SANDWORM

UMA NOVA ERA NA GUERRA CIBERNÉTICA E A CAÇA PELOS HACKERS MAIS PERIGOSOS DO KREMLIN

ANDY GREENBERG

ALTA BOOKS
EDITORA
Rio de Janeiro, 2021

SUMÁRIO

PARTE I

EMERGÊNCIA

Utilize os primeiros momentos para estudar. Você pode perder oportunidades de vitória rápida dessa maneira, mas os momentos de estudo são segurança de sucesso. Leve o tempo necessário e esteja certo.

1

O ZERO-DAY

Além da cúpula do governo federal norte-americano, onde o complexo industrial de inteligência da capital norte-americana se estende até um mar infinito de estacionamentos e prédios comerciais cinza marcados com logos e nomes corporativos pensados para serem esquecidos, há um prédio em Chantilly, Virginia, cujo quarto andar abriga uma sala interna sem janelas. As paredes da sala são pintadas de preto fosco, como se quisessem esculpir um espaço negativo onde nenhuma luz externa penetraria.

Em 2014, pouco mais de um ano antes do início da ciberguerra da Ucrânia, essa era o que a pequena empresa de inteligência privada iSight Partners chamava de sala escura. Nela trabalhava a equipe de dois homens responsável pela pesquisa de vulnerabilidade de software, um trabalho que exigia foco intenso o suficiente para que os funcionários insistissem no desenho de um escritório o mais próximo possível de uma câmara de privação de sentidos.

Foi essa dupla altamente qualificada de habitantes de cavernas que John Hultquist primeiro chamou em uma quarta de manhã naquele mês de setembro, com um pedido raro. Quando Hultquist chegou à sua mesa mais cedo naquele dia, em um escritório muito mais iluminado, uma sala com janelas no lado oposto do prédio da iSight, ele abriu um e-mail do chefe das equipes de coleta de inteligência internacional da iSight, Jason Passwaters. Passwaters havia descoberto uma intrigante amostra de malware que parecia ter sido tirada de um computador na Ucrânia. No e-mail de Passwaters, Hultquist encontrou um presente: seu colega da iSight acreditava que eles haviam colocado as mãos em uma vulnerabilidade de zero-day.

Um zero-day, no jargão hacker, é uma falha secreta de segurança no software, uma falha que a empresa responsável por criar e manter o código do software não conhece. O nome vem do fato de que a empresa teve "zero dias" para responder

e lançar um pacote de atualização para proteger os usuários. Um zero-day poderoso, em particular um que permita ao hacker quebrar os limites do software no qual o bug se encontra e executar seu próprio código em um computador-alvo, pode servir como um tipo de chave mestra global — um passe livre para obter acesso a qualquer máquina que opere aquele software vulnerável, em qualquer parte do mundo onde a vítima esteja conectada à internet.

O arquivo que veio da equipe internacional da iSight para Hultquist era um anexo de PowerPoint. Parecia conseguir executar exatamente esse tipo de código e no Microsoft Office, um dos programas mais ubíquos do mundo.

Enquanto lia o e-mail, Klaxons soava na mente de Hultquist. O arquivo PowerPoint já havia sido analisado pela equipe técnica da iSight em Taiwan, e se a descoberta era o que os analistas taiwaneses acreditavam que poderia ser, isso significava que alguns hackers desconhecidos possuíam — e haviam utilizado — uma habilidade perigosa que lhes permitiria sequestrar contas de milhões de computadores. A Microsoft precisava ser avisada dessa falha imediatamente, mas, em um sentido de interesse próprio, descobrir um zero-day representava um marco para uma empresa pequena como a iSight, que esperava ganhar a glória e atrair clientes na florescente subindústria de segurança de "inteligência contra ameaças". A empresa descobria apenas duas ou três falhas secretas assim por ano. Cada uma era um tipo de curiosidade altamente perigosa e meio abstrata e um golpe de pesquisa significativo. "Para uma empresa pequena, encontrar uma pérola como essa foi muito, muito gratificante", diz Hultquist. "Foi de imensa importância para nós."

