Comunicado de Alerta sobre Ameaças Cibernéticas da RPDC

Emitido em: **15 de abril de 2020**

Título: **Orientação sobre a Ameaça Cibernética da Coreia do Norte**

O Departamento de Estado dos EUA, bem como o Departamento do Tesouro, de Segurança Interna e o Federal Bureau of Investigation (FBI) estão emitindo este comunicado como um recurso abrangente contra a ameaça cibernética norte-coreana para a comunidade internacional, para os defensores das redes de comunicação e para o público em geral. O comunicado destaca a ameaça cibernética imposta pela Coreia do Norte - formalmente conhecida como República Popular Democrática da Coreia (RPDC) - e fornece as etapas recomendadas para mitigar esta ameaça. Em especial, o Anexo 1 lista os recursos do governo dos EUA relacionados a ameaças cibernéticas da RPDC, e o Anexo 2 inclui um link que dá acesso aos relatórios do Painel de Especialistas do Comitê de Sanções da ONU 1718 (RPDC).

As atividades cibernéticas maliciosas da RPDC ameaçam os Estados Unidos e a comunidade internacional em geral e, em especial, representam uma ameaça significativa à integridade e estabilidade do sistema financeiro internacional. Sob a pressão de fortes sanções dos EUA e da ONU, a RPDC tem se envolvido cada vez mais em atividades ilícitas - incluindo crimes cibernéticos - para gerar receita para suas armas de destruição em massa e programas de mísseis balísticos. Em particular, os Estados Unidos estão profundamente preocupados com as atividades cibernéticas maliciosas da Coreia do Norte, às quais o governo dos EUA se refere como HIDDEN COBRA. A RPDC tem a capacidade de realizar atividades cibernéticas disruptivas ou destrutivas com o potencial de afetar a infraestrutura crítica dos EUA. A RPDC também usa recursos cibernéticos para roubar instituições financeiras, e tem demonstrado um padrão de atividade cibernética disruptiva e prejudicial totalmente inconsistente com o crescente consenso internacional sobre o que constitui um comportamento estatal responsável no ciberespaço.

Os Estados Unidos trabalham em estreita colaboração com países que compartilham da mesma visão para focar a atenção e condenar o comportamento disruptivo, destrutivo ou desestabilizador da RPDC no ciberespaço. Um exemplo disso foi o que ocorreu em dezembro de 2017, quando a Austrália, Canadá, Nova Zelândia, Estados Unidos e o Reino Unido atribuíram publicamente à RPDC o ataque de ransomware WannaCry 2.0, e denunciaram a atividade cibernética danosa e irresponsável da RPDC. A Dinamarca e o Japão emitiram declarações de

apoio à denúncia conjunta do danoso ataque de ransomware WannaCry 2.0, que afetou centenas de milhares de computadores em todo o mundo em maio de 2017.

É fundamental que a comunidade internacional, os defensores de redes e o público permaneçam vigilantes e trabalhem em conjunto para mitigar a ameaça cibernética imposta pela Coreia do Norte.

Atividades cibernéticas maliciosas da RPDC direcionadas ao setor financeiro

Muitos atores cibernéticos da RPDC estão subordinados a entidades designadas pela ONU e pelos EUA, como o Reconnaissance General Bureau. Os atores cibernéticos patrocinados pelo Estado norte-coreano consistem principalmente de hackers, criptologistas e desenvolvedores de software que praticam espionagem e furto cibernético direcionado a instituições financeiras, troca de moeda digital, e operações com motivação política contra empresas de mídia estrangeiras. Eles desenvolvem e implementam uma ampla gama de ferramentas de malware em todo o mundo que possibilitam tais atividades, que se tornam cada vez mais sofisticadas. As táticas comuns utilizadas pelos atores cibernéticos da RPDC patrocinados pelo Estado com o intuito de aumentar a receita de forma ilícita incluem, dentre outras:

