OPINIÃO

Quais os impactos do mercado ilegal para a sociedade?

Eduardo Masulo (*)

Quando falamos sobre o mercado ilegal, podemos pensar: o que temos a ver com isso?

Ao nos aprofundarmos no tema, descobrimos que o problema é mais complexo do que parece e que possui impacto direto na vida de toda sociedade, estando presente no nosso dia a dia tanto em relação ao aumento da violência, quanto nos preços dos produtos nas prateleiras e nos combustíveis, por exemplo.

O efeito vai além de redução da arrecadação de impostos para os Estados, transitando nas esferas sociais, econômicas, de segurança, da saúde pública e por aí vai. Somente no ano passado, quando fomos impactados pela pandemia da Covid-19, o Brasil movimentou R$ 287,9 bilhões no mercado ilegal, segundo o FNCP (Fórum Nacional Contra a Pirataria), valor que, apesar ser expressivo, apresentou uma redução se comparado com 2019, que registrou R$ 291,4 bilhões.

Diante desses números, estima-se que o país deixou de arrecadar cerca de R$ 90 bilhões em impostos que poderiam ser revertidos em educação, saúde e segurança, entre outros benefícios para a sociedade. A baixa redução de 1,2% de movimentação no mercado ilegal entre os anos, teve ligação direta com as ações em combate ao vírus.

Barreiras sanitárias em fronteiras apreenderam materiais contrabandeados, houve baixa circulação de pessoas nas ruas e a restrição de diversão adulta noturna impactou diretamente o consumo de cigarros ilegais e de bebidas alcoólicas falsificadas ou contrabandeadas.

Mas, qual a origem e atos ilícitos que alimentam esses negócios? Contrabando, descaminho e roubos de cargas, que são crimes de baixa repercussão e julgados como menor potencial ofensivo e com penas brandas, o que, de certa forma, estimulam o "arriscar" por parte de cidadãos de valores deturpados ou em fragilidade financeira.

E como esses produtos chegam nos pontos de vendas, como os óculos vendidos por ambulantes na praia, assim como maquiagens, artigos de perfumaria, cosméticos, brinquedos, materiais esportivos e eletroeletrônicos vendidos em banquinhas de ruas, conhecidas como camelôs? Isso sem falar da TV por assinatura pirata.

O que sempre julgamos como algo inofensivo, foi a porta descoberta para enriquecimento e fortalecimento do crime organizado, que evoluiu enquanto nosso código penal não. Havendo mercado consumidor desses produtos e serviços, o crime estará presente. A sociedade tem ampla responsabilidade neste sentido e precisa se conscientizar dos seus deveres éticos e morais para que esse cenário seja controlado.

Nossa cultura vive uma notória inversão de valores. Os agentes fiscalizadores passam a ser os vilões quando cumprem seus deveres, enquanto a sociedade tende a se sensibilizar pelo lado do "trabalhador informal", colocando-o como vítima sem perceber os malefícios desta postura, que desconhece o caminho percorrido desses produtos, muitas vezes às custas de sangue. Quando isso ocorre, passamos a ser cúmplices.

Um outro problema nada incomum, infelizmente, é a ausência de fiscalização, seja por falta de braços dos órgãos responsáveis ou pela omissão por não querer correr riscos ou por interesses escusos. Em ambos os casos, quem se beneficia é o crime organizado, que expande seus territórios e nichos de mercados em velocidade surpreendente.

O aumento do desemprego também é outro impacto, pois, em decorrência das facilidades listadas aqui com concorrências desleais, empresas fecham postos de trabalhos e reduzem linhas de produção. Somente a indústria do tabaco no Brasil, em 2019, deixou de gerar cerca de 173 mil empregos diretos e indiretos no cultivo, transporte, armazenamento e distribuição.

É preciso esclarecer que não há julgamento de valores sobre pessoas ou instituições. Porém, é necessário demonstrar que, por meio da própria sociedade e de seus comportamentos indevidos da cultura do benefício próprio - a maioria por falta de informações e outros por conivência - o crime organizado se fortalece e está deixando de ser alimentado somente por venda de drogas. Os delitos estão se reinventando e os mecanismos de combate precisam evoluir.

Mas, a sociedade precisa entender o seu papel dentro desse processo. A ética é um exercício diário que não pode deixar de ser praticada para atender aos interesses pessoais.

(*) - É consultor sênior na ICTS Security, empresa que atua com consultoria e gerenciamento de operações em segurança (www.ictssecurity.com.br).

Programa de estágio

A Ocyan, empresa do setor de óleo e gás, está com inscrições abertas para o Programa de Estágio 2021. Ao todo serão 17 vagas para diversos cursos incluindo tecnologia, engenharias, administração, economia, ciências contábeis e direito para atuação no escritório da empresa no Rio de Janeiro e em sua base, em Macaé (RJ). No ano passado, o programa selecionou 47% de pardos/pretos (negros) e 71% de mulheres, e o desafio de agora é atrair também talentos do subúrbio do Rio de Janeiro e de regiões economicamente menos favorecidas tanto da capital, quanto da cidade de Macaé e adjacências. As inscrições já estão abertas e poderão ser feitas até o dia 02/08 (www.ocyan-sa.com http://www.ocyan-sa.com).

