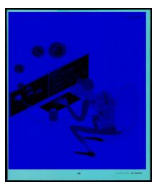


— INOVAR

Hackers de elite

São portugueses e estão entre os melhores do mundo a encontrar falhas de segurança informática, incluindo em grandes empresas como a Uber, Google e Yahoo. Os caçadores de *bugs*, como são chamados, ajudam as empresas a proteger os utilizadores dos criminosos e chegam a receber recompensas de dezenas de milhares de euros. A cotação dos investigadores está em alta e um deles até já ganhou um óscar da cibersegurança.

— Por **Rui da Rocha Ferreira** e ilustração de **Luís Mestre**

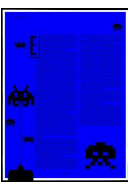


ID: 77422507

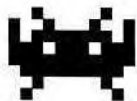
28-10-2018

— INOVAR





— INOVAR



Eram três da manhã em Las Vegas, EUA, quando Miguel Regala começou a receber mensagens de parabéns de outros *hackers*. Não fazia anos – era o resultado de um ataque que tinha feito. Minutos antes, tinha entrado numa aplicação da Uber através de uma falha que encontrara.

Permitia-lhe alterar as informações do perfil de empresas e foi o que fez. Mudou o nome da vítima para “Fisher esteve aqui”, uma alcunha pela qual é conhecido *online*.

“Escolheram o meu relatório como um dos melhores do dia, pagaram-me um bónus e convidaram-me para falar sobre como explorei a vulnerabilidade”, recorda o portuense de 28 anos.

Miguel Regala não estava a cometer qualquer ilegalidade, estava sim a cumprir o desafio para o qual tinha sido convidado pela HackerOne, a mais conhecida das plataformas que permitem recrutar *hackers* para resolver problemas de segurança. “Estás a ‘lutar’ contra os melhores peritos. E para lutares, tens de estar ao nível deles.”

O perfil da empresa que invadiu era de testes, mas podia perfeitamente ter sido o de qualquer cliente desta nova *app*, da área da saúde, da Uber.

Atualmente a viver em Gaia, Miguel Regala deixou há mais de um ano o emprego fixo para dedicar-se à caça de *bugs*. Ainda não o faz a tempo inteiro porque “como és pago por cada *bug* que encontras, se não encontras, não recebes”. “Muito facilmente pode tornar-se um ciclo negativo e pode ser assustador para quando se está a começar ou não se tem experiência” – conta.

Mas é uma atividade que também pode ser extremamente lucrativa. Miguel Regala não revela o valor das recompensas que recebe. “Não vês um médico a terminar uma operação e a dizer ‘acabei de ganhar 12 mil euros, bravo!’ Mas posso dar um exemplo muito bom, em que tivemos um colega norte-americano que, há cerca de um mês, fez num dia 121 mil euros.” Encontrou 14 falhas que lhe renderam, em média, 8600 euros cada.

É preciso saber pôr os valores em perspetiva: depende muito de quem paga; da gravidade da falha encontrada; se aquele sistema já foi testado e do tempo despendido para encontrar o *bug*. O que permite perceber que a vulnerabilidade encontrada por André Batista na empresa Shopify era muito grave: ganhou 21 500 euros por uma série de problemas que denunciou.

“Conseguia redirecionar pagamentos para a minha conta, se fosse preciso. Se uma pessoa mal intencionada descobrisse aquilo, o prejuízo que não dava ao Shopify”, questiona o jovem de 24 anos, que teve a ajuda de um amigo neste *bug*.

Natural de Coimbra, André Batista sempre foi um curioso por computadores e não foi preciso muito até perguntar “como é que seria possível entrar no computador de outra pessoa”.

Conta que foi esta “curiosidade, de ultrapassar limitações de forma criativa”, que lhe deu a dedicação que tem e o fez chegar onde está. O nome André Batista pode até ser-lhe familiar: foi coroado como o *hacker* mais valioso do mundo, em março, depois de ter vencido uma das competições da HackerOne. “Desde que ganhei o concurso, ganhei mais o bichinho [da caça ao *bug*].”