Hultquist, um veterano do exército grande e expansivo do leste do Tennessee, com uma barba preta espessa e um sorriso perene, fazia questão de gritar periodicamente de sua mesa para uma sala ao lado, conhecida como cercado, um modelo organizacional em que diversos profissionais trabalham juntos em uma mesma área aberta. Um lado desse espaço estava alinhado com especialistas em malware e o outro, com analistas de ameaças focados em entender os motivos geopolíticos por trás de ataques digitais. Assim que Hultquist leu o e-mail sobre a amostra de malware da Ucrânia, ele correu para fora do escritório em direção ao cercado, apresentando o problema à sala e atribuindo tarefas para a triagem do que seria, sem que ninguém ali ainda soubesse, uma das maiores descobertas na história da pequena empresa.

Mas foi na outra ponta do corredor, na sala escura, que os monges hackers que a habitavam começariam a entender o significado da descoberta da iSight: uma pequena e oculta maravilha de engenharia maliciosa.

■

Trabalhando em computadores cujos monitores brilhantes serviam como única iluminação da sala, os engenheiros reversos começaram a rodar o arquivo PowerPoint infectado pelo malware repetidas vezes dentro de uma série de máquinas virtuais — simulações efêmeras de um computador abrigadas dentro de um computador físico real, cada uma delas isolada do resto da máquina como a sala escura era isolada do resto dos escritórios da iSight.

Nesses compartimentos isolados, o código poderia ser estudado como um escorpião atrás do vidro de um terrário. Ele permitiria que as vítimas virtuais se infectassem repetidamente, enquanto os engenheiros de reversão teciam simulações de máquinas digitais diferentes, executando versões variadas do Windows e do Microsoft Office, para estudar as dimensões e flexibilidade do ataque. Quando determinaram que o código poderia se extrair do arquivo PowerPoint e ganhar controle total até das versões mais atualizadas do software, eles tiveram a confirmação: era de fato um zero-day, tão raro e poderoso quanto o analista taiwanês havia suspeitado. Ao final da tarde — uma passagem de tempo que ocorreu quase despercebida dentro daquele espaço de trabalho —, eles haviam produzido um relatório detalhado para compartilhar com a Microsoft e seus clientes e codificaram a sua própria versão, reescrevendo-a em uma prova de conceito que demonstrava o ataque como um patógeno em um tubo de ensaio.

O PowerPoint possui "poderes incríveis" — como um dos dois engenheiros de reversão da sala escura, Jon Erickson, me explicou. Ao longo de anos de evolução, o programa se tornou uma máquina de Rube Goldberg cheia de recursos, na maior parte desnecessários, tão intrincada que praticamente serve como sua própria linguagem de programação. E a pessoa responsável por explorar esse zero-day havia estudado profundamente um recurso que permitia a qualquer um incluir um "objeto" de informação dentro da apresentação, como um gráfico ou vídeo puxado de outro lugar no pacote de dados do arquivo PowerPoint, ou até mesmo de um computador remoto na internet.

Nesse caso, os hackers haviam usado o recurso para plantar cuidadosamente dois pacotes de dados dentro da apresentação. O primeiro foi carregado em uma pasta temporária no computador-alvo. O segundo se aproveitou do recurso de animação do PowerPoint: animações do PowerPoint não apenas permitem que palestrantes entediem a plateia com texto em movimento ou desenhos, mas executam comandos no computador em que a apresentação está rodando. Nesse caso, quando a apresentação carregasse aquele arquivo de animação, deflagraria um script automático para clicar com o botão direito no primeiro arquivo da apresentação que havia sido plantado na máquina e escolheria "instalar" no menu, dando ao código uma base de apoio no computador sem que o usuário soubesse. O resultado era como um pacote aparentemente inofensivo deixado na sua porta que, após ser levado para dentro, faz brotar um braço, se abre e li-

bera minúsculos robôs na sua lareira. Tudo isso aconteceria imediatamente e de modo invisível, no instante em que a vítima clicasse duas vezes no anexo para abri-lo.

