amostras compartilhadas por fornecedores tradicionais, **mas também que possam compará-las com amostras indeterminadas e com as suas próprias detecções, treinando os seus algoritmos de aprendizagem de máquina** (se for o caso).

Por que não? Isso não é muito diferente da maneira como os fornecedores estabelecidos há mais tempo usam o VirusTotal. A diferença reside no fato de que, **sob os termos atualizados de compromisso, há um benefício triplo.** Os fornecedores (de qualquer geração) se beneficiam do acesso aos recursos do VirusTotal e daquela enorme biblioteca de amostras. **O VirusTotal se beneficia por agregar as informações,** assim como por seu papel de fornecer serviços premium. **E o resto do mundo se beneficia com a existência de um serviço gratuito que possibilita a verificação de arquivos individuais suspeitos** em uma vasta gama de produtos.

A ampliação desse leque de produtos com a inclusão de tecnologias menos tradicionais deve melhorar a precisão do serviço. Ao mesmo tempo, os participantes mais novos talvez sejam mais cautelosos em não

É simplesmente impossível medir a eficácia de um produto a partir de relatórios do VirusTotal.

abusarem dos relatórios do VT para pseudo-testes e marketing, já que eles mesmos estarão expostos a esse tipo de manipulação.

Avaliação do produto completo

A maneira como os avaliadores alinhados com a AMTSO passaram a realizar "testes do produto completo" nos últimos anos é exatamente a direção que devem tomar para avaliar esses produtos menos "tradicionais" de forma justa (ou pelo menos com o mesmo equilíbrio dedicado aos grandes produtos). É possível argumentar, porém, que os avaliadores podem ser conservadores na metodologia usada. Até pouco tempo atrás, a realização de testes estáticos era a regra de ouro (e, até certo ponto, isso ainda ocorre entre os testadores não alinhados com a AMTSO, que tem desmotivado essa prática desde o início da organização). Apesar de todos os seus defeitos, a AMTSO é maior (e mais desinteressada) que a soma de suas partes porque inclui uma gama de pesquisadores dos fornecedores e das organizações de testes, e as equipes de marketing não são bem representadas. Assim, **as empresas individuais de ambos os lados da divisão são menos capazes de exercer uma influência indevida sobre a organização como um todo em busca de seus próprios interesses. Se as empresas da "next-gen" aceitarem os termos e se envolverem com essa cultura, todos serão beneficiados.** No passado, a AMTSO já sofreu devido à presença de organizações com intenções excessivamente focadas na manipulação ou em coisas piores. Porém, **um melhor equilíbrio entre fornecedores e avaliadores "antigos e novos" dentro da organização apresenta boas possibilidades de sobreviver a qualquer tipo de atividade duvidosa deste estilo.**

No cenozoico

Há vários anos, concluí um artigo para o Virus Bulletin com estas palavras:

> *Podemos imaginar um mundo sem AV, uma vez que, aparentemente, os últimos rituais já estão sendo lidos? As mesmas empresas que não dão o devido crédito ao AV no momento enquanto pegam carona em suas pesquisas serão capazes de igualar a experiência das pessoas que trabalham nos laboratórios de antimalware?*

Acredito que talvez já tenhamos uma resposta. Porém, **se a autodenominada "next-gen" aceita suas próprias limitações, modera seus métodos agressivos de marketing e aprende sobre os benefícios da cooperação entre empresas com diferentes forças e capacidades, todos ainda poderemos usufruir dos benefícios dessa trégua.**

Não são todos os clientes que confiam somente no marketing ao tomarem decisões de compra.

Apesar de todos os seus defeitos, a AMTSO é maior (e mais desinteressada) que a soma de suas partes.

A IoT e o ransomware no setor da saúde: a ponta do iceberg

- Ransomware, a ponta do iceberg
- Dispositivos médicos e de condicionamento físico
- A proteção dos dispositivos médicos

AUTOR

Lysa Myers
Security Researcher

6

A IoT e o ransomware no setor da saúde: a ponta do iceberg

No ano passado, os vazamentos de dados da Anthem e da Premera fizeram com que o público em geral ficasse mais consciente sobre a importância da segurança nas organizações de saúde.

Em 2016, o número de casos de ataques de cibercriminosos no setor da saúde foi menor mas, infelizmente, isso não significa que o problema tenha sido resolvido. Na verdade, houve um aumento no número de ataques bem-sucedidos do tipo ransomware em vários setores este ano, **e instalações médicas são alvos bastante atraentes para esse tipo de ameaça.** Junto com o aumento do número de dispositivos médicos e rastreadores de condicionamento físico conectados à internet, **isso indica que o setor da saúde continuará enfrentando grandes desafios no futuro.**

Ransomware, a ponta do iceberg

Alguns encaram a onda crescente de ataques ransomware como um problema único. **Porém, apesar de causar dores de cabeça e prejuízos enormes, o êxito desse tipo de ataque é o sintoma de uma complicação ainda maior.**

Em geral, as ameaças do tipo ransomware podem ser evitadas seguindo práticas mínimas de segurança nos endpoints e na rede. **De fato, logo após a descoberta das primeiras ocorrências de ransomware, os especialistas em segurança acharam que esse problema não seria nem tão grave nem muito difícil de resolver,** mesmo se o malware não fosse detectado antes de sua execução. Nesses casos, **basta a vítima realizar uma restauração dos backups** e contornar os pedidos de resgate. O único porém é que, no mundo real, **as medidas de segurança** e proteção muitas vezes não são implementadas da maneira esperada pela comunidade de segurança. Em princípio, pode parecer mais caro restaurar os dados a partir de backups do que ceder ao pedido de resgate. Por vezes, **algumas empresas nem mesmo realizam backups frequentes**. É possível que os produtos de segurança desenvolvidos para detectar emails, arquivos, links ou tráfego mal-intencionados **sejam configurados da forma errada ou nem sequer existam.** Talvez as estratégias de backup não sejam implementadas da maneira correta, o que também deixaria os backups vulneráveis a ataques de ransomware ou a outros riscos. Os usuários podem desativar ou evitar o uso dos produtos de segurança quando acreditarem que essas medidas dificultam a realização de seu trabalho. **Seja qual for o motivo, talvez as empresas afetadas achem necessário pagar aos criminosos para reaverem seus dados.**

No setor da saúde, em que o acesso rápido às informações pode representar a diferença entre a vida e a morte, os custos de um ataque de ransomware são bastante ampliados. Os criminosos estão cientes disso e atacam as organizações médicas de propósito. Algumas medidas simples e eficazes serão necessárias para reverter essa tendência. Porém, ao estabelecer uma base sólida de segurança, talvez possamos diminuir os efeitos de futuras ameaças de malware e os riscos representados pelas novas tecnologias.

Em 2016, o número de casos de ataques de cibercriminosos no setor da saúde foi menor mas, infelizmente, isso não significa que o problema tenha sido resolvido.

A importância da avaliação e remediação dos riscos

No WeLiveSecurity, nós abordamos a importância da avaliação dos riscos no setor da saúde. **Ao manter uma classificação atualizada de ativos e métodos de transmissão, conseguimos identificar possíveis vulnerabilidades e riscos.** Quando a probabilidade e os custos potenciais desses riscos são levados em consideração, vemos com mais clareza o que deve ser priorizado.

No caso dos ransomware, a avaliação de riscos pode ajudar a resolver a situação de várias maneiras:

→ Quais ativos estão sujeitos a serem criptografados por um ransomware?
→ Que métodos de transmissão podem permitir a entrada de ransomware na sua rede?
→ Quais modalidades possibilitam que a ameaça receba comandos para criptografar os seus arquivos?
→ Qual é a probabilidade de você ser atingido por essa ameaça?
→ Qual é o volume de prejuízo financeiro que poderia ser causado por um ataque que desse certo?

Infelizmente, os ativos que correm o risco de sofrerem ataques de criptografia são praticamente todos os dados ou sistemas acessíveis pela sua rede ou pela internet. Muitas vezes, os ataques de ransomware começam por emails de phishing que contêm malware ou links para baixar arquivos mal-intencionados. Então, nesse caso, consideraríamos que o método de transmissão foi o email, com um foco na Engenharia Social. Em geral, o malware precisa retomar o contato com um canal de comando e controle (C&C) para receber instruções. Muitas variantes usam protocolos comuns, como o HTTP ou HTTPS. Embora o volume de prejuízo financeiro possa variar de uma empresa para a outra, a probabilidade de sofrer um ataque hoje em dia é muito alta para todos os tipos de setores e empresas.