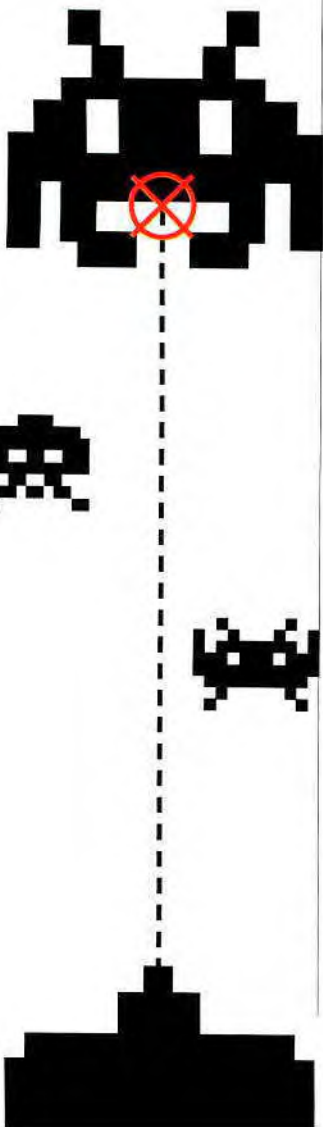
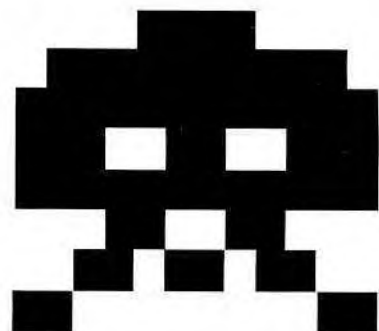
E o que pensam os pais do filho que vai quase todos os meses para o estrangeiro testar as defesas de diferentes empresas? “No início foi um pouco esquisito, mas estiveram sempre muito orgulhosos do meu trabalho e perceberam rapidamente o que fazia. Quando fui para o mestrado disse que gostava disto e eles perceberam.”

O futuro parece promissor: André já está a dar aulas como professor convidado no mestrado de Segurança Informática na Faculdade de Ciências da Universidade do Porto.

Não é o único a quem se augura grandes feitos no mundo do *hacking*. Com apenas 22 anos, Federico Bento já ganhou um *punie*, prémio mais relevante do mundo nesta área. Equivalente ao óscar dos *hackers*, o português arrematou o título de feito épico em 2017.

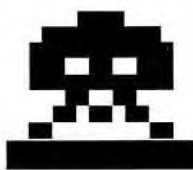
“Um utilizador de uma máquina Linux que não tivesse privilégios, conseguia ter privilégios de superutilizador.” Ou seja, ganhava acesso a toda a máquina. “Senti-me mesmo bem, é o reconhecimento de algo que fizeste.” “Não é algo que defina as pessoas, não sinto que sou o melhor *hacker* do mundo só por ganhar um *punie*, tenho muito para aprender.”

Federico Bento também mostrou que aquela falha não foi sorte de principiante: neste ano vol-





— INOVAR



tou a estar nomeado para os *pwnie* na categoria de melhor falha de escalonamento de privilégios, mas acabaria por perder a corrida para o Meltdown, uma das maiores falhas de segurança informática alguma vez descobertas e que afetou, virtualmente, todos os equipamentos com processadores fabricados nos últimos 20 anos.

O interesse por este mundo dos *bugs* começou aos 15 anos e tudo graças ao cinema. Em particular, a uma cena do filme *Matrix Reloaded*, em que a personagem Trinity ganha acesso a uma rede de energia e desliga todas as luzes de uma cidade. “Gostei mesmo. Tive interesse e comecei a pesquisar como é que se faziam certas coisas.”