Furto Financeiro Cibernético e Lavagem de Dinheiro. O relatório intercalar de 2019 do Painel de Especialistas do Comitê do Conselho de Segurança das Nações Unidas 1718 (relatório intercalar de 2019 do POE - Painel de Especialistas) afirma que a RPDC está cada vez mais apta a gerar receita, apesar das sanções do Conselho de Segurança das Nações Unidas, usando atividades cibernéticas maliciosas para furtar de instituições financeiras por meio de ferramentas e táticas altamente sofisticadas. O relatório intercalar do POE de 2019 observa que, em alguns casos, essas atividades cibernéticas maliciosas também se estenderam à lavagem de recursos através de várias jurisdições. O relatório intercalar do POE de 2019 menciona que investigou dezenas de suspeitos de furtos cibernéticos na Coreia do Norte e verificou que, ao final de 2019, a RPDC tentou subtrair até US$ 2 bilhões por meio de atividades cibernéticas ilícitas. As alegações contidas em uma denúncia de confisco do Departamento de Justiça de março de 2020 são consistentes com algumas partes das conclusões do POE. Mais especificamente, a denúncia de confisco alegava que os agentes cibernéticos norte-coreanos usaram a infraestrutura instalada na Coreia do Norte para levar adiante sua conspiração para *hackear* trocas de moedas digitais, furtar centenas de milhões de dólares em moeda digital e fazer a lavagem do dinheiro.

Campanhas de extorsão. Os atores cibernéticos da RPDC também realizaram campanhas de extorsão contra entidades de países terceiros, comprometendo as redes de determinadas entidades e ameaçando desativá-las a menos que as entidades pagassem um resgate. Em alguns casos, os atores cibernéticos da RPDC exigiram das vítimas pagamento sob o disfarce de acordos de consultoria firmados a longo prazo, a fim de garantir que nenhuma atividade cibernética maliciosa semelhante ocorresse no futuro. Os atores cibernéticos da RPDC também foram pagos para *hackear* sites e extorquir alvos para terceiros.

Cryptojacking. O relatório intercalar do POE de 2019 afirma que o POE também está investigando o uso do "cryptojacking" na RPDC, um esquema para comprometer uma máquina e desviar seus recursos computacionais para minerar moeda digital. O POE identificou vários

incidentes nos quais computadores infectados com malware de criptografia enviavam os ativos extraídos - sendo grande parte em moedas digitais anônimas (também chamadas de "moedas de privacidade") - a servidores localizados na RPDC, inclusive para a Universidade Kim Il Sung em Pyongyang.

Tais atividades destacam a utilização pela RPDC de meios cibernéticos para gerar receita, atenuando simultaneamente o impacto das sanções e demonstrando que qualquer país pode ser exposto e explorado pela RPDC. De acordo com o relatório intercalar do POE de 2019, o POE também está investigando outras atividades, como as tentativas de violação das sanções do Conselho de Segurança da ONU contra a RPDC.

Operações Cibernéticas Publicamente Atribuídas à RPDC pelo Governo dos EUA

A RPDC tem repetidamente mirado as redes governamentais e militares dos EUA e de outros países, bem como as redes relacionadas a entidades privadas e infraestrutura crítica, com o intuito de furtar dados e conduzir atividades cibernéticas disruptivas e danosas. Até a presente data, o governo dos EUA atribuiu publicamente os seguintes incidentes cibernéticos aos atores cibernéticos e conspiradores patrocinados pelo Estado norte-coreano:

- ***Sony Pictures***. Em novembro de 2014, os atores cibernéticos patrocinados pela RPDC supostamente lançaram um ataque cibernético à Sony Pictures Entertainment (SPE) em retaliação ao filme "The Interview", lançado em 2014. Os atores cibernéticos da RPDC invadiram a rede da SPE para roubar dados confidenciais, tendo ameaçado executivos e funcionários da SPE e danificado milhares de computadores.

    - Atualização do FBI sobre a investigação da Sony (19 de dezembro de 2014) https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
    - Denúncia criminal do DOJ (Departamento de Justiça) referente a um programador patrocinado pelo regime norte-coreano (6 de setembro de 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***Assalto ao Banco de Bangladesh.*** Em fevereiro de 2016, atores cibernéticos patrocinados pela RPDC supostamente tentaram roubar pelo menos US$ 1 bilhão de instituições financeiras em todo o mundo e supostamente roubaram US$ 81 milhões do Banco de Bangladesh por meio de transações não autorizadas na rede da Sociedade de Telecomunicações Financeiras Interbancárias Mundiais (SWIFT). De acordo com a denúncia, os atores cibernéticos da RPDC acessaram os terminais de computadores do Banco de Bangladesh que faziam interface com a rede SWIFT, depois de terem comprometido a rede de computadores do banco por meio de e-mails de *spear phishing* direcionados a funcionários do banco. Os atores cibernéticos da RPDC enviaram mensagens SWIFT autenticadas de forma fraudulenta, direcionando o Federal Reserve Bank de Nova York a transferir fundos da conta do Banco de Bangladesh no Federal Reserve para contas controladas pelos conspiradores.