A fim de reduzir os riscos, há diversas medidas que você pode tomar. Por exemplo:

- **A realização de backups regulares** com verificação é uma maneira muito eficaz de evitar danos caso o sistema ou a rede sejam afetados.
- **A segregação da rede** pode limitar os efeitos de um malware após a entrada dele nos seus sistemas.
- **A filtragem de emails** em busca de spam e phishing – além do bloqueio de tipos de arquivos usados com frequência pelos criadores de malware – pode ajudar a diminuir os riscos de impacto.
- **O treinamento inicial** e constante dos usuários pode reduzir as chances de execução de um malware.
- **O incentivo de que os seus usuários** encaminhem emails ou arquivos suspeitos para as equipes de TI ou de segurança pode ajudar a aumentar a eficácia dos seus métodos de filtragem.
- **Todos os softwares antimalware** usados no gateway, na rede e nos endpoints podem ajudar a identificar e prevenir a entrada de malware na rede ou a diminuir os danos causados por um eventual êxito nas tentativas de superação das suas defesas iniciais.
- **Firewalls e softwares usados para evitar** as invasões podem ajudar a identificar um tráfego desconhecido ou indesejado na rede.

Esses passos não apenas reduziriam os riscos de ataques de ransomware, mas também a probabilidade de vários outros tipos de problemas. A avaliação dos riscos e o aprimoramento das condutas gerais de segurança de uma organização podem reduzir de forma significativa a frequência e a gravidade de todos os tipos de violações de segurança.

Os ativos que correm o risco de sofrerem ataques de criptografia são praticamente todos os dados ou sistemas acessíveis pela sua rede ou pela internet.

Dispositivos médicos e de condicionamento físico

Com a informatização crescente do setor da saúde, cada vez mais pacientes e profissionais da saúde utilizam aparelhos médicos e de condicionamento físico. **Estes dispositivos costumam conter várias informações sigilosas,** mas, muitas vezes, a segurança e a privacidade deles não são uma preocupação até que seja tarde demais. **Como vimos na tendência dos ransomware, os riscos de dispor de informações muito confidenciais sem uma base sólida de segurança podem causar problemas sérios.** Porém, como estamos falando de uma tecnologia relativamente nova, é um bom momento para refletirmos sobre como proteger esses aparelhos.

Dispositivos médicos das redes de saúde

Os aparelhos médicos utilizados nas redes hospitalares podem ser máquinas grandes e caras, que costumam executar sistemas operacionais normais que, muitas vezes, estão bastante desatualizados (como o Windows XP Embedded). É comum que esses dispositivos proporcionem um acesso fácil ao restante da rede hospitalar, em que vários tipos diferentes de dados sigilosos são mantidos – como informações financeiras de cobrança, dados de identidade para seguradoras e informações de saúde geradas durante as consultas dos pacientes. **Do ponto de vista dos criminosos, esses dados encerram uma lucratividade gigante que pode chegar a até dez vezes mais que as informações de cartões de crédito ou débito.**

Os dispositivos médicos de um hospital costumam usar um sistema operacional semelhante às máquinas de desktop, e, assim, **é possível usar as mesmas tecnologias e técnicas para protegê-los.** No entanto, **caso um aparelho use um sistema operacional muito ultrapassado** (e talvez até sem suporte), **será necessário implementar uma proteção adicional significativa.** Pode ser melhor manter a máquina completamente desconectada de todas as conexões de rede. Ainda assim, alguns cuidados devem ser tomados para a proteção contra ameaças transmitidas por mídias removíveis.

Dispositivos médicos e rastreadores domésticos

Os aparelhos médicos e rastreadores para uso doméstico geralmente são muito pequenos, o que permite que sejam usados ou implantados sem causarem incômodo. A maioria usa sistemas operacionais próprios ou baseados em Linux. Eles podem se conectar à internet ou fazer a sincronização com um dispositivo móvel ou computador desktop. E, assim como no caso dos aparelhos hospitalares, eles também acabam sendo atualizados com pouquíssima frequência, caso seja necessário.

Os dispositivos usados pelos pacientes em casa não costumam armazenar as informações de cartões, mas é possível que eles salvem outros dados que os criminosos podem utilizar para roubos ou falsificações, tais como endereços de email, nomes, senhas de usuários e dados de GPS, incluindo os endereços de casa ou do trabalho. Além disso, eles podem indicar quando uma pessoa está fora de casa ou dormindo. **Um ataque a um dispositivo médico implantável pode possibilitar que os criminosos efetuem alterações às medidas prescritas, podendo causar problemas médicos graves ou mesmo fatais.**

Em um aparelho médico pessoal, é muito importante evitar que a máquina seja usada para prejudicar os usuários ou violar a privacidade deles. Obviamente, um ataque a uma bomba de insulina ou a um marca-passo conectado à internet será bastante diferente da invasão de um rastreador de condicionamento físico. As medidas de segurança necessárias para proteger os dispositivos serão as mesmas, apesar de uma bomba de

Os riscos de dispor de informações muito confidenciais sem uma base sólida de segurança podem causar problemas sérios.

insulina ou marca-passo poderem ter mais restrições na configuração padrão.

A proteção dos dispositivos médicos

Os fabricantes dos itens médicos pessoais e hospitalares têm a chance de conduzir uma mudança para promover uma segurança aprimorada ao refletir seriamente sobre ela desde a fase inicial dos projetos. **Os criadores desses aparelhos devem tomar várias providências** para torná-los mais seguros:

- **Concentrar-se na privacidade:** aprender os sete princípios do conceito Privacy by Design.
- **Criptografar os dados:** Proteger as informações no disco e em trânsito com uma criptografia forte sempre que houver um envio por email, pela web ou por mensagens instantâneas, por exemplo, ou quando ocorrer uma sincronização com o computador do usuário.
- **Esclarecer as opções de armazenamento de dados:** Dar aos usuários a capacidade de armazenar as informações rastreadas de forma local, não apenas na nuvem.
- **Autenticar o acesso à conta:** Verificar se as pessoas são realmente quem elas dizem ser. É essencial fazer uma autenticação antes de permitir a visualização, compartilhamento ou modificação das informações nos dispositivos implantados, pois as consequências do uso indevido são muito maiores. É importante realizar uma autenticação múltipla para conceder o acesso à conta online.
- **Criar um estado à prova de falhas:** Erros e falhas acontecem. Os aparelhos devem usar como padrão um estado que mantenha o acesso a funcionalidades críticas e não exponha os usuários a riscos quando ocorrerem problemas.
- **Supor que os códigos podem ser usados com más intenções:** Códigos legítimos podem ser aplicados para obrigar o dispositivo a executar códigos não autenticados. Levar essa hipótese em consideração ao lidar com os erros é vital para que os dispositivos não sejam usados para o mal.
- **Preparar-se para as vulnerabilidades:** Estabelecer e transmitir ao público uma política de divulgação responsável para os relatórios de vulnerabilidade.
- **Preparar-se para as violações de segurança:** Criar um plano de resposta a incidentes para conseguir ter uma reação adequada no caso de uma violação dos dados. Assim, você economizará tempo e será capaz de escolher as suas palavras com cautela caso haja uma emergência.
- **Preparar-se para o controle governamental:** no caso dos Estados Unidos, as agências en los Estados Unidos, o uso dos dispositivos médicos de perto. Assim, as alterações feitas agora poderão evitar problemas jurídicos e multas pesadas no futuro.

É provável que a segurança do setor da saúde vire o centro das atenções em um futuro próximo. Apesar dos problemas atuais, existe a oportunidade de promovermos uma transformação significativa que possa servir como o modelo de uma mudança positiva para outros setores em um momento no qual a Internet das Coisas começa a adentrar a nossa casa e o nosso ambiente de trabalho.

Os dispositivos usados pelos pacientes em casa não costumam armazenar as informações de cartões, mas é possível que eles salvem outros dados que os criminosos podem utilizar para roubos ou falsificações.

