Data: 27-01-2020

Título: Da Microsoft ao Cristo Rei. Esta startup portuguesa descobre falhas na internet

Pub: dinheiro vivo

Tipo: Internet Secção: Nacional

Da Microsoft ao Cristo Rei. Esta startup portuguesa descobre falhas na internet

A equipa principal da BinaryEdge, com Florentino Bexiga, Tiago Henriques (CEO) e Marco Silva (CTO), da esquerda para a direita (foto cedida pelos próprios)

João Tomé 27.01.2020

O seu motor de busca especial analisa a internet (e os vários IPs) 240 vezes por mês, em busca de possíveis vulnerabilidades de pessoas e empresas. São portugueses, entre Lisboa, Algarve, Zurique e Londres e já reportaram várias fragilidades em Portugal e foram base para revelações mundiais. Agora foram comprados por empresa norte-americana. Esta é a sua história.

Uma vulnerabilidade no sistema de ar condicionado do Cristo Rei, em Almada, permitia ter controlo remoto do sistema e colocar, por exemplo, a temperatura a 40 graus para incómodo dos visitantes. Um certo tipo de *web cam* chinesas de marca branca vendidas em Portugal permite que qualquer um tenha acesso remoto às imagens dessas câmaras, que podem ir de cafés, quartos com bebés, quintas ou bares de alterne. Uma vulnerabilidade na plataforma WinRest permitia gerir as faturas e pagar refeições em centenas de restaurantes.

Todas estas falhas em Portugal foram descobertas e reportadas pela empresa portuguesa BinaryEdge, gerida por dois portugueses, um em Zurique e outro em Londres, e alimentada por uma equipa de mais sete pessoas (até há alguns dias eram só mais três) que trabalha, de casa, entre Lisboa e o Algarve. A *startup* que, por obra de algum acaso, tem

sede na Suíça também já deixou alertas de fragilidades à Vodafone Portugal, NOS, a várias *startups* e a organizações estatais. Mas o trabalho desta *startup* criada em 2014 e comprada agora por uma empresa dos EUA vai muito além do país onde nasceu – na verdade nasceu na internet. "A plataforma que criámos permite que nós ou as pessoas que a usam consigam identificar e reportar ataques e vulnerabilidades a todo o tipo de empresas, pequenas ou grandes. Muitas delas figuram na lista dos Fortune 500". Quem o diz é Tiago Henriques, o fundador e CEO da Binary Edge e que tem o seu trabalho "de sonho", a partir do seu apartamento, em Zurique.

Existem 7,6 mil milhões de pessoas no planeta, mais de 4,3 mil milhões (57%) usa a internet. Em Portugal são 78% (8 dos 10,27 milhões). A BinaryEdge tem sido peça fulcral para expor, recentemente, algumas das maiores fugas de dados. Como exemplo, Tiago Henriques admite que "**um hacker tem um tanque e há empresas a responder com um pauzinho", como veremos de seguida.**

A ferramenta das últimas fugas de dados

Esta semana a empresa esteve em destaque em duas situações bem mediáticas. Primeiro porque foi a ferramenta que permitiu à gigante Microsoft ficar a saber que os dados de 250 milhões de clientes estavam expostos online – foi esta quinta-feira revelado. O investigador que descobriu a fragilidade num servidor do gigante tecnológico usou o serviço da *scan*, uma espécie de motor de busca, da BinaryEdge, para o conseguir.

Já em novembro a revista Wired noticiava que tinha sido descoberto um servidor que expunha online 1,2 mil milhões de registos – um total de 4 terabytes – com dados pessoais que envolviam endereços de e-mail, números de telefones e perfis no Facebook, Twitter ou LinkedIn. Esses registos expostos foram descobertos graças ao serviço de pesquisa da BinaryEdge e alimentaram durante uma década "usurpadores de identidade e burlões que

criaram um mercado negro online que agregava os dados pessoais para entrar em contas pessoais, roubar dinheiro ou a identidade de indivíduos".