Erickson, o engenheiro de reversão que lidou primeiro com o zero-day na sala escura da iSight, se lembra do trabalho desmontando e desarmando o ataque como um evento um tanto quanto raro e fascinante, mas totalmente impessoal. Em sua carreira, ele havia lidado apenas com um punhado de zero-days reais encontrados ao acaso. Mas ele havia analisado milhares de outras amostras de malware e havia aprendido a pensar nelas como espécimes para estudo sem considerar o autor por trás delas — o humano que havia construído sua maquinaria tortuosa. "Era só algum cara desconhecido e alguma coisa desconhecida que eu nunca tinha visto", afirmou.

Mas zero-days têm autoria. E quando Erickson começou a desmembrar esse em sua oficina escurecida naquela manhã, ele não estava simplesmente estudando um quebra-cabeças inanimado e natural. Ele estava admirando as primeiras pistas de uma inteligência malévola e remota.

2

BLACKENERGY

Assim que o frenesi inicial da iSight ao redor da descoberta do zero-day diminuiu, ficaram as perguntas: quem havia escrito o código de ataque? Em quem eles estavam mirando o código e por quê?

Essas questões caíram sobre Drew Robinson, um analista de malware na iSight que John Hultquist descreveu como "andarilho do dia": Robinson possuía a maioria das habilidades de engenharia reversa da equipe de vampiros da sala escura, mas sentava-se no cercado ensolarado ao lado do escritório de Hultquist, responsável por uma análise de ângulo muito maior de campanhas de hacking, do pessoal que as executava até suas motivações políticas. O trabalho de Robinson seria seguir as pistas técnicas dentro do PowerPoint para resolver os mistérios maiores da operação oculta que elas representavam.

Minutos depois de Hultquist entrar no cercado para anunciar a descoberta de prioridade máxima do zero-day do PowerPoint naquela manhã de quarta-feira, Robinson estava se debruçando sobre o conteúdo da armadilha do anexo. A apresentação parecia ser uma lista de nomes escritos em caracteres cirílicos sobre uma bandeira ucraniana azul e amarela, com uma marca d'água do brasão de armas ucraniano, um tridente azul-claro sobre um escudo amarelo. Aqueles nomes, Robinson descobriu depois de usar o Google Tradutor, eram uma lista de supostos "terroristas" — aqueles que ficaram do lado da Rússia no conflito ucraniano que havia começado no início do ano, quando tropas russas invadiram o Leste do país e a península da Crimeia, inflamando movimentos separatistas e deflagrando uma guerra em curso.

A escolha dos hackers por uma mensagem anti-Rússia para carregar sua infecção de zero-day foi a primeira pista para Robinson de que o e-mail deveria ser uma operação russa com alvos ucranianos, jogando com o patriotismo do país e os medos de simpatizantes internos no Kremlin. Mas, enquanto ele procurava

pistas sobre os hackers por trás do estratagema, logo descobriu outro fio solto para puxar. Quando o zero-day do PowerPoint executava, o arquivo baixado no sistema da vítima revelou ser uma variante de um pedaço de um malware notório, que logo seria ainda mais notório. Era chamado BlackEnergy.

A história curta do BlackEnergy até aquele momento já continha, em algum sentido, sua própria introdução sobre a taxonomia de operações hackers comuns, dos "script kiddies" mais baixos — hackers tão sem habilidade que só poderiam utilizar ferramentas escritas por alguém com mais conhecimento — até cibercriminosos profissionais. A ferramenta foi criada originalmente por um hacker russo chamado Dmytro Oleksiuk, também conhecido pela alcunha Cr4sh. Por volta de 2007, Oleksiuk tinha vendido o BlackEnergy em fóruns russos de hackers, custando em torno de US$40, com sua alcunha destacada como um grafite no canto do painel de controle.[1]