- Denúncia criminal do DOJ referente a um programador patrocinado pelo regime norte-coreano (6 de setembro de 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***WannaCry 2.0***. Atores cibernéticos patrocinados pelo Estado norte-coreano desenvolveram o ransomware conhecido como WannaCry 2.0, além de duas versões anteriores do ransomware. Em maio de 2017, o ransomware WannaCry 2.0 infectou centenas de milhares de computadores em hospitais, escolas, empresas e residências em mais de 150 países. O ransomware WannaCry 2.0 criptografa os dados de um computador infectado e permite que os atores cibernéticos exijam pagamentos de resgate na moeda digital Bitcoin. O Departamento do Tesouro apontou para um programador de computador norte-coreano por sua atuação na conspiração WannaCry 2.0, por seu papel no ataque cibernético da Sony Pictures e no assalto ao Banco de Bangladesh, e apontou também para organização para a qual trabalhava.

  - Alerta técnico da CISA: Indicadores Associados ao WannaCry Ransomware (12 de maio de 2017) https://www.us-cert.gov/ncas/alerts/TA17-132A
  - Coletiva de Imprensa da Casa Branca sobre a Atribuição do WannaCry Ransomware (19 de dezembro de 2017) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
  - Denúncia criminal do DOJ referente a um programador patrocinado pelo regime norte-coreano (6 de setembro de 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
  - O Departamento do Tesouro acusa a Coreia do Norte de vários ataques cibernéticos (6 de setembro de 2018) https://home.treasury.gov/news/press-releases/sm473

- ***Campanha FASTCash.*** Desde o final de 2016, os atores cibernéticos patrocinados pelo Estado norte-coreano empregam um esquema fraudulento de retirada de dinheiro em caixas eletrônicos conhecido como "FASTCash" para roubar milhões de dólares de caixas eletrônicos na Ásia e na África. Os esquemas FASTCash comprometem remotamente os servidores de aplicativos de trocas de pagamentos dentro dos bancos para facilitar transações fraudulentas. Durante um incidente ocorrido em 2017, os atores cibernéticos da RPDC ativaram a retirada simultânea de dinheiro em caixas eletrônicos localizados em mais de 30 países. Em outro incidente ocorrido em 2018, os atores cibernéticos da RPDC ativaram a retirada simultânea de dinheiro em caixas eletrônicos localizados em mais de 23 países.

  - Alerta da CISA sobre a campanha FASTCash (2 de outubro de 2018) https://www.us-cert.gov/ncas/alerts/TA18-275A
  - Relatório de análise de malware da CISA: Malware relacionado ao FASTCash (2 de outubro de 2018) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***Hack de Bolsa de Moeda Digital.*** Conforme detalhado nas alegações apresentadas em uma denúncia do Departamento de Justiça para confisco *in rem* em abril de 2018, os atores cibernéticos patrocinados pela RPDC *hackearam* uma bolsa de moeda digital e roubaram cerca de US$ 250 milhões em criptomoedas. A denúncia descreveu ainda como os ativos roubados foram lavados por meio de centenas de transações automáticas em moeda digital para ofuscar as origens dos fundos, na tentativa de impedir a aplicação da lei para rastrear os ativos. Dois cidadãos chineses foram incluídos na denúncia por supostamente terem feito a lavagem subsequente dos ativos em nome do grupo norte-coreano, recebendo aproximadamente $91 milhões das contas controladas pela RPDC, bem como um adicional de $9,5 milhões de um *hack* em outra bolsa. Em março de 2020, o Departamento do Tesouro apontou para dois indivíduos conforme as autoridades sancionadoras cibernéticas e da RPDC, juntamente com um anúncio do Departamento de Justiça de que os indivíduos haviam sido anteriormente indiciados por lavagem de dinheiro e por cobranças não licenciadas de remessas de dinheiro, e que 113 contas em moeda digital estavam sujeitas a confisco.