Compra de milhões por um mundo mais seguro

Naquela que foi uma semana em cheio para a startup, foi também anunciada oficialmente a venda da BinaryEdge a uma empresa norte-americana especializada em seguros online, a Coalition. Embora os valores não sejam oficiais, pudemos perceber que foram vários milhões – "bem acima dos 10 milhões", que era "o valor mínimo que aceitava para ponderar vender" – que convenceram Tiago Henriques, sócio maioritário, a vender o seu bebé. "O Joshua Motta, CEO da Coalition, voou até Zurique para me convencer". E como o fez? Além do dinheiro, há uma ideia comum: "ele contou-me o seu plano secreto (*secret master plan*) e sentir que, juntos, podemos resolver o risco cibernético".

"Enquanto a Coalition tem uma força impressionante a nível negócio, são mesmo líderes em crescimento na área de seguros online e ciber risco nos EUA, nós temos a força tecnológica", admite o responsável. Embora toda a empresa tenha sido vendida, Tiago e os seus parceiros "no crime" Marco Silva e Florentino Bexiga, ficaram com ações da Coalition e são, agora, o braço tecnológico da empresa norte-americana, mantendo os serviços que já tinham antes. Tiago passou a ser *general manager costomer security* da Coalition, Marco mantém o cargo de CTO da BinaryEdge e a gerir a parte tecnológica.

"Agora queremos continuar a crescer e a ajudar empresas e pessoas a estarem mais seguras", admite Marco Silva, a partir de Londres, onde reside com a mulher e o filho. O motivo? "Porque adoro a cidade e posso trabalhar de qualquer lado no mundo – vou alternando entre casa, a biblioteca ou um *cowork*".

E como é que a startup norte-americana ficou interessada? "Estávamos com um crescimento brutal desde que lançámos há uns meses a versão pública do nosso motor de busca e temos também um portfólio de clientes empresariais bastante extenso e de empresas grandes. Além disso estávamos já a preparar uma segunda ronda de investimento e a Coalition era cliente há mais de um ano".

O objetivo, agora, é crescer a nível global com Coalition. **"Continuo a viver o meu sonho e acordo todas a manhãs motivado para trabalhar nesta área", admite Tiago Henriques**. Para já, a ideia é manter-se por Zurique, onde vive com a mulher. "A empresa está registada aqui até porque era onde tínhamos o nosso primeiro investidor, mas a nível de impostos também temos muitas vantagens cá", explica, indicando que a nível de reputação internacional "dá jeito" estar na Suíça, visto como país neutro. No entanto, dentro de três ou quatro anos quer voltar para Portugal. Já Marco quer manter-se na "vibrante" Londres, onde vive há cinco anos com a mulher e o filho de dois anos (já nasceu em Inglaterra), mas admite que o Brexit pode mudar essa perspetiva.

A equipa principal da BinaryEdge numa viagem aos EUA

E como tudo começou? Uma paixão chamada internet

Chegaram a ouvir profetas da desgraça vaticinar um falhanço rotundo para a empresa. "Chamaram-lhe uma ferramenta de *scanning* sem hipótese, mas nunca liguei ao mediatismo nem às críticas". Tiago Henriques tinha uma paixão e uma ideia de fazer melhor do que já existia no campo do registo dos dados na internet e assim nasceu a BinaryEdge.

Tiago é um algarvio de 31 anos que nasceu e estudou em Lagos e depressa saiu do país para estudar – tirou engenharia de software na Universidade Brighton (Inglaterra) e tirou mestrado em *computer forensics* em Bedfordshire. Marco Silva é um português nascido na África do Sul, que viveu desde que se lembra em Lisboa e que é mestre em engenharia de redes e telecomunicações – em curso tirado no Instituto Superior Técnico (pólo do Taguspark) – da equipa central da empresa faz ainda parte Florentino Bexiga, que trabalha a partir de Faro, em Portugal.