A ferramenta foi criada para um único propósito rápido: o chamado ataque de negação de serviço, ou DDoS, ataques planejados para inundar sites com pedidos fraudulentos por informação de centenas ou milhares de computadores simultaneamente, derrubando-os do ar. Infecte a máquina de uma vítima com BlackEnergy e ela se torna membro de uma botnet, uma coleção de computadores sequestrados, ou bots. Um operador de botnet poderia configurar o software de uso fácil de Oleksiuk para controlar qual alvo suas máquinas escravizadas encheriam de pedidos falsos, assim como o tipo e o ritmo desse bombardeio digital.

Ao final de 2007, a empresa de segurança Arbor Networks contou mais de trinta botnets construídas com BlackEnergy, a maioria mirando seus ataques em sites russos.[2] Mas, no espectro de sofisticação de ciberataque, ataques de negação de serviço eram, em sua maioria, brutos e cegos. Afinal de contas, eles poderiam causar quedas de serviço dispendiosas, mas não os vazamentos de dados sérios infligidos por técnicas de hacking mais penetrantes.

Nos anos seguintes, porém, o BlackEnergy evoluiu. Empresas de segurança começaram a detectar uma nova versão do programa, agora equipado com um arsenal de recursos intercambiáveis. Essa versão renovada da ferramenta ainda poderia atingir sites com tráfego falso, mas também poderia ser programada para enviar spam por e-mail, destruir arquivos nos computadores infestados e roubar nomes de usuário e senhas de bancos.*

* Conforme usos cibercriminosos mais sofisticados do BlackEnergy se espalharam, seu criador original, Oleksiuk, tomou cuidado para se distanciar disso — sobretudo depois de o BlackEnergy ser conectado a uma fraude financeira contra bancos russos, uma jogada perigosa em um país conhecido por ignorar quando cibercriminosos focavam vítimas ocidentais. "O fato de que o código-fonte estava disponível para tantas pessoas em todo tipo de lugar (semi) privado pode significar que alguém o pegou para suas próprias necessidades", Oleksiuk tentou explicar em uma publicação

Agora, diante dos olhos de Robinson, o BlackEnergy havia reemergido em mais um formato diferente. A versão que ele estava observando do seu assento no cercado da iSight parecia diferente de todas que ele havia lido antes — certamente não era uma simples ferramenta de ataque a sites, e também não deveria ser uma ferramenta de fraude financeira. Afinal, por que um esquema de cibercrime focado em fraude estaria usando uma lista de terroristas pró-Rússia como isca? O ardil parecia ter um alvo político. A partir da primeira olhada na amostra do BlackEnergy ucraniano, ele começou a suspeitar que estava olhando para uma variante do código com um novo objetivo: não o simples crime, mas a espionagem.*

Logo depois, Robinson começou a seguir outra pista de Passwaters, o chefe das equipes de inteligência internacionais que primeiro encontraram o zero-day do PowerPoint, uma pista que revelaria algo a mais sobre o propósito do malware. Quando Robinson rodou essa nova amostra de BlackEnergy em uma máquina virtual, ela tentou se conectar pela internet a um endereço de IP em algum lugar na Europa. Aquele endereço de IP pertencia a um servidor de comando e controle que funcionava como o mestre de marionetes remoto do programa. E quando o próprio Robinson se conectou através de seu navegador a essa máquina distante, ficou espantado ao ver que ela havia sido deixada sem proteção alguma. Qualquer um poderia vasculhar seus arquivos.

Os arquivos incluíam, por incrível que pareça, um tipo de documento de ajuda para essa versão única do BlackEnergy que convenientemente listava seus comandos. Isso confirmou as suspeitas de Robinson: a versão entregue de zero-day do BlackEnergy possuía uma matriz de habilidades de coleta de dados muito maior do que a amostra comum de malware encontrada em investigações de cibercrimes. O programa poderia tirar screenshots, extrair arquivos e chaves de criptografia das máquinas das vítimas e gravar teclas pressionadas, tudo isso uma marca de ciberespionagem meticulosa e com alvo certo em vez de uma extorsão por fraude bancária motivada por lucro.

intitulada "Fuck Me I'm Famous", no blog LiveJournal em 2009. "Para suspeitar que o autor desse programa de bot, cuja assinatura estava escrita em versões públicas há três anos, está envolvido em maquinações criminosas, você teria que ser um completo idiota."

