MISHA GLENNY

Mercado sombrio

O cibercrime e você

Tradução
Augusto Pacheco Calil
Jorge Schlesinger
Luiz A. de Araújo

Companhia Das Letras

Grafia atualizada segundo o Acordo Ortográfico da Língua Portuguesa de 1990, que entrou em vigor no Brasil em 2009.

Título original
DarkMarket — CyberThieves, CyberCops and you

Capa
Kiko Farkas e Adriano Guarnieri/ Máquina Estúdio

Preparação
Beatriz Antunes

Revisão técnica
André Conti

Índice remissivo
Luciano Marchiori

Revisão
Luciane Helena Gomide
Jane Pessoa

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Glenny, Misha
Mercado sombrio : o cibercrime e você / Misha Glenny ; tradução Augusto Pacheco Calil, Jorge Schlesinger, Luiz A. de Araújo — São Paulo : Companhia das Letras, 2011.

Título original: DarkMarket — CyberThieves, CyberCops and you
Bibliografia
ISBN 978-85-359-1988-2

1. Crime organizado — Política governamental 2. Crime por computador 3. Crime por computador — Prevenção I. Título.

11-11821 CDD 364.168

Índice para catálogo sistemático:
1. Cibercrime : Problemas sociais 364.168

[2011]

EDITORA SCHWARCZ LTDA.
Rua Bandeira Paulista, 702, cj. 32
04532-002 — São Paulo — SP
Telefone (11) 3707-3500
Fax (11) 3707-3501
www.companhiadasletras.com.br
www.blogdacompanhia.com.br

Sumário

PARTE III

PARTE IV

PARTE V

INTERLÚDIO

Livro Dois

PARTE I

PARTE II

PARTE III

PARTE IV

Prólogo

CRIME@SÉCULO21.COM

Na implacável busca humana por conveniência e crescimento econômico, desenvolvemos em pouco tempo um nível alarmante de dependência em relação aos sistemas em rede. Em menos de duas décadas, grande parte da chamada "infraestrutura nacional crítica" da maioria dos países (CNI, na língua dos geeks) passou a ser controlada por sistemas computadorizados cada vez mais complexos.

Os computadores dirigem importantes parcelas de nossa vida: regulam nossa comunicação, nossos veículos, nossa interação com o comércio e o Estado, nosso trabalho, nosso lazer — nosso *tudo*. Num dos muitos julgamentos de crimes cibernéticos que presenciei nos últimos anos, um juiz britânico impôs uma ordem restritiva a um hacker, que entraria em vigor assim que ele fosse libertado da prisão. Ele seria posto sob a supervisão de um policial, que deveria impedi-lo de acessar a internet por mais de uma hora por semana. "Quando meu cliente terminar de cumprir sua

sentença", destacou o advogado do réu durante a audiência, "não haverá quase nenhuma atividade humana que não seja mediada pela internet. Como é possível que ele leve uma vida normal sob tais circunstâncias?" Foi uma pergunta retórica.

Mas, de todo modo, uma boa pergunta. Aqueles que já esqueceram o celular em casa por algumas horas com certeza experimentaram uma intensa sensação de perda e irritação, semelhante aos sintomas de abstinência sentidos por dependentes de drogas. Curiosamente, quando privados de seus telefones por três dias, a corrosiva sensação de inquietude costuma ser substituída pela euforia da libertação, conforme a pessoa é transportada de volta a um mundo, não tão distante, no qual não tínhamos nem precisávamos de celulares e organizávamos nossa vida muito bem sem eles. Hoje em dia, no entanto, a maioria sente que não é possível viver sem esses pequenos computadores portáteis.

Talvez a máquina mais comparável ao computador seja o carro. A partir dos anos 1940, quando ele se tornou um artigo padrão nas famílias, apenas uma minoria dos motoristas compreendia o que de fato ocorria sob o capô. Ainda assim, um bom número deles era capaz de consertar o próprio veículo em caso de pane, e um número ainda maior de proprietários sabia dar um jeito no carburador para ao menos chegar em casa. A maioria conseguia, no mínimo, trocar um pneu furado.

Hoje, se o problema for apenas um pneu furado, é provável que a pessoa chegue a seu destino. Mas um número cada vez maior de panes é agora causado por um defeito no computador da caixa de controle — o invólucro de plástico preto que costuma ficar atrás do motor. Se o problema for aí, nem mesmo se o motorista for um experiente mecânico de tanques de guerra ele conseguirá fazer o carro andar. Talvez um engenheiro da computação fosse capaz de resolver o problema, mas na maior parte dos casos, porém, é preciso mesmo substituir a unidade.