O que fazer em meio a um ataque de ransomware?

Identificação da variante do ataque e localização dos backups estão entre as ações recomendadas pela Fortinet

Imagem de Pete Linforth por Pixabay

Os ataques de ransomware estão cada vez mais frequentes. De acordo com o relatório global de ameaças do FortiGuard Labs, da Fortinet, esse crime aumentou sete vezes na última metade de 2020 e se tornou ainda mais extensivo, atingindo quase todos os setores e países do mundo.

Ao mesmo tempo, as táticas dos criminosos mudam constantemente e já não basta possuir as estratégias defensivas corretas, mas avaliar continuamente as políticas de segurança, para garantir que as redes possuam as respostas atualizadas contra esse tipo de ataque.

Com isso em mente, a Fortinet, líder global em soluções de cibersegurança, preparou um checklist para ajudar organizações a lidarem com um ataque de ransomware quando ele acontecer:

Execute o plano de RI: Se disponível, comece a executar seu plano de resposta a incidentes (RI) imediatamente. Se você não tiver um, as etapas abaixo podem ajudar. Em alternativa, contate o seu fornecedor de segurança para obter ajuda ou reporte o incidente à sua companhia de seguros; eles podem já ter uma lista de provedores de segurança especializados que podem ajudá-lo. Considere o potencial impacto que o incidente de segurança pode ter.

Isole seus sistemas e interrompa a propagação: Existem várias técnicas para isolar a ameaça e impedir que ela se espalhe. Primeiro, identifique o alcance do ataque. Se o incidente já for generalizado, implemente bloqueios no nível da rede, como isolar o tráfego no switch ou na borda do firewall, ou considere desligar temporariamente a conexão com a Internet. Se disponível, a tecnologia de detecção e resposta de endpoint (EDR) pode bloquear o ataque no nível do processo, o que seria a melhor opção imediata com o mínimo de interrupção dos negócios. A maioria dos invasores de ransomware encontra uma vulnerabilidade para entrar em sua organização, como RDP exposto e e-mails de phishing.

Identifique a variante do ransomware: Muitas das táticas, técnicas e procedimentos (TTPs) de cada variante de ransomware estão documentados publicamente. Determinar com qual cepa você está lidando pode dar pistas sobre a localização da ameaça e como ela está se espalhando. Dependendo da variante, algumas ferramentas de descriptografia podem já estar disponíveis para você quebrar a criptografia de seus arquivos.

Identifique o acesso inicial: Determinar o ponto de acesso inicial, ou o primeiro sistema comprometido, ajudará a identificar e fechar a brecha em sua segurança. Os vetores de acesso inicial comuns são phishing, exploits em seus serviços de borda (como serviços de Área de Trabalho Remota) e o uso não autorizado de credenciais. Determinar o ponto inicial de acesso às vezes é difícil e pode exigir a experiência de equipes forenses digitais e especialistas em RI.

Identifique todos os sistemas e contas infectados (escopo): Identifique qualquer malware ativo ou sobras persistentes em sistemas que ainda estão se comunicando com o servidor de comando e controle (C2). As técnicas de persistência comuns incluem a criação de novos processos que executam a carga maliciosa, o uso de chaves de registro de execução ou a criação de novas tarefas programadas.

Descubra se os dados foram exfiltrados: Muitas vezes, os ataques de ransomware não apenas criptografam seus arquivos, mas também exfiltram seus dados. Eles farão isso para aumentar as chances de pagamento de resgate, ameaçando postar dados proprietários ou embaraçosos online. Procure por sinais de exfiltração de dados, como grandes transferências de dados em seus dispositivos de borda de firewall. Procure comunicações estranhas de servidores que vão para aplicações de armazenamento em nuvem.

Localize seus backups e determine a integridade: Um ataque de ransomware tentará limpar seus backups online e cópias de sombra de volume para diminuir as chances de recuperação de dados. Por isso, certifique-se de que sua tecnologia de backup não foi afetada pelo incidente e ainda está operacional. Os invasores geralmente ficam em sua rede por dias, se não semanas, antes de decidirem criptografar seus arquivos. Isso significa que backups podem conter cargas maliciosas e que não podem ser restaurados para um sistema limpo. Analise seus backups para determinar sua integridade.