* Inclusive, analistas de segurança na empresa de segurança Kaspersky suspeitavam em silêncio de que alguém estivesse usando o BlackEnergy para espionagem sofisticada desde o começo de 2013. Versões da ferramenta que não eram mais oferecidas para compra nos fóruns hacker começaram a aparecer, e algumas eram criadas para infectar máquinas que rodavam Linux – um sistema operacional raro o suficiente que os hackers deveriam estar usando para operações de espionagem precisas, e não roubo indiscriminado. "O uso de crimeware havia ido embora", disse-me a analista Maria Garnaeva, da Kaspersky. "Foi nessa hora que os hackers, usando isso, se tornaram um grupo de ataque com alvo distinto."

Mas ainda mais importante do que os conteúdos daquele arquivo explicativo era a linguagem em que ele estava escrito: em russo.

3

ARRAKIS 02

A indústria de cibersegurança avisa constantemente sobre o "problema de atribuição" — em que os hackers por trás de qualquer operação, especialmente as mais sofisticadas, distantes, são muitas vezes impossíveis de localizar. A internet oferece muitas oportunidades para proxies, desvios de direção e uma incerteza geográfica esmagadora. Mas, identificando o servidor de comando e controle desprotegido, Robinson havia rompido o mistério da BlackEnergy da iSight com um detalhe raro de identificação. Apesar de todo o cuidado que mostraram no hacking do PowerPoint, os hackers pareciam ter deixado escapar uma pista concreta de sua nacionalidade.

Mas, depois daquela sorte inesperada, Robinson ainda tinha a tarefa de mergulhar nas entranhas do código do malware em busca de mais pistas e, também, para criar uma "assinatura" que empresas de segurança e clientes da iSight pudessem usar a fim de detectar se outras redes haviam sido infectadas com o mesmo programa. Decifrar a funcionalidade do código do malware não seria nem um pouco fácil como foi rastrear o servidor de comando e controle. Como Robinson aprenderia meticulosamente ao longo dos próximos dias de trabalho duro e estafante, o código havia sido embaralhado por inteiro com três camadas alternadas de compressão e criptografia.

Em outras palavras, desvendar os segredos do malware era um tipo de caça ao tesouro. Apesar de Robinson saber que o malware era autônomo e, portanto, deveria incluir todas as chaves de criptografia necessárias para se desembaralhar e rodar seu código, a chave de cada camada desse processo só poderia ser encontrada depois de decodificar a camada superior. E, mesmo depois de adivinhar o algoritmo de compressão que os hackers haviam utilizado, ao fazer uma varredura do ruído aparentemente aleatório em busca de padrões reconhecíveis, Robinson ainda passou dias trabalhando para identificar o esquema de crip-

tografia que eles usaram — uma modificação única de um sistema existente. Enquanto se embrenhava cada vez mais fundo no quebra-cabeça, ele olhava de sua mesa e descobria que horas haviam se passado. Mesmo em casa, ele se encontrava em pé, absorto no chuveiro, revirando o código na cabeça repetidas vezes.

Quando finalmente quebrou aquelas camadas de ofuscação após uma semana de tentativa e erro, Robinson foi recompensado com a visão dos milhões de zeros e uns da amostra do BlackEnergy — uma coleção de dados que era, em uma primeira olhada, ainda totalmente sem sentido. Afinal, este era o programa em sua forma compilada, traduzida para o binário legível para a máquina, em vez de qualquer linguagem de programação legível para humanos. Para entender o binário, Robinson teria que observá-lo ser executado passo a passo no computador, desenrolando-o em tempo real com uma ferramenta comum de engenharia reversa chamada IDA Pro, que traduzia as funções dos comandos em código durante a execução. "É quase como se você estivesse tentando determinar a aparência de alguém olhando apenas para seu DNA", disse Robinson. "E o Deus que criou essa pessoa estava tentando deixar o processo o mais difícil possível."