Federico é, à semelhança dos outros entrevistados, um *self-made hacker*, pois encontrou *online* os materiais disponíveis para aprender o que queria sobre segurança informática. Mas em vez de participar em programas de caça aos *bugs*, fá-lo mais “por iniciativa própria”.

Mesmo a solo, consegue ganhar algum dinheiro. O *bug* do óscar dos *hackers* afetava também um *software* da Google. Submeteu a falha, a tecnológica validou e deu-lhe 450 euros. “Ainda estou a estudar, não gosto muito de encontrar *bugs* por dinheiro, é mais por gosto próprio.”

Apesar de ainda não olhar muito para o futuro, Federico sabe que poderá ter de passar pelo estrangeiro. “Aqui em Portugal não sei se há muito emprego [em exploração de falhas].”

Quem já está fora de Portugal há três anos é Duarte Silva. O investigador está na Holanda, onde trabalha para uma grande organização internacional. “Em Portugal já estava a trabalhar na área de cibersegurança. Mas não havia evolução de carreira, era muito parado.”

Quando teve o primeiro contacto com a caça aos *bugs*, através da plataforma BugCrowd, que funciona de forma semelhante à HackerOne, Duarte não ficou muito convencido. “Um ano e meio depois resolvi visitar as *bug bounties*. Na altura já havia muitos mais programas e foi aí que ganhei bastante interesse.” Diz que tem andado de volta do *router* Technicolor que tem lá em casa e que milhares de outras pessoas usam na Holanda, pois é dado pelo fornecedor de internet. “Tenho estado a descobrir falhas e a reportar.”

Na opinião deste especialista de 33 anos, natural do Montijo, o sucesso dos portugueses na caça aos *bugs* justifica-se por esta ser “uma das gerações mais bem formadas em Portugal” e pela muito falada capacidade de desenrascar do povo português. “Improvisar é uma capacidade que é muito boa para os *bugs* e nós temos um dom.”

Joe Sechman, vice-presidente de entrega de testes de penetração da Cobalt, outra plataforma

Um estudo da BugCrowd (2016) diz que os portugueses descobrem falhas mais críticas, o que lhes dá mais reputação e dinheiro.

de caça ao *bug*, atesta a qualidade portuguesa. “Nos últimos dois anos, Portugal cresceu e tem agora a terceira maior concentração de investigadores no núcleo da Cobalt e quase um quarto dos lugares na nossa administração de conselheiros de pesquisa”, disse, por *e-mail*.

“É importante mostrar o que se faz de bem em Portugal e o respeito que temos lá fora”, refere por seu lado David Sopas, visto como um dos precursores da caça ao *bug* em Portugal. Na sua lista de “vítimas” estão nomes como Yahoo, Yelp, *The New York Times*, Zomato e até o Departamento de Defesa dos EUA (“era uma base de dados militares reformados”, explica).

“Para um país pequeno, com poucos profissionais na área, ter o impacto que temos no mundo dos *bugs*, acho fantástico. E tem tendência a melhorar, pois motiva e ensina outros jovens.”

O também cofundador da Char49 explica que em muitos casos encontrar a falha não chega. “É importante entregar um bom relatório ou um vídeo a explicar passo-a-passo como lá chegaste, a tua linha de raciocínio, como resolver, testar novamente quando eles resolverem. Esses por menores valorizam o próprio *bug*.”

Nascido no Luxemburgo, onde os pais eram emigrantes, regressou ainda novo para Portugal. Agora, a viver na Figueira da Foz, conta com relatório de mais de 600 falhas identificadas em diferentes programas de caça ao *bug*. “A tua própria reputação está em jogo, por isso tentava sempre encontrar as falhas mais graves.”

David Sopas e companhia são alguns dos elementos que nos últimos anos têm ajudado a construir aquela que é uma elite de *hackers* portugueses, com fama internacional.