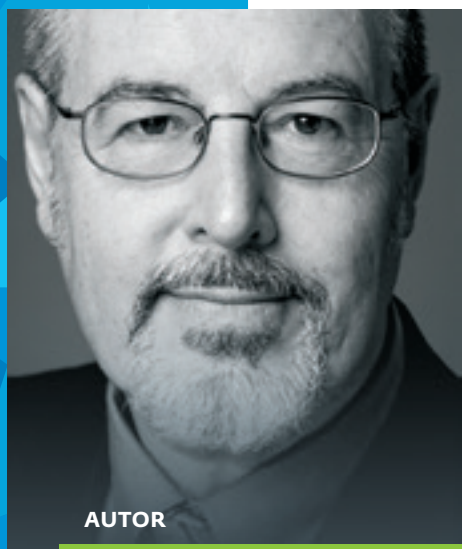
Apesar dos problemas atuais, existe a oportunidade de promovermos uma transformação significativa que possa servir como o modelo de uma mudança positiva para outros setores em um momento no qual a Internet das Coisas começa a adentrar a nossa casa e o nosso ambiente de trabalho.

Ameaças para infraestruturas críticas: a dimensão da Internet

- Definição de incidentes
- Incidentes problemáticos
- Um panorama preocupante

AUTOR

Cameron Camp
Malware Researcher



AUTOR

Stephen Cobb
Senior Security Researcher

7

Ameaças para infraestruturas críticas: a dimensão da Internet

Ataques digitais contra infraestruturas críticas constituíram uma tendência importante em 2016, e pode-se esperar que eles continuem a gerar manchetes e a perturbar a nossa vida em 2017.

O primeiro artigo de 2016 sobre segurança da We Live Security foi uma análise sobre a energia escura de Anton Cherepanov, um código malicioso usado em ataques contra empresas ucranianas de energia que resultaram em interrupções de energia elétrica por várias horas em centenas de milhares de casas naquela região do mundo.

No entanto, antes de discutirmos esse e outros incidentes, será útil comentar sobre a terminologia do assunto. Parece que "infraestrutura" pode significar coisas diferentes para diferentes pessoas, e nem todos concordam sobre o que "crítica" significa nesse contexto.

Definição de incidentes

Nos EUA, o Departamento de Segurança Interna (DHS) é responsável por proteger a infraestrutura crítica, que é composta por dezesseis setores *"cujos ativos, sistemas e redes, sejam eles físicos ou virtuais, são considerados tão essenciais para os Estados Unidos que a sua incapacitação ou destruição teria um efeito debilitante na segurança, na segurança econômica nacional, na saúde ou segurança pública nacional, ou em qualquer combinação desses elementos"*.

Você encontrará links com definições detalhadas dos dezesseis setores no endereço www.dhs.gov. Porém, gostaríamos de listar os títulos aqui para enfatizar como a infraestrutura crítica generalizada funciona:

- Instalações químicas
- Instalações comerciais
- Comunicações
- Manufatura crítica
- Barragens
- Bases industriais de defesa
- Serviços de emergência
- Energia
- Serviços financeiros
- Alimentação e agricultura
- Instalações governamentais
- Saúde Pública
- Tecnologia da Informação
- Reatores nucleares, materiais e resíduos
- Sistemas de transporte
- Sistemas de abastecimento hídrico.

Todos esses setores dependem, até certo ponto, da infraestrutura digital conhecida como internet; às vezes, entretanto, há uma confusão entre o que consideramos uma infraestrutura crítica e uma infraestrutura de internet. A diferença fica clara quando observamos dois incidentes importantes de 2016: as interrupções de energia na Ucrânia mencionadas no início e o fenômeno conhecido como ataque Dyn IoT DDoS de 21 de outubro (que foi abreviado como 21/10).

Parece que "infraestrutura" pode significar coisas diferentes para diferentes pessoas, e nem todos concordam sobre o que "crítica" significa nesse contexto.

Incidentes problemáticos

Os ataques feitos ao fornecimento de energia na Ucrânia foram possíveis devido à infraestrutura de internet. Os criminosos usaram e-mail e outras formas de conectividade com a internet para ganhar um ponto de apoio na rede dos computadores da concessionária de energia. Em algumas organizações atacadas, a falta de obstáculos eficazes possibilitou que os agressores acessassem pela internet as aplicações que controlam a distribuição de energia elétrica de forma remota. O pesquisador Robert Lipovsky da ESET coloca os ataques em contexto: *"No dia 23 de dezembro de 2015, cerca de metade dos lares na região de Ivano-Frankivsk da Ucrânia (com uma população de cerca de 1,4 milhão de pessoas) ficou sem eletricidade por várias horas"*. **Uma interrupção de energia como essa é claramente um ataque à infraestrutura crítica, bem como um possível prenúncio do que está por vir caso esse seja um ensaio para ataques futuros.**

O incidente 21/10 foi uma série de ataques DDoS (ataques de recusa de serviços) que utilizou dezenas de milhões de aparelhos conectados à internet (conhecidos em conjunto como a internet das coisas ou IoT) para atingir os servidores de uma empresa chamada Dyn, que presta serviços de nomes de domínio (DNS) para várias empresas famosas dos Estados Unidos. O DNS é o "caderninho de endereços" da internet, um sistema que serve para garantir que as solicitações de informação feitas na internet sejam entregues ao host correto (servidor, notebook, tablet, smartphone, geladeira inteligente e assim por diante). **O efeito do 10/21 foi evitar ou retardar o tráfego para sites, servidores de conteúdo e outros serviços de internet, como o e-mail.** Devido à natureza altamente interdependente **dos serviços de internet, o 10/21 teve um impacto negativo** em uma porcentagem significativa de empresas americanas devido a uma reação de danos colaterais escalonados em cadeia – muito embora elas não fossem o alvo direto do ataque.

Imagine uma empresa que venda software on-line. A loja dela na web não é o alvo dos ofensores, mas o tráfego do site cai porque os servidores que distribuem os anúncios on-line com os produtos da empresa estão inacessíveis. As páginas do site da empresa não são carregadas direito porque dependem de uma rede de distribuição de conteúdo (CDN) que está temporariamente indisponível. Mesmo quando os clientes conseguem concluir suas compras on-line, alguns talvez não consigam acessar o servidor de conteúdo para baixar o produto que acabaram de adquirir. É possível que outros não consigam ativar suas compras porque o servidor de licenciamento de software atinge o tempo limite. Os clientes frustrados não param de enviar e-mails à empresa. As linhas do atendimento ao cliente tocam sem parar. A saudação telefônica da empresa é alterada para informar a situação a quem liga. As campanhas de publicidade on-line e as compras de palavras-chave no mecanismo de pesquisa são suspensas para economizar dinheiro e reduzir a frustração entre os clientes em potencial. Há uma perda de receita. Os funcionários acabam tendo que ir além das suas responsabilidades de sempre.

Claro, cada empresa foi impactada de uma forma pelo 21/10. Algumas pessoas passaram por interrupções prolongadas, outras ficaram off-line por apenas alguns minutos, mas mesmo um minuto de tempo de internet pode representar um número grande de transações. Por exemplo: a receita de varejo on-line da Amazon é maior que 200.000 dólares por minuto. Nesse mesmo minuto, mais de 50.000 aplicativos são baixados pela App Store da Apple. **É óbvio que o 21/10 demonstrou como a infraestrutura da internet é essencial para o comércio diário, mas será que ele também foi um ataque à infraestrutura crítica?**

É óbvio que o 21/10 demonstrou como a infraestrutura da internet é essencial para o comércio diário, mas será que ele também foi um ataque à infraestrutura crítica?

Não ouvimos nenhum relato sobre o 21/10 ter prejudicado setores críticos como transporte, recursos hídricos, agronegócio, energia, dentre outros. No entanto, **não é nada difícil ver como variações do ataque 21/10 no serviço de DNS poderiam ter um impacto em elementos da infraestrutura crítica** como passagens aéreas, comunicação na cadeia de abastecimento ou até mesmo a distribuição de energia. E é possível enxergar esses ataques como parte de um padrão indicado por Bruce Schneier, um especialista em segurança: *"Durante os últimos um ou dois anos, alguém tem sondado as defesas das empresas que executam porções críticas da internet"*.

Um panorama preocupante

A tendência provável para 2017 é uma sondagem ainda maior da infraestrutura crítica por meio da infraestrutura de internet. Diversos criminosos continuarão procurando maneiras de causar danos, recusar serviços ou usar dados para chantagens.