Os sistemas de computadores são muito mais complexos e frágeis que os motores de combustão interna, de forma que, em caso de problemas, apenas um minúsculo grupo de pessoas sabe o que fazer além de se guiar pelo conhecido mantra: "Já tentou reiniciar o sistema?".

Agora nos encontramos numa situação em que essa minúscula elite (podemos chamá-los de geeks, nerds, programadores, securocratas ou pelo termo que preferirmos) detém um entendimento profundo de uma tecnologia que a cada dia comanda nossa vida de maneira mais intensa e extensa, enquanto a maioria de nós não entende nada do seu funcionamento. Comecei a reconhecer a dimensão do problema durante as pesquisas para o meu livro anterior sobre o crime organizado global, *McMáfia*. Viajei ao Brasil para investigar os crimes cibernéticos porque esse país cativante é, além de suas muitas qualidades positivas, um grande centro de práticas nefastas na rede — apesar de poucos saberem disso na época.

No Brasil conheci ladrões cibernéticos que tinham criado uma fraude de *phishing* muito bem-sucedida. O *phishing* continua a ser um dos pilares mais infalíveis da criminalidade na internet. Há duas variações simples. A vítima abre um e-mail indesejado. O anexo pode conter um vírus, permitindo a outro computador em qualquer lugar do planeta monitorar toda a atividade na máquina infectada, como a digitação de senhas bancárias, por exemplo. O outro truque consiste em disparar um e-mail que pareça ter sido enviado por um banco ou outra instituição que possa solicitar login, senha e outros dados do usuário. Se o destinatário cair no truque, o remetente torna-se então capaz de usar tais informações para acessar suas contas na internet. Os hackers brasileiros demonstraram passo a passo como fizeram para transferir para si mesmos milhões de dólares de contas no Brasil, na Espanha, em Portugal, na Grã-Bretanha e nos Estados Unidos.

Visitei então os ciberpoliciais em Brasília que tinham apanhado quatro outros membros dessa quadrilha (apesar de um número ao menos duas vezes maior nunca ter sido rastreado pela polícia), e depois entrevistei o chefe da X-Force, departamento de operações secretas da empresa americana de segurança ISS. No intervalo de mais ou menos uma semana, percebi que o crime organizado convencional, por mais matizes e variações que tenha, traz muito mais riscos para seus perpetradores que o crime cibernético.

O crime organizado à moda antiga, ligado à tecnologia e aos meios de comunicação do século XX, lida com dois consideráveis desafios para atingir o sucesso. A polícia representa o principal risco para seus negócios. A eficácia do policiamento varia com a geografia e o tempo. O crime organizado se adapta a essas diferentes condições e escolhe um, dentre uma série de métodos, para lidar com as forças da lei e da ordem. Pode tentar vencê-las pela força ou corrompê-las; pode corromper os políticos que exercem autoridade sobre a polícia; ou pode dificultar as investigações.

Mas então enfrenta um segundo problema: a ameaça da concorrência, outros malfeitores que caçam sua presa nas mesmas águas. Também nesse caso os grupos ligados ao crime organizado podem tentar se impor pela força, sugerir uma aliança, ou ainda concordar em ser incorporados pelos rivais.

Em nenhum desses casos, porém, a organização criminosa pode optar por ignorar seu rival — atitude que representaria o caminho da derrota, com resultados por vezes fatais. Para garantir a sobrevivência e a prosperidade é fundamental ter a capacidade de se comunicar com os colegas criminosos e a polícia, e, mais importante, de mandar a mensagem correta a ambos.

No Brasil, aprendi rápido que o crime do século XXI é diferente.

O mais importante: é muito difícil identificar quando as pes-

soas têm más intenções na rede. As leis que regem a internet variam muito de país para país. E esse é um dado significativo, porque, muitas vezes, no ambiente virtual um crime é cometido a partir de um endereço IP (sigla em inglês para protocolo da internet) localizado num determinado país contra um indivíduo ou corporação de outro país, antes de ser concluído (ou transformado em lucro) num terceiro. Um policial na Colômbia, por exemplo, pode identificar que o endereço IP responsável por coordenar um ataque a um banco colombiano vem do Cazaquistão. Em seguida descobre que essa ação não é considerada crime naquele país, e por isso seus equivalentes cazaques em Astana não terão motivos para investigar o crime.