Porém, na segunda semana, a análise microscópica e passo a passo dos dados binários finalmente começou a dar frutos. Quando ele conseguiu decodificar as configurações do malware, elas continham o chamado código de campanha — essencialmente uma etiqueta associada com aquela versão do malware que os hackers poderiam usar para separar e rastrear qualquer vítima infectada. E, para a amostra do BlackEnergy que veio do PowerPoint ucraniano, esse código de campanha era um que ele reconheceu imediatamente, não de sua carreira como analista de malware, mas de sua vida pessoal como nerd de ficção científica: "arrakis02".

Na verdade, para Robinson, ou praticamente qualquer outro geek conhecedor de ficção científica, a palavra "Arrakis" é mais do que reconhecível: é tão familiar quanto Tatooine ou Terra Média, o cenário de um pilar central do cânone cultural. Arrakis é o planeta desértico onde o romance *Duna*, o épico de 1965 de Frank Herbert, se desenrola.

A história de *Duna* se passa em um mundo no qual a Terra foi destruída por uma guerra nuclear mundial contra máquinas de inteligência artificial. Ela segue o destino de um dos nobres da família Atreides depois que eles foram instalados como governantes de Arrakis — também conhecida como Duna — e, então, politicamente sabotados e arrancados do poder por seus rivais do mal, os Harkonnens.

Depois que os Atreides são derrubados, o herói adolescente do livro, Paul Atreides, se refugia no vasto deserto do planeta, onde vermes de areia gigan-

tes vivem no subterrâneo, ocasionalmente emergindo para consumir tudo em seu caminho. Enquanto cresce, Atreides aprende os costumes dos nativos de Arrakis, conhecidos como Fremen, incluindo a habilidade de capturar e montar os vermes de areia. Por fim, ele lidera um levante de guerrilha espartana e, guiando os vermes de areia para uma batalha devastadora, ele e os nativos Fremen tomam a capital de volta, e sua insurgência assume o controle de todo o império global que havia apoiado o golpe dos Harkonnen.

"Sejam quem for esses hackers, parece que são fãs de Frank Herbert", Robinson se lembra de pensar.

■

Quando ele encontrou aquele código de campanha arrakis02, Robinson pôde sentir que havia tropeçado em algo mais do que uma pista peculiar sobre os hackers que escolheram aquele nome. Ele sentiu pela primeira vez que estava enxergando o interior de suas mentes e imaginações. Na verdade, ele começou a imaginar se isso poderia servir de impressão digital. Talvez pudesse encontrá-la em outras cenas do crime.

Ao longo dos dias seguintes, Robinson deixou de lado a versão ucraniana de PowerPoint do BlackEnergy e foi escavar nos arquivos de antigas amostras de malware da iSight e em um banco de dados chamado VirusTotal. De propriedade da Alphabet, empresa-mãe do Google, VirusTotal permite que qualquer pesquisador de segurança que esteja testando um pedaço de malware faça o upload e compare-o com dezenas de produtos comerciais de antivírus — um método rápido e imperfeito para ver se outras empresas de segurança detectaram o código em outro lugar e o que elas podem saber sobre ele. Como resultado, VirusTotal montou uma enorme coleção das amostras de código selvagens reunidas ao longo de mais de uma década, que pesquisadores podem pagar para acessar. Robinson começou a rodar uma série de varreduras desses arquivos de malware, procurando por pedaços de código similares ao que ele havia descoberto com sua amostra do BlackEnergy para comparar com amostras de código mais antigas no catálogo da iSight e do VirusTotal.