Também esperamos ver novos ataques à infraestrutura da internet em si, o que interromperá o acesso a dados e serviços. E, claro, alguns desses dados e serviços podem ser vitais para o bom funcionamento de uma ou mais das dezesseis categorias de infraestrutura crítica. Por exemplo: alguns hackers criminosos vêm demonstrando que estão dispostos a transformar dados e sistemas médicos em um alvo. É provável que isso vire uma tendência global. Ao mesmo tempo, sabemos que diferentes países vêm se esforçando para melhorar a segurança digital dos sistemas de suporte à infraestrutura crítica. Nos EUA, há 24 ISACs (Centros de Análise e Compartilhamento de Informações) que abrangem a maioria dos aspectos desses dezesseis setores de infraestrutura crítica e oferecem canais expressos de comunicação e compartilhamento de conhecimentos sobre segurança digital. Em setembro, o Industrial Internet Consortium publicou uma proposta de estrutura de segurança para a internet das coisas industrial a fim de alcançar um amplo consenso na indústria sobre como proteger esse setor de tanto crescimento.

Torcemos demais para que esforços como esse e outros ao redor do mundo conquistem o apoio e os recursos necessários. No entanto, será preciso mais do que boas intenções para isso acontecer. Talvez seja até necessário contar com **uma pressão política exercida por quem provavelmente mais sentirá os danos causados pelos ataques digitais contra as infraestruturas críticas: o eleitorado.** Por exemplo: pode-se pensar em uma legislação que conceda ao governo um poder maior para proteger a rede elétrica contra ataques digitais seja algo óbvio e natural. De fato, o senado americano aprovou uma legislação como essa com apoio bipartidário em abril de 2016. No entanto, essa lei ainda não foi aprovada, e 2017 está quase chegando.

Conforme o cenário global fica cada vez mais interligado e interdependente além das fronteiras políticas, físicas e ideológicas, **espera-se uma mistura interessante e complexa de reações políticas e sociais dos países** que devem começar a lidar com as implicações de um ataque a essa infraestrutura crítica – assim como a definição do que seria uma reação adequada de defesa ou ataque, se for o caso. **Dizer que teremos um ano complicado pela frente seria um eufemismo.**

Não é nada difícil ver como variações do ataque 21/10 no serviço de DNS poderiam ter um impacto em elementos da infraestrutura crítica.

Desafios e implicações das legislações sobre cibersegurança

- Segurança cibernética: organização, colaboração e disseminação global
- Desafios e implicações da promulgação de leis relacionadas à segurança cibernética
- Em prol do desenvolvimento e da disseminação da cultura de segurança cibernética

AUTOR

Miguel Angel Mendoza
Security Researcher

8

Desafios e implicações das legislações sobre cibersegurança

O impacto da tecnologia atingiu quase todos os aspectos da sociedade e continuará intervindo neste sentido ao longo dos próximos anos.

Na atualidade, grande parte das atividades não teria como existir sem os sistemas de informação, os dispositivos eletrônicos ou as redes de dados, uma tendência que leva à hiperconectividade. Paralelamente, desenvolvem-se **novas ameaças e vulnerabilidades determinantes no tocante aos riscos, os quais continuam a crescer em número, frequência e impacto.** Assim sendo, as consequências da tecnologia para as sociedades atuais, assim como os riscos associados à sua utilização, mostram a **necessidade de proteger a informação e outros bens em diferentes níveis e esferas, agora não tão somente nas indústrias, empresas ou junto aos usuários, mas inclusive nos próprios países.** Por conseguinte, as legislações convocam ao aumento e à melhoria da segurança, com base em critérios objetivos fundados na moral e na ética.

A promulgação de leis relacionadas ao universo da segurança cibernética realça a importância de se poder contar com marcos regulatórios aplicáveis em larga escala, capazes de contribuir para reduzir os incidentes de segurança, combater a criminalidade cibernética, concomitantemente ao desenvolvimento e à promoção de uma cultura de segurança cibernética. No entanto, para além dos benefícios que as legislações possam trazer para a segurança dos dados, a realidade é que **existem diferentes tensões, posturas e contrapontos, os quais fazem da sua aplicação uma tarefa não tão fácil.** Na presente seção, destacamos algumas das legislações mais significativas em nível mundial, bem como alguns dos desafios atuais e futuros enfrentados pelos Estados, empresas e usuários/cidadãos pelo mundo afora.

Segurança cibernética: organização, colaboração e disseminação global

Nos últimos tempos, observa-se uma tendência para o desenvolvimento de novas legislações voltadas para a segurança cibernética em âmbito global. A partir da colaboração entre os setores público e privado, em prol da troca de informações e da criação de órgãos de segurança cibernética nos diferentes países, **pretende-se contar com ferramentas para enfrentar os riscos da era digital e legislar em matéria de crimes cibernéticos.**

União Europeia

Recentemente, a União Europeia adotou a Diretriz NIS para a segurança de redes e sistemas de informação, buscando a promulgação de legislações que levem os países membros a estarem equipados e preparados para dar resposta a incidentes, graças à criação de uma Equipe de Resposta a Incidentes de Segurança Informática (CSIRT) e de uma autoridade nacional competente na matéria. A criação de uma rede CSIRT pretende promover uma cooperação rápida e eficaz, o intercâmbio de informações relacionadas com os riscos e o desenvolvimento de uma cultura de segurança nos setores essenciais da economia e da sociedade, tais como: energético, de transportes, financeiro, de saúde e de infraestrutura digital. As novas leis procuram

Para além dos benefícios que as legislações possam trazer para a segurança dos dados, a realidade é que existem diferentes tensões, posturas e contrapontos, os quais fazem da sua aplicação uma tarefa não tão fácil.

gerar um mesmo nível de desenvolvimento das capacidades em segurança cibernética, visando evitar incidentes que ameacem as atividades econômicas, a infraestrutura, a confiabilidade ou o funcionamento de sistemas redes críticos em cada país.

Estados Unidos

No final do ano passado, o Congresso dos Estados Unidos aprovou a chamada Lei de Segurança Cibernética, no intuito de proteger o país contra ataques cibernéticos, por meio de um marco legal capaz de promover a troca de informações relativas às ameaças cibernéticas, entre o setor privado e o governo, de forma responsável e com rapidez suficiente para enfrentar as emergências. De acordo com a lei, as informações sobre uma ameaça presente em um sistema podem ser compartilhadas, visando prevenir um ataque ou mitigar um eventual risco que possa afetar outras empresas, organizações ou usuários. Graças ao uso de controles de segurança, da coleta de informações e de medidas de proteção, as organizações e o governo podem coordenar ações de inteligência e de defesa.

América Latina

Em um relatório recentemente publicado, aplicou-se um modelo para determinar a capacidade de segurança cibernética, nos países da América Latina e do Caribe. Este documento destaca a importância de uma divulgação responsável das informações nas organizações dos setores público e privado, por ocasião da identificação de uma vulnerabilidade. Ele igualmente sublinha a importância de marcos legais, da investigação, do processamento de provas eletrônicas, assim como da formação e capacitação de juízes e procuradores em matéria de segurança cibernética. A adesão às convenções internacionais, tal como aquela de Budapeste, e a assinatura de acordos transfronteiriços em prol da cooperação são outros aspectos determinantes. Da mesma forma, as práticas habituais, associadas ao uso de tecnologias voltadas para a segurança, são levadas em conta na formação de uma "sociedade cibernética resiliente".

Ásia - Pacífico

Outro estudo que busca avaliar o nível de maturidade em termos de segurança cibernética, com foco em países da zona Ásia-Pacífico, igualmente considera as legislações como um indicador-chave no campo da segurança. Neste ano, até o momento, vários países da região lançaram novas políticas ou estratégias em matéria de segurança cibernética, tendo atualizado marcos regulatórios existentes a fim de se adaptarem a novos desafios e a questões emergentes. Por exemplo, a Austrália implementou a sua estratégia de segurança cibernética, envolvendo recursos suplementares e o incentivo a uma maior associação do setor privado com a polícia cibernética nacional. Outros países, tais como a Nova Zelândia, lançaram estratégias nacionais de segurança cibernética, com foco na melhoria da sua capacidade de resiliência, na cooperação internacional e na resposta a crimes cibernéticos.