Muitos criminosos cibernéticos são inteligentes o bastante para pesquisar e explorar discrepâncias como esta. "Nunca uso cartões de crédito ou de débito americanos", disse-me um dos mais bem-sucedidos *carders* (especializado em fraudar cartões) da Suécia. "Isso me colocaria sob a jurisdição legal dos Estados Unidos, onde quer que eu estivesse. Por isso uso apenas cartões europeus e canadenses, o que me deixa ao mesmo tempo feliz e seguro — eles nunca vão me apanhar."

A diferença que separa os Estados Unidos da Europa e do Canadá é de grande importância, pois essas são as regiões que apresentam a maior concentração de vítimas de crimes cibernéticos. Os dois últimos contam com leis muito mais robustas para proteger as liberdades e os direitos individuais na rede. Seguidos governos americanos conferiram ao aparato policial poderes maiores do que a maioria dos governos europeus estaria disposta a considerar, permitindo aos policiais um acesso mais fácil aos dados de empresas privadas em nome da luta contra o crime e o terrorismo.

Poderíamos argumentar, por exemplo, que a onipresença multiplataforma e multitarefa do Google viola os princípios da legis-

lação antitruste americana e que a aglomeração de todos aqueles dados pessoais consiste ao mesmo tempo em uma oportunidade para os criminosos e uma ameaça às liberdades civis. Mas o Google poderia perfeitamente responder que a própria essência de sua genialidade e de seu sucesso está na onipresença multiplataforma e multitarefa do site, e que isso em si promove a segurança e os interesses comerciais americanos. Se desejar, o governo americano pode, em questão de horas, acessar os dados do Google recorrendo a procedimentos legais e, como o Google reúne dados de todo o mundo, isso confere a Washington uma imensa vantagem estratégica. Outros governos desejariam ter a mesma sorte. Diferentemente de seus equivalentes chineses, russos e médio-orientais, o governo americano não precisa invadir os sistemas do Google para explorar seus segredos. Em vez disso, pode obter facilmente uma ordem judicial. Quem abriria mão desse poder em nome da legislação antitruste?

A internet é uma teoria da grande bolha — resolvemos um problema que a afeta, mas outro, aparentemente intratável, vem à tona em outra parte.

E, para quem a policia, o maior de todos os problemas é o anonimato. Por enquanto, continua sendo possível para qualquer pessoa com acesso à internet e dotada de conhecimentos específicos mascarar a localização física de um computador.

Há duas maneiras principais de se fazer isso: a primeira muralha cibernética é a VPN, ou rede virtual privada, que faz com que um número de computadores partilhe o mesmo endereço IP. Normalmente um endereço IP é atribuído a uma única máquina, mas, com uma VPN, vários computadores localizados em partes diferentes do mundo podem aparentar estar situados em Botsuana, por exemplo.

Para aqueles que não se satisfazem com a proteção oferecida pela VPN, existe também a possibilidade de erguer uma segun-

da barreira cibernética por meio dos chamados servidores *proxy*. Um computador nas Ilhas Seychelles pode estar usando um *proxy* na China ou na Guatemala. O *proxy* não revela que o IP original está transmitindo a partir das Seychelles — mas seja como for o computador faz parte de uma VPN centrada na Groenlândia.

Configurar tudo isso exige habilidades avançadas de computação, e por isso tais técnicas tendem a ser usadas pelos dois únicos grupos envolvidos no crime cibernético: hackers de verdade e criminosos de verdade. Mas essa elite de operadores, que representa um novo tipo de crime organizado sério, é apenas uma pequena parte dos que se envolvem nos crimes computadorizados.

Os demais são participantes menores, que agem individualmente, roubam somas não muito expressivas, são ladrões de galinha que mal valem o esforço de caçá-los, levando-se em consideração os recursos escassos à disposição das forças policiais. Apesar de esses personagens não se darem ao trabalho de configurar VPNs, *proxies* e toda uma série de outras técnicas de ocultamento, eles ainda podem dificultar muito a vida dos policiais ao criptografar suas comunicações.