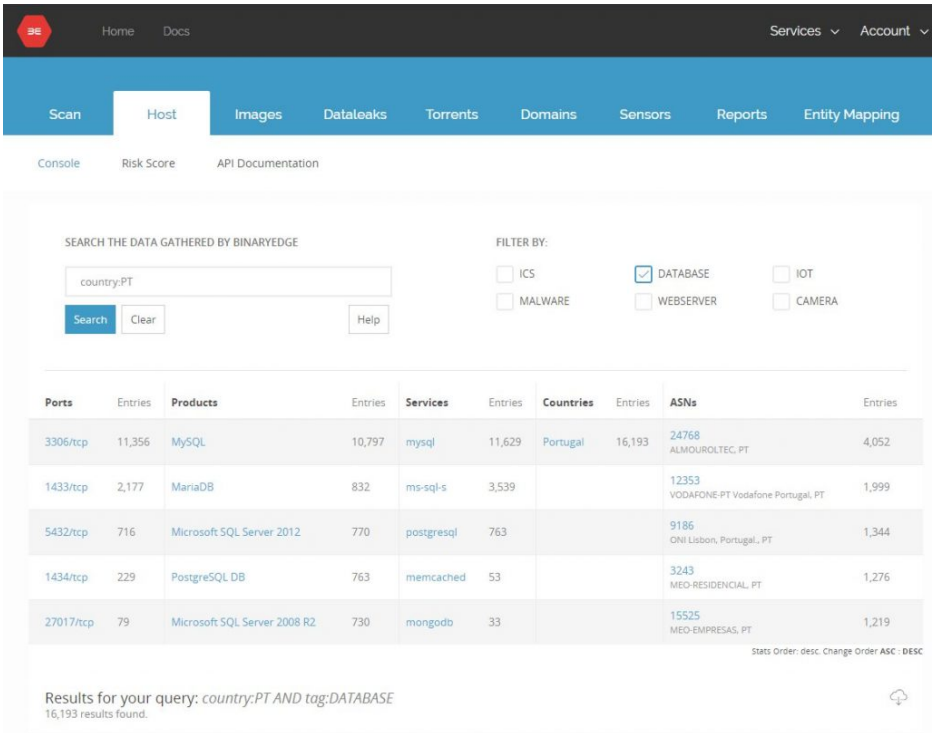
A ideia para a empresa começou a surgir em 2011, quando Tiago criou com alguns amigos uma equipa de investigação informática – PT Coresec – que tentava procurar dados expostos ou fugas de informação na internet. "Na altura tinha surgido um motor de busca nesta área chamado Shodan, mas tinha uma qualidade muito fraca dos dados obtidos e nós achávamos que conseguíamos fazer melhor". Fizeram um protótipo onde guardavam os dados dos chamados scans à internet, mas nada oficial.

Tiago e Marco conheceram-se numa conferência de cibersegurança. Mais tarde, Marco Silva partiu para a Suíça para trabalhar para uma fintech e convenceu Tiago a ir também.

Foi nesta altura que graças ao Codebits, conferência criada por Celso Martinho (agora CEO da BrightPixel), Tiago quis transformar a ideia de apenas uma equipa de segurança numa empresa oficial, que acabou por nascer em dezembro de 2014 – embora só tenha sido registada em abril de 2015. Cedo perceberam que seria difícil ter apoio financeiro em Portugal. "Quando começámos a procurar investimento em Portugal davam-nos 50 mil euros por 20% da empresa, mas na Suíça conseguimos rapidamente meio milhão de euros e, em setembro de 2015, já tínhamos o dinheiro que precisávamos", explica Tiago.

Inicialmente criaram uma versão básica e privada do motor de busca para conseguirem alguns clientes. Isto permitiu começar a expandir algumas das funcionalidades da plataforma que antes não existiam, enquanto já eram pagos por clientes. Continuam nesse mesmo processo até agosto de 2018, altura em que abriram ao público uma versão limitada da plataforma, e na qual têm hoje mais de 15.000 utilizadores.