    - Sanções do Tesouro contra indivíduos que fazem lavagem de criptomoedas para o Grupo Lazarus (2 de março de 2020) https://home.treasury.gov/news/press-releases/sm924
    - DOJ Indicia Dois Cidadãos Chineses Acusados de Lavagem de Criptomoedas Decorrentes do Hack da Bolsa e Apresenta Denúncia de Confisco Civil (2 de março de 2020) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

Medidas de Combate à Ameaça Cibernética da RPDC

A Coreia do Norte tem como alvo a infraestrutura cibernética em âmbito global para gerar receita para as prioridades do seu regime, inclusive para os programas de armas de destruição em massa. Rogamos que os governos, indústria, sociedade civil e indivíduos tomem todas as medidas necessárias mencionadas abaixo para se protegerem e combaterem a ameaça cibernética da RPDC:

- **Aumentar a conscientização sobre a ameaça cibernética da RPDC.** Destacar a gravidade, o escopo e a variedade de atividades cibernéticas maliciosas realizadas pela RPDC aumentará a conscientização dos setores público e privado sobre a ameaça, e promoverá a adoção e implementação de medidas apropriadas de prevenção e mitigação de riscos.

- **Compartilhamento de Informações sobre a Ameaça Cibernética da RPDC.** O compartilhamento de informações em âmbito nacional e internacional para detecção e defesa contra as ameaças cibernéticas da RPDC permitirá maior segurança cibernética de redes e sistemas. As melhores práticas devem ser compartilhadas com os governos e o setor privado. De acordo com as disposições da Lei de Compartilhamento de Informações sobre Segurança Cibernética de 2015 (6 U.S.C. §§ 1501–1510), entidades não federais podem compartilhar indicadores de ameaças cibernéticas e

medidas defensivas relacionadas ao HIDDEN COBRA com entidades federais e não federais.

- **Implementação e Promoção das Melhores Práticas de Segurança Cibernética.** A adoção de medidas técnicas e comportamentais para reforçar a segurança cibernética contribuirá para uma infraestrutura cibernética mais segura e resiliente nos EUA e no contexto global. Instituições financeiras, incluindo empresas de prestação de serviços financeiros, devem adotar medidas independentes para se protegerem contra as atividades cibernéticas maliciosas da RPDC. Essas medidas são, por exemplo: compartilhamento de informações sobre ameaças através de canais governamentais e/ou da indústria, segmentação de redes para minimizar riscos, manutenção regular de cópias de backup de dados, treinamento focado em conscientização sobre táticas comuns de engenharia social, implementação de políticas que regem o compartilhamento de informações e acesso às redes, e desenvolvimento de planos de resposta a incidentes cibernéticos. O Modelo de Maturidade em Cibersegurança do Departamento de Energia e a Estrutura de Cibersegurança do Instituto Nacional de Padrões e Tecnologia dispõem orientações sobre o desenvolvimento e a implementação de práticas robustas de segurança cibernética. Conforme verificado no anexo I, a Agência de Segurança Cibernética e Infraestrutura (CISA) viabiliza amplos recursos, incluindo alertas técnicos e relatórios de análise de malware para permitir que os defensores de rede identifiquem e reduzam a exposição a atividades cibernéticas maliciosas.

- **Notificação aos Órgãos de Aplicação da Lei.** Na eventualidade de uma organização suspeitar que foi vítima de atividade cibernética maliciosa proveniente ou não da RPDC, é essencial notificar os Órgãos de Aplicação da Lei em tempo hábil. Isto tanto agiliza a investigação quanto, no caso de crime financeiro, pode aumentar as chances de recuperação dos ativos que foram furtados.

  As agências de aplicação da lei nos EUA apreenderam milhões de dólares em moeda digital furatada por atores cibernéticos norte-coreanos. Todos os tipos de instituições financeiras, incluindo empresas de serviços financeiros, são incentivadas a cooperar na linha de frente, respondendo às solicitações dos órgão de cumprimento da lei nos EUA quando pedem informações sobre ameaças cibernéticas, e também no processo final, identificando os bens confiscados após terem recebido solicitação das autoridades dos EUA, ou por ordem judicial, sempre cooperando com as autoridades dos EUA em apoio à busca e apreensão de tais bens.