Programas que garantem a criptografia da comunicação escrita (e até falada ou filmada) estão disponíveis à farta na rede, mas dentre todos o que mais se destaca é o PGP, o simpático e coloquial Pretty Good Privacy (Privacidade Bem Decente).

A criptografia é uma poderosa ferramenta, que desempenha um papel importante na segurança cibernética. Trata-se de uma maneira de embaralhar a linguagem usando chaves matemáticas geradas digitalmente, cuja permutação é tão complexa que só pode ser revelada àqueles que possuem a senha correta. No momento, os documentos criptografados são seguros, apesar de a Agência de Segurança Nacional de Washington (NSA), a mais poderosa agência de espionagem digital do mundo, estar sempre buscando formas de decifrá-los. No submundo dos criminosos

cibernéticos, já circulam rumores segundo os quais a NSA e seus parceiros de espionagem no Canadá, Grã-Bretanha, Austrália e Nova Zelândia já possuiriam a capacidade de quebrar esses sistemas públicos de criptografia com o uso do seu orwelliano sistema Echelon. De acordo com o que se diz, o Echelon seria capaz de acessar comunicações via telefone, satélite e e-mail em qualquer ponto do planeta.

As implicações políticas da criptografia digital são tão amplas que o governo americano começou a classificar os softwares criptográficos como "munições" na década de 1990, enquanto na Rússia, se a polícia ou a KGB um dia encontrarem um único arquivo criptografado no computador de um usuário, a pessoa poderá ser detida e passar vários anos na cadeia, mesmo que o documento contenha apenas uma lista semanal de compras. Conforme governos e corporações reúnem cada vez mais informações pessoais sobre seus cidadãos ou clientes, a criptografia se torna uma das últimas linhas de defesa ao alcance dos indivíduos para garantir a própria privacidade. É também um instrumento de valor incalculável para quem atua em atividades criminosas na rede.

Assim como os criminosos tradicionais precisam desenvolver maneiras de falar uns com os outros e diferenciar amigos, adversários, policiais e rivais, os cibervilões enfrentam o desafio permanente de tentar estabelecer as credenciais fidedignas de quem quer que esteja conversando com eles na rede. Parte deste livro é dedicada a contar como eles desenvolveram métodos para identificar uns aos outros, e como as forças policiais de todo o mundo tentaram ludibriar a capacidade dos hackers de identificar agentes e informantes confidenciais (CIS) infiltrados na internet.

Ao longo dos anos 1990, a maneira mais simples de evitar que convidados indesejados bisbilhotassem atividades criminosas estava na introdução de um rigoroso sistema de sabatinas e concessão de acesso aos sites dedicados ao debate de práticas inde-

vidas na rede. Apesar dessa medida de segurança, não demorou mais que alguns meses para que forças da lei — o Serviço Secreto americano e agências de espionagem como o FSB (sucessor da KGB) — estivessem rastejando por todos esses sites, após fingirem pacientemente ser criminosos para obter acesso, ou ter persuadido informantes a trabalhar para eles.

A interpretação de certos agentes foi tão convincente que algumas agências da lei chegaram até a dedicar seus recursos à perseguição desses policiais infiltrados, filiados a organizações irmãs, tomando-os por criminosos de verdade.

Como resultado de suas iniciativas, as forças policiais e os espiões conseguiram, ao longo da última década, compilar um grande banco de dados de hackers criminosos: seus apelidos, sua localização real ou presumida, o tipo de atividade em que se envolvem e com quem costumam se comunicar com regularidade. O escalão mais baixo dos criminosos cibernéticos teve seus dados devassados. Mas, apesar de todo esse volume de informação, continua sendo extremamente difícil processar um criminoso cibernético.

É aí que a própria natureza da rede — em particular sua interconectividade — traz uma imensa dor de cabeça para as forças da lei: ninguém pode ter certeza absoluta da identidade daqueles com quem está se comunicando. Estaríamos lidando com um hacker criminoso comum? Ou alguém que conta com amigos no poder? Será mesmo um criminoso do outro lado? Ou um agente infiltrado? Ou um pesquisador militar avaliando as possibilidades das técnicas criminosas de invasão de sistemas? Somos nós que observamos nosso interlocutor ou é ele quem nos observa? Será que ele está tentando obter lucro para si mesmo? Ou para a Al-Qaeda?

"É como uma partida de xadrez heptadimensional", comentou o futurologista Bruno Guissani, "no qual nunca podemos ter certeza de quem é o nosso oponente."