Para já, têm dois tipos de conta para utilizadores individuais, uma gratuita com número muito limitado de pesquisas e a versão paga onde é possível comprar créditos que permitem um certo número de pesquisas. Depois há o serviço para empresas, que é bem mais restrito. "Esse serviço tem certas funcionalidades que podiam ser usadas por atores maliciosos e, por isso, não permitimos que qualquer um use", alerta Tiago Henriques. Para isso analisam com cuidado as empresas candidatas a esse tipo de conta. "Vemos se são fiáveis, como usam os dados e fazemos um contrato com eles que remete a responsabilidade legal do uso da informação recolhida para eles".



Print screen da plataforma da BinaryEdge onde estão expostas as vulnerabilidades em servidor da Microsoft

Explicador: E o que fazem mesmo?

O mundo da cibersegurança pode parecer chinês para a maioria dos 4,3 mil milhões de utilizadores de internet. Mas é possível recorrer a exemplos para explicar o conceito do que a BinaryEdge faz: "imaginem que a internet é uma estrada com prédios dos dois lados, nós somos o fotógrafo atento às fechaduras e janelas que tira fotos **240 vezes por mês a toda a internet**". Por outras palavras, a BinaryEdge é um Google da Cibersegurança com esteróides. Enquanto o motor de busca da Google visita todas as páginas da internet e guarda uma cópia para se puder fazer a pesquisa indexada, "nós visitamos todos os endereços de IP da internet, vemos os serviços ativos, dispositivos ligados, endereços de email ou páginas web com sessões a funcionar e vemos o que está a correr por ali".

E o que é isso permite? É essa informação que abre a porta para os utilizadores "treinados" verem vestígios de vulnerabilidades, ou seja, as empresas ficam a perceber onde estão frágeis ou que servidor ou até funcionário está a expor dados de forma perigosa. Daí surgem os vários alertas a instituições, empresas ou até indivíduos.

A acrescentar a esse serviço inicial, a startup tem ainda um serviço para as empresas que permite perceber quem está a atacar, que tipo de ataque é e que máquinas em concreto estão infectadas. "Conseguimos ajudar a indicar que servidores são maliciosos".

É dessa forma que utilizadores que usam o motor de busca têm conseguido encontrar várias vulnerabilidades de proporções épicas, isto porque a equipa da BinaryEdge não consegue explorá-las a todas – embora esteja atenta. "O *scan* é feito a **4,2 mil milhões de endereços de IP**, há muito para analisar e encontrar e é aí que a nossa comunidade de 15 mil utilizadores entra. Usam a plataforma e é possível, assim, notificar as organizações do que está ou foi exposto".

Fragilidades (e falta de cuidado) no mundo atual

Marco e Tiago têm uma certeza, enquanto os hackers vão evoluindo, a maioria das empresas nem por isso. "Não vejo que haja mais ou menos ameaças na internet nesta altura. É como uma onda, há picos de vulnerabilidades em certas alturas do ano e formas de ataque novas que vão sendo tratadas". O que preocupa Marco Silva é que "a ciber higiene das empresas é muito fraca, com grandes bases de dados sem estarem protegidas sequer por uma simples password, ficando expostas para a internet". Além disso "há uma **despreocupação incrível para com os dados dos utilizadores**".

A higiene básica de segurança é o maior problema das empresas, admite, porque continuam com níveis de cibersegurança "da antiguidade". Mesmo colaborações com governos é "difícil", "porque o processo de reportar uma brecha é demorado, muitos processos são manuais e até que consigam ver quem está exposto e acabar com a fragilidade é uma eternidade".

Daí que Tiago dê a metáfora: "**um hacker tem um tanque e há empresas a responder com um pauzinho".** As vulnerabilidades mais comuns mesmo em grandes empresas, como as do *ranking* Fortune 500 está mais relacionada com a gestão das máquinas. "É o chamado *shadow IT*, as empresas acumulam endereços IP e máquinas de

que se esquecem, ou um funcionário usou de forma leviana dados em processos internos ligados à nuvem e, sem ninguém perceber, abrem a porta a brechas (*leaks*)". Um dos exemplos mais típicos é quando existem aquisições de empresas, em que "o processo de passar as máquinas para os novos processos deixa também muitos dados expostos". "E isto acontece tanto em empresas gigantes com milhões para a segurança como em startups novas", garante Marco Silva.