- **Reforço do *Compliance* quanto ao Combate à Lavagem de Dinheiro (AML) / Combate ao Financiamento do Terrorismo (CFT) / Combate ao Financiamento da Proliferação (CPF)**. Os países devem implementar rápida e efetivamente os padrões do Grupo de Ação Financeira Internacional (GAFI) para AML/CFT/CPF. Isso inclui a garantia de que as instituições financeiras e outras entidades abrangidas usem medidas de mitigação de risco de acordo com os padrões, declarações e orientações públicas do GAFI. Especificamente, o GAFI pediu que todos os países apliquem contramedidas de proteção ao sistema financeiro internacional face aos

riscos financeiros contínuos da lavagem de dinheiro, financiamento do terrorismo e a proliferação que emanam da RPDC.[1] As contramedidas também visam a aconselhar todas as instituições financeiras e outras entidades abrangidas a darem especial atenção às relações e transações comerciais com a RPDC, incluindo empresas, instituições financeiras e representantes que atuam em seu nome. Em conformidade com a Resolução 2270, parágrafo 22 do Conselho de Segurança das Nações Unidas, os Estados Membros devem fechar filiais, subsidiárias e escritórios de representação dos bancos da RPDC em seus territórios e cessar as relações de correspondente com os bancos da RPDC.

Além disso, em junho de 2019, o GAFI alterou suas normas para exigir que todos os países regulem e supervisionem os provedores de serviços de ativos digitais, incluindo o câmbio de moedas digitais, e mitiguem os riscos ao realizar transações em moeda digital. Os provedores de serviços de ativos digitais devem ficar atentos às mudanças nas atividades dos clientes, pois seus negócios podem ser usados para facilitar a lavagem de dinheiro, o financiamento da proliferação e do terrorismo. Os Estados Unidos estão particularmente preocupados com plataformas que fornecem funcionalidade para pagamentos e serviços bancários anônimos sem monitoramento das transações, dos relatórios de atividades suspeitas, sem a adoção de *due diligence* de cliente, entre outras obrigações.

As instituições financeiras nos EUA, incluindo prestadores de serviços de ativos digitais localizados no exterior e que fazem negócios parciais ou integrais nos Estados Unidos, e outras empresas e pessoas abrangidas, devem garantir o cumprimento das obrigações regulatórias nos termos da Lei de Sigilo Bancário (conforme implementada pela regulamentação da Rede de Execução de Crimes Financeiros [FinCEN] do Departamento do Tesouro, no item 31 CFR, Capítulo X). Para instituições financeiras, essas obrigações incluem o desenvolvimento e a manutenção de programas eficazes de combate à lavagem de dinheiro, razoavelmente concebidos para impedir que empresas de serviços financeiros sejam usadas para facilitar a lavagem de dinheiro e o financiamento de atividades terroristas, além de identificar e reportar transações suspeitas no relatório de atividades suspeitas do FinCEN, incluindo aquelas realizadas, afetadas ou facilitadas por eventos cibernéticos ou pelo financiamento ilícito envolvendo ativos digitais.

Cooperação Internacional. Para combater as atividades cibernéticas maliciosas da RPDC, os Estados Unidos mantêm comunicação regular com os países para aumentar a conscientização sobre a ameaça cibernética da RPDC, para isso compartilhando informações e evidências por canais diplomáticos, militares, policiais e judiciais, defensores de redes, além de outros canais. Para dificultar os esforços da RPDC no sentido de subtrair fundos por meios cibernéticos e para se defender contra as atividades cibernéticas maliciosas da RPDC, os Estados Unidos instam veementemente os países a reforçarem a defesa de redes de dados, encerrar os *joint ventures* com a RPDC em países terceiros e expulsar trabalhadores norte-coreanos na área de tecnologia da

[1] *A íntegra do chamado à ação do GAFI sobre a Coreia do Norte pode ser encontrada aqui:* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html.

informação (TI) de maneira condizente com a lei internacional aplicável. Uma resolução do Conselho de Segurança da ONU de 2017 exigiu que todos os Estados Membros repatriassem cidadãos da RPDC que auferiam renda no exterior, incluindo trabalhadores de TI, até 22 de dezembro de 2019. Os Estados Unidos também buscam aumentar a capacidade dos governos estrangeiros e do setor privado para que melhor possam entender, identificar, defender-se, investigar, processar e responder a ameaças cibernéticas da RPDC, e participar dos esforços internacionais para ajudar a garantir a estabilidade do ciberespaço.