Limpe os sistemas ou crie novas arquiteturas: Se existe confiança na capacidade de identificar todos os malwares ativos e incidentes de persistência em seus sistemas, então talvez não seja necessário reconstrui-los. No entanto, pode ser mais fácil e seguro criar sistemas novos e limpos. Você pode até considerar a construção de um ambiente limpo e totalmente separado para o qual poderá então migrar. Isso não costuma demorar muito em um ambiente virtual. Ao reconstruir ou higienizar sua rede, certifique-se de que os controles de segurança apropriados estejam instalados e de que estejam seguindo as práticas recomendadas para garantir que os dispositivos não sejam infectados novamente.

Reporte o incidente: É importante relatar o incidente. É preciso também determinar se o relato às autoridades legais é necessário e obrigatório. Sua equipe jurídica pode ajudar a resolver quaisquer obrigações legais em torno de dados regulamentados. Se o ataque for grave e sua empresa abranger várias regiões geográficas, você pode precisar entrar em contato com os serviços de aplicação da lei nacionais e não locais.

Pagando o resgate?: As autoridades policiais desaconselham o pagamento do resgate, no entanto, se você estiver pensando em fazê-lo, deverá contratar uma empresa de segurança com habilidades especializadas para ajudá-lo. Além disso, pagar o resgate não corrigirá as vulnerabilidades exploradas pelos invasores, portanto, certifique-se de ter identificado o acesso inicial e fechado as brechas.

Conduza uma revisão pós-incidente: Analise sua resposta ao incidente para entender o que deu certo e para documentar oportunidades de melhoria. Isso garante a melhoria contínua de suas capacidades de resposta e recuperação para o futuro. Considere simular os detalhes técnicos e não técnicos do ataque para que você possa revisar suas opções.

"Quando ocorre um ataque de ransomware, tomar as medidas corretas é essencial para minimizar o impacto sobre a equipe e a organização", explica Alexandre Bonatti, diretor de Engenharia da Fortinet Brasil. "Depois que um ataque ocorre, o pânico pode se espalhar pela empresa e criar problemas maiores. Os CISOs sabem que sobreviver a um ataque de ransomware requer um plano de resposta a incidentes, mas o desafio está na hora de documentar um plano completo e ter os recursos certos para implementá-lo quando necessário."

News @TI

Hitachi conclui aquisição da GlobalLogic

@ A Hitachi Ltd. anunciou que concluiu a aquisição da GlobalLogic Inc. de acordo com os termos do contrato definitivo assinado em 31 de março de 2021. Conforme anunciado no comunicado à imprensa no dia de 31 de março, a Hitachi Global Digital Holdings LLC, uma subsidiária da Hitachi nos Estados Unidos, adquiriu 100% das ações em circulação da GlobalLogic Worldwide Holdings, Inc. a empresa controladora da GlobalLogic, dessa forma, a GlobalLogic Worldwide Holdings e a GlobalLogic tornaram-se subsidiárias integrais da HGDH (www.hitachi.com).

JA Brasil abre 590 vagas gratuitas para o programa Tech.já

@ A carreira na área de tecnologia é uma das mais promissoras no país, com a expectativa de uma demanda de 420 mil novas vagas até 2024, segundo a Brasscom, associação do setor. No entanto, a formação de novos profissionais não acompanha essa evolução, formando 46 mil novas pessoas com perfil tecnológico por ano. De olho neste descasamento entre oferta e procura, a JA Brasil (Junior Achievement), uma das maiores organizações mundiais de preparação de jovens para o mercado de trabalho, com o apoio do Google.org e do BID Lab (Laboratório de Inovação do Grupo BID), está lançando novas turmas do programa TECH.JÁ, que capacita jovens na área de Suporte em Tecnologia da Informação (TI). O curso é gratuito e oferece 590 vagas. Inscrições: https://bit.ly/techja2021_2

Mais de 100 vagas de estágio no país

@ A Enel Brasil, um dos maiores grupos privados do setor de energia do país, abre mais de 100 vagas para seu Programa de Estágio 2021 nos estados de São Paulo, Rio de Janeiro, Ceará e Goiás. Podem se candidatar jovens talentos que estejam a dois anos da conclusão do ensino superior nas áreas de Engenharia Elétrica, Engenharia de Produção, Engenharia Civil, Computação, Administração, Marketing, Economia, Direito e Psicologia. As inscrições podem ser feitas até o dia 5 de agosto pelo link https://app.jobconvo.com/pt-br/careers/enel/64026924-8d01-4c66-b2ed-feb4ec57abb1/ .

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** Publisher: **Lilian Mancuso** (lilian@netjen.com.br)

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: Tatiana Sapateiro – tatiana@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza. *Revisão:* Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080 – Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br) – Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90 - JUCESP, Nire 35218211731 (6/6/2003) - Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

RIO DE JANEIRO: **J.C. REPRESENTAÇÕES E PUBLICIDADES EIRELI**
Av. Rio Branco, 173 / 602 e 603 – Centro - Rio de Janeiro - CEP 20040-007
Tel. (21) 2262-7469 – CNPJ 30.868.129/0001-87