"São *web cams* ligadas à internet, sem passwords ou usernames, completamente desprotegidas e onde é possível ver o que elas captam"

Espiar à distância: Portugal também é afetado

Em Portugal já notificaram desde startups, a empresas como Vodafone ou NOS, bem como várias organizações estatais. No caso do Estado português e dos problemas descobertos aí têm uma vantagem face a denúncias em outros países, já que conhecem várias pessoas do Centro Nacional de Cibersegurança (e não só) e reportam as fragilidades de forma direta e sem burocracias. "Não sabemos como poderia funcionar sem termos este acesso direto", admite Tiago Henriques.

Além do caso do ar condicionado dentro do Cristo Rei de que já falámos, exposto a qualquer pessoa com acesso à internet, um dos casos mais difíceis de reportar que descobriram em Portugal foi o de câmaras – *web cams* – de uma marca branca chinesa, expostas a uma invasão da privacidade preocupante. "São *web cams* ligadas à internet, sem passwords ou usernames, completamente desprotegidas e onde é possível ver o que elas captam", explica Tiago. O problema destes produtos comprados por famílias e não por empresas é que torna o processo de denúncia "muito difícil". Vimos quintas onde alguém alimentava os porcos, quartos com bebés e até negócios privadas desprotegidos", admite Mário Silva.

Num dos casos, uma câmara exposta de um café permitia ver parte da rua de Lisboa onde ficava e, através do Google Maps, puderem descobrir e avisar o estabelecimento em causa. Os IP destas câmaras só permitem ver a cidade onde estão ou que é um serviço de internet da NOS ou da Altice. "Não temos como reportar, porque mesmo se denunciássemos a situação aos fornecedores de ligações de internet, são tantos os endereços IP que eles não teriam a escala necessária para encontrar os visados", diz.

No caso da WinRest, uma plataforma de gestão de pagamentos focada nos restaurantes, uma vulnerabilidade permitia gerir de forma remota faturas, apagá-las ou mesmo pagar contas (sem fazer qualquer pagamento). "No limite alguém podia ir a esse restaurante, comer e pegar no telemóvel para colocar a conta como paga na plataforma", admite Tiago Henriques. Apesar da denúncia feita e de ter havido melhorias, atualmente indicam que ainda existem 26 restaurantes expostos.

Smartphones e colunas inteligentes vulneráveis

No duelo iOS contra Android, Tiago Henriques explica-nos que, teoricamente os iPhone e o sistema operativo iOS é mais seguro do que o Android, "isto porque se vê mais vulnerabilidades em Android". "Não só o Android é mais vulnerável, como a lojas de apps

da Google tem um controlo das apps lá publicadas mais reduzido, comparado com a Apple", admite.

Isso mesmo é o que permite que "atores maliciosos publiquem lá apps" que recolhem dados indevidamente "e/ou dão controlo a certas ferramentas do telefone (como a câmara) muito mais facilmente".

Já sobre as vulnerabilidades das famosas colunas inteligentes da Amazon ou Google (ou outro tipo de aparelhos da chamada Internet das Coisas que, cada vez mais, ficam disponíveis para as casas), tem uma opinião diferente. "Não costumam estar diretamente expostas a ataques porque não expõem serviços abertos para a internet". Apesar disso, "há outras marcas com menos controlo e que podem permitem acesso facilitado às colunas", ou seja, podem tornar possível espiar casas alheias. Mas nesta era digital ninguém está imune e Tiago admite que "já houve vários problemas de privacidade com a Amazon e Google, "nas quais se veio a saber que colaboradores internos conseguiam ouvir gravações das colunas".