Desafios e implicações da promulgação de leis relacionadas à segurança cibernética

O atual estádio em matéria de riscos impõe a necessidade de se poder contar com marcos regulatórios para a gestão da segurança, uma tendência no âmbito organizacional. De forma semelhante, **quando nos referimos às legislações, fazemos referência à aplicação de normas em ampla escala, em busca de uma regulamentação da segurança cibernética de nível nacional.** Geralmente, as legislações têm impacto positivo na normatização das condutas. No entanto, **há desafios que devem ser superados para uma efetiva aplicação das leis.** Por exemplo, o informe do Global Agenda Council on Cybersecurity levanta desafios enfrentados pelo países que começaram a legislar sobre o assunto, a partir da Convenção de Budapeste. Contudo, eles podem igualmente ser

A promulgação de leis relacionadas ao universo da segurança cibernética realça a importância de se poder contar com marcos regulatórios aplicáveis em larga escala, capazes de contribuir para reduzir os incidentes de segurança.

apresentados em outros acordos e convenções de alcance global ou regional, inclusive com iniciativas específicas de cada país. A realidade indica que, dada a influência da tecnologia e dos hábitos a ela associados, a implementação de uma legislação pode ter impacto em vários interesses, os quais incluem desde empresas de tecnologia até os próprios usuários. **A partir dessas tensões, originam-se diferentes conflitos e desafios que destacamos a seguir.**

Atraso na publicação de leis

Diferentes elementos determinam a criação de leis nos diferentes países, de tal forma que a sua promulgação atende a várias condições, tais como questões políticas ou de relevância em eventos e iniciativas locais ou ainda a adesão a acordos internacionais que incentivem a alcançar um mesmo nível de desenvolvimento na colaboração transfronteiriça. No entanto, em razão destas mesmas condições e características, as legislações são adiadas. Por exemplo, até este ano, quase metade dos países que ratificaram a sua participação na Convenção de Budapeste levou uma década ou mais para complementar a referida ratificação, entre outras razões, devido ao atraso no desenvolvimento das suas leis. Além disso, o acordo tem foco em alguns aspectos legais, no amplo leque de possibilidades relacionadas ao campo da segurança cibernética.

Leis alheias ao contexto e ao tempo

Com relação ao ponto anterior, é preciso igualmente levar em conta que a tecnologia está avançando em ritmo acelerado, de modo que o desenvolvimento de normas pode apresentar atraso considerável em relação aos avanços tecnológicos. Da mesma forma que as organizações atualizam continuamente os seus regulamentos em matéria de mudanças no nível de risco e no tocante às novas tecnologias, **as leis devem estar na vanguarda no que diz respeito às questões atuais e emergentes passíveis de regulamentação.** Assim sendo, talvez a maneira de remediar esta disparidade seja **adotar um enfoque com base na regulamentação do comportamento humano, ao invés de tecnologias que podem se tornar obsoletas em prazos relativamente curtos.** Esta pode vir a ser a maneira mais confiável para que as referidas regulamentações sejam eficazes, entretanto, é igualmente necessário salientar que no futuro podem surgir tensões. Por exemplo, o fato de se tentar regulamentar comportamentos que, eventualmente se convertam em leis tácitas, tal como o uso das redes sociais.

A tecnologia está avançando em ritmo acelerado, de modo que o desenvolvimento de normas pode apresentar atraso considerável em relação aos avanços tecnológicos.

Heterogeneidade técnica e jurídica

Acrescenta-se a este quadro anterior o fato de **os países estarem em condições diferentes para aderirem aos acordos internacionais ou regionais,** os quais, inclusive, determinam as iniciativas próprias ao desenvolvimento das suas leis. As brechas legais e técnicas dificultam os esforços para responder, investigar e julgar incidentes de segurança cibernética, tornando-se inibidoras da colaboração internacional. Por exemplo, as iniciativas regionais ou bilaterais são desenvolvidas em função de necessidades específicas, tal como é o caso do Escudo para Proteção da Privacidade entre a União Europeia e os Estados Unidos, um quadro legal que visa proteger os direitos fundamentais de qualquer pessoa da UE cujos dados pessoais tenham sido transferidos para empresas norte-americanas. Isso certamente não leva em conta a colaboração com outros países ou regiões.

Conflitos legais e princípios básicos

Neste mesmo contexto, geralmente se pensou nas legislações como algo positivo, entretanto, não há leis perfeitas e elas são, pelo contrário, passíveis de serem melhoradas, especialmente se considerarmos que **existem projetos que poderiam atentar contra os princípios sobre os quais se baseia a Internet e, até mesmo, contra alguns direitos humanos.** Com base na ideia, segundo a qual, a Internet é livre e não tem fronteiras e as leis são aplicáveis em âmbito nacional, há casos em que surgem conflitos

constitucionais ou legais, principalmente acerca dos significados e conceitos inerentes à privacidade ou à liberdade de expressão. **Neste caso, é possível novamente constatar a manifestação do eterno debate entre privacidade e segurança.**

Limitações no âmbito da aplicação

Seguindo a mesma lógica, a ausência de legislações ou de acordos sobre questões pontuais mina a colaboração internacional e até mesmo no âmbito de um mesmo território. **Os setores público e privado enfrentam um desafio no tocante ao acesso à informação para as investigações, com desdobramentos na segurança, no direito à privacidade e nos interesses comerciais, particularmente em relação às empresas de tecnologia.** A título de exemplo, há o caso bem conhecido que confrontou o FBI e a Apple em que uma juíza americana solicitou a colaboração da gigante tecnológica para desbloquear o iPhone de um terrorista envolvido em um atentado ou ainda o recente caso em que um juiz do Rio de Janeiro ordenou o bloqueio do WhatsApp no Brasil e a aplicação de multas ao Facebook. Sem dúvida, **eventos desta natureza evidenciam a necessidade de acordos locais e transfronteiriços de colaboração,** a fim de se evitar a transgressão entre os interesses de ambas as partes.

Em prol do desenvolvimento e da disseminação da cultura de segurança cibernética

A promulgação de leis relativas à segurança cibernética já há anos ganhou relevância em nível internacional, em razão da quantidade, da frequência e do impacto dos incidentes registrados ao redor do mundo. Várias iniciativas consideram a legislação na matériasobre o assunto como um elemento fundamental para o aumento do nível de maturidade nos países. **Assim sendo, a meta consiste em poder contar com medidas legais de proteção, em diferentes níveis e esferas.** Portanto, as legislações começaram igualmente a levar em consideração os elementos necessários para a segurança dos países, desde a sua capacidade em responder a incidentes de grande amplitude, passando pela proteção da sua infraestrutura crítica, pela sua capacidade em colaborar com outros países, e até mesmo considerando o desenvolvimento de uma cultura de segurança passível de ser difundida em meio à população. **Tudo isso sem negligenciar problemas já conhecidos, tais como a privacidade, a proteção de dados pessoais e os crimes cibernéticos.**

Estamos diante de uma tendência crescente no tocante ao desenvolvimento de novas legislações, as quais determinam o modo de proteção dos bens de uma nação no contexto da segurança cibernética, além de estimularem a cooperação e a colaboração entre os setores público e privado de cada país, o que igualmente ocorre em nível internacional, no intuito de bloquear as ameaças e ataques cibernéticos atuais e futuros. Contudo, **apesar dos benefícios que isso possa representar, existem desafios que devem ser superados para se alcançar este objetivo e compreender as características, necessidades e condições tanto do setor público quanto do privado, assim como de todos os envolvidos,** entre os quais estão as populações em sua condição tanto de usuário quanto de cidadão. Os obstáculos e as limitações para a colaboração podem incluir falta de confiança, legislações ineficazes e interesses conflitantes entre os diferentes setores. A partir desses desafios e tensões, vislumbra-se a necessidade de se definir regras claras para todos os participantes, talvez a partir de acordos internacionais, regionais ou locais, as quais contemplem todas as partes envolvidas, no intuito de que a legislação seja realmente eficaz, podendo ser aplicada e cumprida. Sem dúvida, **há um longo caminho a ser percorrido, o que requer a colaboração entre os governos, a iniciativa privada, o setor acadêmico e, obviamente, os usuários;** tudo isso visando obter uma finalidade de maior alcance, voltada para o desenvolvimento da cultura de segurança cibernética.

Os obstáculos e as limitações para a colaboração podem incluir falta de confiança, legislações ineficazes e interesses conflitantes entre os diferentes setores.