Ele logo obteve resultado. Outra amostra do BlackEnergy de quatro meses antes, em maio de 2014, era uma cópia imperfeita do que foi baixado pelo PowerPoint ucraniano. Quando Robinson escavou o código de campanha, encontrou o que estava procurando: houseatreides94, outra referência inconfundível de *Duna*. Dessa vez, a amostra do BlackEnergy estava escondida em um arquivo do Word, em uma discussão sobre os preços de petróleo e gás aparentemente projetada como isca para uma empresa de energia polonesa.

Nas semanas seguintes, Robinson continuou explorando seu arquivo de programas maliciosos. Com o tempo, criou suas próprias ferramentas que poderiam buscar por combinações de malware, automatizar o processo de destravar as camadas de criptografia obscura do arquivo e, então, puxar o código de campanha. Sua coleção de amostras começou a crescer aos poucos: BasharoftheSardaukars, SalusaSecundus2, epsiloneridani0, como se os hackers estivessem tentando impressioná-lo com seu crescente conhecimento obscuro dos detalhes de *Duna*.

Cada uma dessas referências a *Duna* estava ligada, como as duas primeiras que ele havia encontrado, a um documento de isca que revelava algo sobre as vítimas alvo do malware. Um deles era um documento diplomático discutindo o "cabo de guerra" da Europa com a Rússia pela Ucrânia enquanto o país passava por dificuldades com um movimento popular puxando-o na direção do Ocidente e a influência persistente da Rússia. Outro documento parecia planejado como uma isca para visitantes de um evento no País de Gales e um evento relacionado à OTAN na Eslováquia, que focava, em parte, a espionagem russa. Outro parecia até mirar especificamente um pesquisador acadêmico norte-americano que se concentrava na política externa da Rússia, cuja identidade a iSight decidiu não revelar publicamente. Graças às úteis referências a *Duna* dos hackers, todos aqueles ataques discrepantes poderiam, enfim, ser conectados uns aos outros.

Mas algumas das vítimas não se pareciam com os indivíduos usuais da espionagem geopolítica russa. Por exemplo, por que exatamente os hackers estavam focando uma empresa de energia polonesa? Outra isca, a iSight descobriria mais tarde, mirava a agência de ferrovias ucraniana, Ukrzaliznytsia.

Mas, enquanto cavava cada vez mais fundo no monte de lixo da indústria de segurança, caçando referências a *Duna*, Robinson foi surpreendido por outro fato: enquanto o zero-day do PowerPoint que eles haviam descoberto foi uma novidade, a campanha de amplo ataque dos hackers se estendia não por meses, mas por anos. A aparição mais antiga das iscas dos hackers ligadas a *Duna* é de 2009. Até Robinson conseguir reunir as migalhas das operações, eles estavam penetrando nas organizações em segredo há meia década.

■

Após seis semanas de análise, a iSight estava pronta para ir a público com suas descobertas: algo que parecia ser uma vasta campanha de espionagem altamente sofisticada, com todas as indicações de ser uma operação do governo russo mirando a OTAN e a Ucrânia.

Enquanto Robinson desfiava meticulosamente essa operação, seu chefe, John Hultquist, se tornara tão obcecado pelo trabalho dos hackers russos quanto os

analistas de malware examinando o código. Robinson sentou-se no lado do cercado mais próximo do escritório do chefe, e Hultquist gritava perguntas a ele, com seu sotaque do Tennessee atravessando as paredes com facilidade. Mas, na metade de outubro, Hultquist já invadia o cercado quase diariamente para pedir atualizações a Robinson, enquanto o mistério se desenrolava a partir daquele primeiro zero-day do PowerPoint.