Consequências do Envolvimento em Conduta Proibida ou Sancionável

Indivíduos e entidades que estejam envolvidos ou apoiando atividades cibernéticas ligadas à RPDC, incluindo o processamento de transações financeiras relacionadas, devem estar cientes das possíveis consequências de se envolver em conduta proibida ou sancionável.

O Escritório de Controle de Ativos Estrangeiros (OFAC) do Departamento do Tesouro tem autoridade para impor sanções a qualquer pessoa que tenha, dentre outros:

- Participado de atividades significativas que comprometam a segurança cibernética em nome do governo da Coreia do Norte ou do Partido dos Trabalhadores da Coreia;
- Trabalhado na indústria de tecnologia da informação (TI) na Coreia do Norte;
- Participado de outras atividades cibernéticas maliciosas; ou
- Participado de pelo menos uma atividade significativa de importação ou exportação de quaisquer bens, serviços ou tecnologia para a Coreia do Norte.

Além disso, se o Secretário do Tesouro, em consulta com o Secretário de Estado, determinar que uma instituição financeira estrangeira conduziu ou facilitou intencionalmente atividades significativas de comércio com a Coreia do Norte, ou conduziu ou facilitou intencionalmente uma transação significativa em nome de uma pessoa apontada conforme previsto em uma Ordem Executiva relacionada à Coreia do Norte, ou conforme previsto na Ordem Executiva 13382 (Proliferadores de Armas de Destruição em Massa e Seus Apoiadores) para atividades relacionadas à Coreia do Norte, tal instituição pode, entre outras restrições potenciais, perder o direito de manter uma conta correspondente ou que processe pagamento nos Estados Unidos.

O OFAC investiga as aparentes violações dos seus regulamentos de sanções e exerce autoridade de execução, conforme descrito nas Diretrizes de Aplicação de Sanções Econômicas, 31 C.F.R. parte 501, apêndice A. As pessoas que violarem os Regulamentos de Sanções impostas à Coreia do Norte, 31 C.F.R. parte 510, podem enfrentar penalidades monetárias civis, chegando até às penas máximas legais aplicáveis ou ao dobro do valor da transação subjacente.

O relatório intercalar do POE de 2019 observa que o uso e a tentativa de uso da RPDC de meios cibernéticos para roubar fundos de bancos e de bolsas de moedas digitais, pode representar uma violação de várias resoluções do Conselho de Segurança das Nações Unidas (UNSCRs) (*i.e.*, parágrafo operacional do UNSCR 1718 (OP) 8(d); UNSCR 2094, PO 8 e 11; e UNSCR 2270, OP 32). As Resoluções do Conselho de Segurança das Nações Unidas (UNSCR) relativas à RPDC também preveem vários mecanismos para incentivar o cumprimento das sanções relacionadas à RPDC impostas pela ONU. Por exemplo, o Comitê 1718 do Conselho de

Segurança da ONU pode impor sanções específicas (*i.e.*, congelamento de ativos e, para indivíduos, proibição de viagens) a qualquer indivíduo ou entidade que se envolva em uma transação comercial com entidades designadas pela ONU ou evasão de sanções.

O Departamento de Justiça processa criminalmente violações intencionais das leis de sanções aplicáveis, tais como a Lei Internacional de Poderes Econômicos de Emergência 50 U.S.C. §§ 1701 e segs. As pessoas que deliberadamente violarem tais leis podem enfrentar até 20 anos de prisão, multas de até US$ 1 milhão ou totalizando o dobro da renda bruta, o que for maior, e o confisco de todos os fundos envolvidos em tais transações. O Departamento de Justiça também processa criminalmente violações intencionais da Lei de Sigilo Bancário (BSA), 31 U.S.C. §§ 5318 e 5322, que exige que as instituições financeiras mantenham, entre outras determinações, programas eficazes de combate à lavagem de dinheiro e apresentem determinadas denúncias ao FinCEN. As pessoas que violarem a BSA podem enfrentar até 5 anos de prisão, uma multa de até US$ 250.000 e possível confisco dos bens envolvidos nas violações. Quando apropriado, o Departamento de Justiça também processará criminalmente empresas e outras entidades que violarem essas leis. O Departamento de Justiça também trabalha com parceiros estrangeiros para compartilhar provas em apoio às investigações criminais e processos judiciais.