Plataformas de jogo: os potenciais riscos dos consoles integrados aos computadores

AUTOR

Cassius de Oliveira Puodzius
Security Researcher

9

Plataformas de jogo: os potenciais riscos dos consoles integrados aos computadores

Os jogos utilizam tecnologias de ponta com hardware e software avançados para oferecer a melhor experiência de entretenimento aos usuários.

Por serem tão populares e bem-sucedidos, eles transformaram a indústria de jogos em um setor importante do mercado global que, apesar de crises financeiras, apresentou um crescimento veloz e deve continuar em expansão no futuro próximo.

A segurança é essencial para os jogos, porque milhares de pessoas ao redor do mundo investem grandes quantias de dinheiro para jogar em diversas plataformas, como consoles, computadores e telefones celulares. Não resta dúvida **de que isso faz com que as plataformas de jogos sejam alvos valiosos de atividades ilegais de *cracking*** (e *hacking* bem-intencionado para fortalecer a segurança) por pessoas em busca de fama, diversão e lucro

De acordo com o Relatório global do mercado de jogos em 2016 preparado pela Newzoo, **esse mercado crescerá 8,5% em 2016, chegando a uma receita de quase cem bilhões de dólares.** Os jogos para dispositivos móveis têm um papel importante nesse crescimento, pois os smartphones e tablets produzirão 36,9 bilhões de dólares até o final de 2016, o que representa 37% de todo o mercado de jogos. A estimativa de **crescimento anual para essa área é de 6,6% nos próximos anos, atingindo uma receita de 118,6 bilhões de dólares em 2019.** A consolidação dos jogos para os aparelhos móveis e as experiências interessantes de jogabilidade possibilitadas pela integração universal de diferentes plataformas possibilitam que a indústria de jogos tenha um sucesso constante. Sendo assim, **a estratégia de crescimento desse mercado conta com duas apostas principais: a diversificação e os jogos casuais.**

Cenário de ameaças da indústria de jogos

O modelo de negócios da área de jogos evoluiu de forma drástica nos últimos anos, o que pode ser atribuído parcialmente às medidas desenvolvidas para garantir a segurança do usuário. No entanto, **essas ameaças continuam se adaptando às mudanças e prejudicando os jogadores.**

No passado, os jogos geravam receita principalmente pela "venda de pacotes de software ", de acordo com a qual os usuários compravam uma licença inicial e recebiam o direito de jogar aquele título o quanto quisessem. Esse modelo de negócios continua sendo relevante no mercado de jogos, embora tenha diminuído ao longo dos últimos anos. **Uma das razões que fazem as empresas do setor abandonarem esse modelo é a pirataria.** Por exemplo, a Nintendo, uma gigante da indústria de jogos, diz o seguinte sobre a falsificação: *"La piratería sigue siendo una grave amenaza para el negocio de Nintendo y para las más de 1.400 empresas desarrolladoras que trabajan con el objetivo de ofrecer juegos únicos e innovadores para esta plataforma"*.

A segurança é essencial para os jogos, porque milhares de pessoas ao redor do mundo investem grandes quantias de dinheiro para jogar.

Apesar dos esforços do setor para implantar medidas defensivas de combate à pirataria, **temos visto os consoles sendo atacados com frequência nas últimas décadas.** Um exemplo foi o grupo failoverflow que lançou um hack para o PlayStation 4 em 2016. Embora eles não tenham realizado nenhuma falsificação, suas atividades tiveram o efeito colateral de facilitar a pirataria.

Para lidar com a pirataria e diversificar o modelo de negócios do mercado de jogos, esse setor vem desenvolvendo "outros formatos de distribuição". ao longo dos últimos anos. **Esses formatos incluem assinaturas, jogos digitais completos, conteúdo digital em complementos, jogos para redes móveis e sociais,** e outras formas de venda diferentes do tradicional pacote de software.

Esse modelo de negócios que acabou de ser criado é muito mais dependente da Internet do que "as vendas de pacotes de software". Além disso, as plataformas de jogos que mantêm uma conexão de rede representam um pouco de risco para a segurança computacional, porque **os criminosos podem explorar as vulnerabilidades da máquina para controlar a plataforma de jogo de forma remota ou instalar um malware de acesso às informações confidenciais dos jogadores.**

No entanto, os jogos online não são uma novidade. Esses sistemas surgiram para PC nos primórdios da Internet, devido ao suporte de hardware. Com a expansão da Internet em banda larga, os jogos online seguiram a tendência ao lançar títulos muito bem-sucedidos que conseguiram um grande número de jogadores e evoluíram para o que chamamos de jogos MMO (Multijogador Massivo Online). Por exemplo: em 2010, o jogo World of Warcraft (WoW) alcançou um pico de doze milhões de assinantes em todo o mundo. Conforme o modelo de negócio vai evoluindo, ele também começa a atrair novos tipos de ameaças. Os jogos online enfrentam perigos comuns do mundo cibernético, como os malware ocultos nos instaladores, o que inclui os trojanos dos softwares do jogo ou as campanhas mal-intencionadas, que aparecem como jogos populares para espalhar os malware ou roubar as contas dos jogadores. Porém, essa modalidade tem sido explorada por outras formas específicas de contravenção.

Conforme os jogadores vão se envolvendo com o jogo, é comum observar uma mistura do mundo virtual com a realidade. **Os cibercriminosos tiram proveito dessa interface entre os dois mundos e utilizam os jogos online para a lavagem de dinheiro.**

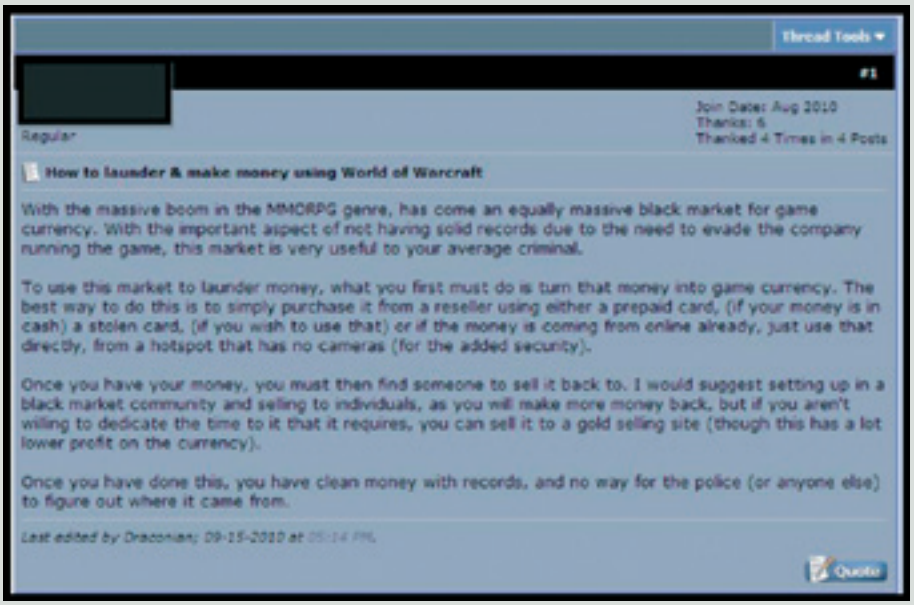
Isso acontece porque os bens virtuais são negociados em sites de comércio eletrônico como o eBay, em que os itens de jogo que foram roubados das contas de outros jogadores ou comprados usando dinheiro ilegal são vendidos para outros jogadores em troca de dinheiro limpo e de verdade. No caso do WoW, esse tipo de incidente causou tamanho impacto que a Blizzard decidiu emitir um alerta de segurança após uma série de logins não autorizados e relatórios de jogadores sobre golpes de "lavagem de dinheiro" em 2013.

Outro método que os cibercriminosos usam para conseguir os dados dos usuários é por meio do ataque direto às empresas de jogos. A Blizzard, o Steam, e a Sony (dentre outras) sofreram violações de dados que representaram riscos como a já mencionada lavagem de dinheiro ou a perda financeira para a empresa e para os clientes, com casos em que números de cartões de crédito e informações pessoais foram roubados dos clientes.

Apesar das ameaças cibernéticas, os jogos de console começaram a entrar no mundo online cerca de uma década atrás – afinal de contas, estamos falando de um mercado

Conforme o modelo de negócio vai evoluindo, ele também começa a atrair novos tipos de ameaças.