Mesmo com todos os truques espertos dos hackers, Hultquist sabia que conseguir qualquer atenção para a descoberta ainda dependeria de experiência com a mídia. Na época, ciberespiões chineses, e não russos, eram os inimigos número um da mídia e da indústria de segurança norte-americanas. Empresas como Northrop Grumman, Dow Chemical e Google haviam sido todas invadidas por hackers chineses em uma série de campanhas chocantes de roubo de dados — focadas, na maior parte, em propriedade intelectual e segredos comerciais —, fazendo o então diretor da NSA, Keith Alexander, chamar o evento de "a maior transferência de riqueza na história".[1] Uma operação de espionagem russa com alvos nada surpreendentes do Leste Europeu como esta, apesar de todas as habilidades insidiosas envolvidas e de sua longevidade, corria o risco de se perder no ruído.

Os hackers precisariam de um nome chamativo e atraente. Essa escolha, como era de costume na indústria de cibersegurança, era prerrogativa da iSight, a empresa que havia descoberto o grupo.* E claramente o nome deveria referenciar a aparente obsessão dos ciberespiões por *Duna.*

Robinson, fã de *Duna* desde adolescente, sugeriu que eles nomeassem a operação hacker como "Bene Gesserit", referência a uma ordem mística de mulheres que possuem poderes quase mágicos de manipulação psicológica no livro. Hultquist, que nunca leu o livro de Frank Herbert, vetou a ideia por ser muito confusa e difícil de pronunciar.

Em vez disso, Hultquist escolheu um nome mais direto, que ele esperava que evocasse um monstro oculto, se mexendo logo abaixo da superfície, ocasionalmente emergindo para brandir um terrível poder — um nome mais adequado do que o próprio Hultquist poderia saber na época. Ele chamou o grupo de Sandworm, os vermes de areia.

* Na verdade, a iSight não foi necessariamente a primeira a ligar os pontos sobre as impressões digitais do grupo de hackers. A empresa eslovaca ESET estava, ao mesmo tempo, fazendo as mesmas descobertas, incluindo os códigos de campanha com temática de *Duna* no malware do grupo. A ESET até apresentou suas descobertas na conferência Virus Bulletin em Seattle, em setembro de 2014. Mas como a ESET não publicou suas descobertas online, os analistas da iSight me contaram que não sabiam dessa pesquisa paralela, e a iSight foi largamente creditada — talvez por engano — como a primeira a descobrir o Sandworm.

4

MULTIPLICADOR DE FORÇAS

Seis semanas após a descoberta do Sandworm, a equipe da iSight teve uma rodada de bebidas no escritório para celebrar, reunindo-se no bar que a empresa mantinha abastecido no fim do corredor do cercado de analistas. A estreia do Sandworm no cenário mundial foi tudo que Hultquist havia esperado. Quando a empresa foi a público com sua descoberta de uma campanha de espionagem russa que já durava cinco anos, incluía um zero-day e tinha a temática de *Duna*, as notícias se espalharam pela indústria e a mídia, com histórias aparecendo no *Washington Post*, *Wired* e inúmeras publicações das indústrias de tecnologia e segurança. Robinson se lembra de brindar com Hultquist com um copo de vodka em homenagem à nova espécie de hacker russo que eles haviam desenterrado.

Mas, naquela mesma noite, a 4 mil quilômetros a oeste, outro pesquisador de segurança ainda estava escavando. Kyle Wilhoit, um analista de malware para a empresa japonesa Trend Micro, viu o relatório online da iSight sobre o Sandworm naquela tarde, no meio de infindáveis reuniões da conferência corporativa que ele estava participando em um hotel em Cupertino, na Califórnia. Wilhoit conhecia a iSight por sua reputação — e conhecia John Hultquist em particular. Wilhoit anotou para se lembrar de dar uma olhada com calma no relatório ao final do dia. Ele sentia que descobertas tão significativas como as da iSight tendiam a um efeito cascata. Talvez isso gerasse novas descobertas para ele e a Trend Micro.

Naquela noite, sentado no bar do hotel, Wilhoit e outro pesquisador da Trend Micro, Jim Gogolinski, pegaram seus notebooks e baixaram tudo que a iSight havia tornado público — os chamados indicadores de comprometimento que a empresa havia publicado na esperança de ajudar outras potenciais vítimas do Sandworm a detectarem e bloquearem seus atacantes.