Post de um fórum que explica como lavar dinheiro ilícito com jogos MMO



Fonte: **Laundering Money Online: a review of cybercriminals' methods** escrito por Jean-Loup Richet.

gigantesco e muito capitalizado. Empresas gigantes do ramo de jogos de console como Microsoft (Xbox), Nintendo (Wii) e Sony (PlayStation) lançaram o Xbox Live (2002), a Nintendo Wi-Fi Connection (2005) e a PlayStation Network (conhecida como PSN, 2006), respectivamente.

Todas as iniciativas mencionadas são serviços de distribuição online projetados para fornecer sistemas multijogador e mídias digitais, e passaram por várias reformulações desde a sua criação. A Nintendo Wi-Fi Connection, por exemplo, foi substituída pela Nintendo Network (conhecida como NN) em 2012. Ao todo, as comunidades de rede abrangem quase 185 milhões de membros. Esse número **elevado de integrantes transformou as redes de jogos em grandes alvos** para a atividade de cibercriminosos. Na véspera do Natal de 2014, um grupo conhecido como Lizard Squad conseguiu atacar a Playstation Network e o Xbox Live, o que tirou os serviços do ar por muitas horas e parou logo após o grupo receber três mil cupons de MegaPrivacy

Já deve ter ficado evidente que o cenário de ameaças da indústria de jogos é bastante desafiador. No entanto, isso não é nenhuma surpresa se considerarmos a perspectiva de tamanho, riqueza e crescimento do mercado. As empresas de jogos fazem investimentos significativos para enfrentar as ameaças cibernéticas ao mesmo tempo em que buscam a expansão do mercado lançando jogos para mais plataformas e atraindo mais jogadores.

Convergência e ameaças futuras

Ter um número maior de jogadores e de operações monetárias dentro do jogo gera grandes desafios de segurança para o futuro. Além disso, a **integração dos consoles com computadores e telefones celulares está crescendo rapidamente, o que pode ter um impacto significativo na segurança** dessas informações nos próximos anos.

O relatório global sobre o mercado de jogos publicado pela Newzoo em 2016 revela que

A integração dos consoles com computadores e telefones celulares está crescendo rapidamente, o que pode ter um impacto significativo na segurança dessas informações nos próximos anos.

87% dos jogadores de console também jogam em PCs e utilizam o computador como uma "central para os jogos de console". Algo que corrobora essa informação é o fato de que os PCs e celulares são considerados dispositivos essenciais, ao passo que os consoles de jogos não são. Além disso, é importante ressaltar que os computadores são aparelhos muito mais adequados para o compartilhamento de conteúdo online do que os consoles, e os usuários de PC fazem atualizações com mais frequência.

A Microsoft apelidou sua estratégia de convergência de "compre uma vez, jogue em qualquer lugar". Em 2013, a empresa contratou Jason Holtman que costumava ser responsável pelo popular serviço de jogos Steam, da Valve, para liderar a evolução da plataforma de jogos da Microsoft. O processo foi descrito como "a possibilidade de jogar um título no seu Xbox e passar ao PC continuando de onde você parou sem precisar comprar ou jogar as mesmas fases outra vez".

Na verdade, os fabricantes de console já estão implementando essa ideia em uma certa medida. O Wii U consegue transmitir os jogos para o GamePad, o PlayStation 4, para o Vita. No caso do Xbox da Microsoft, o objetivo é fazer a transmissão para os PCs.

No início de 2015, a Microsoft anunciou que planeja renovar o Xbox App para PC, lançado em 2012, para oferecer acesso ao Xbox Live, controle remoto e a funcionalidade de uma segunda tela para o Xbox. A partir de 2015, o Xbox e o Windows 10 terão uma integração caprichada para criar o ambiente de jogo ideal da Microsoft.

Poucos meses após o anúncio do Xbox App, a transmissão de Xbox para PC foi lançada na GDC 2015. A opção do Xbox App para iOS e Android veio em 2016, quando o aplicativo foi rebatizado e remodelado para incluir funcionalidades do Xbox App do Windows 10.

Essa integração pode permitir que spyware que estiverem sendo executados em PCs e aparelhos móveis comprometidos se infiltrem em bate-papos de jogadores e consigam acesso a senhas de diferentes aplicativos, que costumavam ser restritas apenas aos consoles do Xbox.

Até o momento, **talvez possa parecer que a evolução dos jogos para console na direção das outras plataformas seja uma tendência unidirecional, mas não é o caso.** A Valve, uma empresa americana criadora de jogos online renomadíssimos para PC, está caminhando no sentido oposto.

O portfólio dela inclui títulos de grande sucesso como *Half-Life, Counter Strike e Dota*. Além disso, a Valve é proprietária do Steam, a maior plataforma de jogos online do mundo, que é alvo do TeslaCrypt, um ransomware que criptografa mais de 185 tipos diferentes de arquivos associados aos jogos.

O Steam anunciou um recorde de 125 milhões de usuários ativos em todo o mundo em 2015. O site da plataforma exibe estatísticas em tempo real que mostram **um pico de quase 12,5 milhões de usuários logados nas últimas 48 horas** (no momento em que este texto estava sendo escrito).

Um recurso chamado *in-home streaming* foi lançado pelo Steam em maio de 2014. Com ele, os jogadores que têm vários computadores executando o Steam dentro da mesma rede podem integrar e realizar a instalação de forma remota, abrir os softwares e jogar em computadores diferentes. Desse modo, é possível rodar um jogo de PC em um computador com poucos recursos que esteja conectado a uma outra máquina principal que seja para jogos, e os dois computadores nem precisam contar com os mesmos sistemas operacionais. Por outro lado, o mecanismo do *in-home streaming* concede acesso total a desktops remotos, , o que poderia ser usado para uma movimentação latera na rede.

Essa integração pode permitir que spywares que estiverem sendo executados em PCs e aparelhos móveis comprometidos se infiltrem em bate-papos de jogadores e consigam acesso a senhas de diferentes aplicativos, que costumavam ser restritas apenas aos consoles do Xbox.

No final de 2013, a Valve lançou o SteamOS, , uma plataforma Linux projetada para rodar jogos do Steam. O desenvolvimento desse sistema abriu o caminho para a principal estratégia da Valve: conquistar o mercado de jogos de console com a Steam Machine. A Valve lançou a Steam Machine em novembro de 2015. Trata-se de um computador de jogos semelhante aos consoles que executa o SteamOS e possibilita que os usuários joguem pelo Steam (online) na tela da TV. Ainda que não seja **possível indicar quais empresas de jogo terão mais sucesso na estratégia de diversificação, é justo afirmar que a convergência será o carro-chefe desse setor.**

Até mesmo os acessórios vestíveis estão virando plataformas para jogos. Após o sucesso estrondoso do Pokémon GO, um aplicativo de jogo lançado em 2016 que ultrapassou quinhentos milhões de downloads em todo o mundo, a Niantic Labs anunciou que já tem um aplicativo do Apple Watch pronto para lançamento.

Sob o ponto de vista da segurança, a convergência traz grandes preocupações, uma vez que haverá mais dados (valiosos) fluindo de e para muitos aparelhos e plataformas diferentes. Além disso, **haverá mais recursos sob um possível risco de serem explorados por um criminoso** como parte da iniciativa recente, de criar botnets para controlar os dispositivos da IoT (internet das coisas).

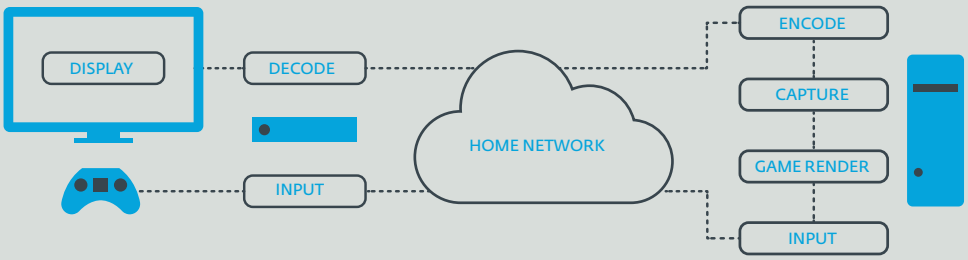
No âmbito pessoal, **os jogos têm acesso a informações que costumam ser cobiçadas por cibercriminosos, como os dados pessoais e os números de cartões de crédito.** Além disso, com a expansão dos jogos para novas plataformas, o alcance dos dados tende a ser ainda maior. Por exemplo: por meio de uma falha de segurança existente em algum jogo rodando em um acessório vestível, os cibercriminosos poderiam roubar o histórico médico das vítimas.

Conforme os ataques ganham abrangência – e os jogos ficam cada vez mais online –, a necessidade de elevar o nível de segurança também cresce. **As ameaças enfrentadas por esse setor no momento tendem a atingir plataformas que não costumavam ser tão frequentes,** e os incidentes de segurança devem causar ainda mais impacto.

Principalmente hoje em dia, com o crescimento do debate sobre jogos e produtividade no ambiente de trabalho, as casas e empresas poderão ficar expostas às ameaças cibernéticas no momento em que aceitarem jogos em suas redes. O simples

Sob o ponto de vista da segurança, a convergência traz grandes preocupações, uma vez que haverá mais dados (valiosos) fluindo de e para muitos aparelhos e plataformas diferentes.

Esquema de "Retransmissão em casa" do Steam



Fonte: Steam

fato de ter um console de jogos dentro do escritório pode expor toda a empresa a APTs (ameaças persistentes avançadas, na sigla em inglês) **que utilizem a plataforma de jogos como um pivô para a rede interna.** Além disso, os incidentes de segurança relacionados aos jogos terão um possível impacto muito maior sobre os jogadores. Pense no caso da Microsoft, que encarou o vazamento das chaves particulares do certificado digital do "xboxlive.com" em novembro de 2015, o que significava que essas informações poderiam ser usadas para assumir o papel dos servidores da Microsoft não só contra os jogadores de console do Xbox Live, mas também contra os usuários de PC e aparelhos móveis.

Além dos cuidados habituais qque sempre devemos ter com os jogos online, principalmente para os lançamentos de grande sucesso como o Pokémon GO em 2016), **os desenvolvedores devem considerar o escalonamento do fluxo de dados entre dispositivos durante o jogo para garantir que os aparelhos não sejam usados para fins maliciosos** nem virem uma porta de entrada para redes domésticas e empresariais.

As ameaças enfrentadas por esse setor no momento tendem a atingir plataformas que não costumavam ser tão frequentes, e os incidentes de segurança devem causar ainda mais impacto.

Conclusão

Nesta nova edição do relatório sobre Tendências abordamos temas bem variados: desde questões gerais, tais como as infraestruturas críticas ou os desafios em matéria de legislação que os países devem enfrentar, até questões mais cotidianas e próximas do usuário final, a exemplo das ameaças em dispositivos da Internet das Coisas ou em consoles de videogames.

Conclusão

Apesar da diversidade e da variedade dos temas abordados ao longo das diferentes seções, há algo em comum a todos: **o fator humano.**

Uma frase se tornou quase um dogma em segurança informática: **"os usuários finais são o elo mais fraco da cadeia de segurança".** Este estado de coisas tem sido comumente empregado pelos cibercriminosos para espalhar as suas ameaças. Isso é algo que não pode ser negado, **daí a necessidade dos usuários e das empresas estarem capacitados em matéria de segurança, conhecerem as ameaças, saberem como elas se propagam e terem ciência de que medidas devam ser implementadas para protegerem a sua privacidade e as suas informações.** Mas com a atual concepção de conscientização não é suficiente: a relevância do fator humano deve adquirir outro nível de importância.

Estamos em um momento no qual o surgimento de novos aplicativos e dispositivos ocorre de modo acelerado: realidade virtual, realidade aumentada, integração de tecnologias em todos os níveis (desde consoles de videogames até dispositivos IoT), virtualização de servidores no ambiente corporativo e outros. **Todas estas inovações poderiam se constituir (e, certamente, isso ocorrerá) como novos vetores de ataque** a serem aproveitados pelos cibercriminosos, somando-se à longa lista de vetores já existentes.

Além disso, essa situação é agravada quando observamos que ainda há usuários que caem facilmente em campanhas de phishing ou baixam aplicativos maliciosos em seus dispositivos, sem tê-los protegido adequadamente. **Este quadro se torna menos otimista quando percebemos no horizonte que tudo parece estar preparado para que sejam exploradas ameaças como o RoT (Ransomware of Things)**. Em suma: estamos em um estágio em que temos usuários que utilizam tecnologia de última geração, mas com conceitos de segurança com mais de 10 anos de idade.

Entretanto, o rápido avanço tecnológico nos impõe outros desafios no tocante aos riscos enfrentados pelos usuários e, portanto, no que diz respeito à sua consciência. **Na retaguarda de novo aplicativo ou de cada novo dispositivo há um grupo de pessoas que deveria, desde a fase de concepção, pensar na segurança das informações.** O fato de existirem mais vulnerabilidades críticas não é algo fortuito, pois está claro que a área de ataque está sempre em ampliação, o que determina uma postura que considere a segurança desde a concepção do projeto.

Além disso, a consciência deveria alcançar indústrias e setores que até o momento não estiveram tão ligados à segurança da informação. Em razão da informação sensível que processam, identificamos como tendências importantes no próximo ano a segurança em infraestruturas críticas no setor da saúde. Entretanto, **o treinamento/capacitação e a sensibilização/conscientização nessas esferas devem igualmente ser acompanhados de uma gestão adequada e de controles efetivos,** complementados suplementarmente por leis e regulamentos.

Para além do fato dessa retrospectiva poder soar um tanto pessimista, **a realidade é que há efetivamente muitas possibilidades de se fazer uso seguro da tecnologia.** 2017 está se configurando como um ano em que vão continuar crescendo os desafios

Estamos em um estágio em que temos usuários que utilizam tecnologia de última geração, mas com conceitos de segurança com mais de 10 anos de idade.

em matéria de segurança e estamos no momento certo para enfrentar esses desafios.

Não se trata apenas de treinar e capacitar o usuário final, é preciso que os governos adotem marcos legais que favoreçam o tratamento das questões de segurança cibernética, as quais envolvem desde institucionalizar a capacitação voltada para a temática da segurança, até para proteger adequadamente as infraestruturas críticas. Neste sentido, **é igualmente imprescindível que as empresas decidam implementar uma política de gestão adequada em prol da segurança de sua informação e que os desenvolvedores não posterguem o tratamento da questão da segurança nos seus produtos** em detrimento da usabilidade.

A informação e a sua manipulação são aspectos-chave nas sociedades atuais e, portanto, uma proteção adequada se faz essencial. Entretanto, **considerando a multiplicidade de aspectos e de atores envolvidos, ninguém poderia desconsiderar os problemas relacionados ao assunto.** Assim sendo, é o momento de nos ocuparmos de todos os aspectos da segurança apresentados ao longo deste relatório, enfatizando que se trata de um trabalho conjunto entre as diferentes partes envolvidas: desde os grandes fabricantes de tecnologia, empresas e governos, até os usuários, obviamente. **Se conseguirmos alcançar consensos e acordos no tocante a essas temáticas, o futuro da segurança da informação será promissor.**

2017 está se configurando como um ano em que vão continuar crescendo os desafios em matéria de segurança e estamos no momento certo para enfrentar esses desafios.

Fundada em 1992, a ESET é uma companhia global de soluções de software de segurança que provê proteção de última geração contra ameaças informáticas. A empresa conta com escritórios centrais em Bratislava (Eslováquia), e de coordenação em San Diego (Estados Unidos), Buenos Aires (Argentina) e Singapura. Em 2012 a empresa comemorou seus 20 anos na indústria da segurança da informação. Além disso, atualmente a ESET possui outras sedes em Londres (Reino Unido), Praga (República Checa), Cracóvia (Polônia), Jena (Alemanha), São Paulo (Brasil) e Cidade do México (México).

Desde 2004, a ESET opera na América Latina, em Buenos Aires (Argentina), onde dispõem de uma equipe de profissionais capacitados para responder às demandas do mercado de forma concisa e imediata, além de um Laboratório de Investigação com foco no descobrimento proativo de diversas ameaças informáticas.

Além disso, desde 2009, foi aberto um escritório em São Paulo (Brasil), com o objetivo de desenvolver o mercado local. O escritório faz parte da Sede Regional de Buenos Aires, mas tem estrutura e pessoal próprio com o objetivo de trabalhar mais próximo do mercado brasileiro.

Para mais informações visite: **blogs.eset.com.br/laboratorio/**

www.eset.com.br

ENJOY SAFER TECHNOLOGY™