De acordo com o título 31 do US Code §5318 (k), o Secretário do Tesouro ou o Procurador Geral pode intimar uma instituição financeira estrangeira que mantém uma conta bancária correspondente nos Estados Unidos a apresentar registros armazenados no exterior. Quando o Secretário do Tesouro ou o Procurador Geral notificar por escrito a uma instituição financeira dos EUA que uma instituição financeira estrangeira não cumpriu tal intimação, a instituição financeira dos EUA deve encerrar o relacionamento bancário correspondente dentro de dez dias úteis. Caso contrário, as instituições financeiras americanas poderão estar sujeitas a penalidades civis diárias.

Recompensas para Levar a RPDC à Justiça

Caso você tenha informações sobre atividades ilícitas da RPDC no ciberespaço, incluindo operações passadas ou em curso, o fornecimento de tais informações por meio do programa *Rewards for Justice* do Departamento de Estado poderá torná-lo elegível a receber um prêmio de até US$ 5 milhões. Para mais detalhes, visite www.rewardsforjustice.net.

ANEXO I: Informações Públicas do Governo dos EUA e Recursos de Combate a Ameaças Cibernéticas da RPDC

Gabinete do Diretor de Inteligência Internacional para Avaliação de Ameaças Mundiais da Comunidade de Inteligência dos EUA. Em 2019, a Comunidade de Inteligência dos EUA concluiu que a RPDC representa uma ameaça cibernética significativa para as instituições financeiras e continua sendo uma ameaça de espionagem cibernética, tendo a capacidade de realizar ataques cibernéticos disruptivos. A RPDC continua usando recursos cibernéticos para furtar de instituições financeiras e gerar receita. As operações de crimes cibernéticos de Pyongyang incluem tentativas de furtar mais de US$ 1,1 bilhão de instituições financeiras em todo o mundo - incluindo um roubo cibernético bem sucedido estimado em US$ 81 milhões do Banco de Bangladesh. O relatório pode ser encontrado em https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Relatórios Técnicos da Agência de Segurança Cibernética e Infraestrutura (CISA). O governo dos EUA refere-se às atividades cibernéticas maliciosas da RPDC como HIDDEN COBRA. Os relatórios HIDDEN COBRA fornecem detalhes técnicos sobre as ferramentas e a infraestrutura usadas pelos atores cibernéticos da RPDC. Tais relatórios permitem que os defensores de rede identifiquem e reduzam a exposição às atividades cibernéticas maliciosas da RPDC. O website da CISA contém as últimas atualizações sobre ameaças persistentes: https://www.us-cert.gov/northkorea.

Além disso, a CISA fornece amplo conhecimento e práticas de segurança cibernética e de infraestrutura aos principais interessados, bem como compartilha tais conhecimentos para permitir melhor gestão de riscos, com o intuito de proteger funções críticas da nação. Esses são os links de acesso aos recursos da CISA:

- Proteção à infraestrutura crítica: https://www.cisa.gov/protecting-critical-infrastructure
- Segurança cibernética: https://www.cisa.gov/cyber-safety
- Detecção e prevenção: https://www.cisa.gov/detection-and-prevention
- Compartilhamento de informações: https://www.cisa.gov/information-sharing-and-awareness
- Insights da Cisa: https://www.cisa.gov/insights
- Combate ao crime cibernético: https://www.cisa.gov/combating-cyber-crime
- Informações essenciais sobre cibernética: https://www.cisa.gov/cyber-essentials
- Dicas: https://www.us-cert.gov/ncas/tips
- Sistema nacional de conscientização cibernética: https://www.us-cert.gov/ncas
- Consultoria em Sistemas de Controle Industrial: https://www.us-cert.gov/ics
- Como relatar incidentes, phishing, malware e vulnerabilidades: https://www.us-cert.gov/report

Relatórios PIN e FLASH do FBI. O sistema de Private Industry Notifications (PIN) do FBI fornece informações atuais que aumentam a percepção do setor privado sobre possíveis ameaças cibernéticas. Os relatórios emitidos pelo Liaison Alert System (FLASH) do FBI contêm informações críticas coletadas pelo FBI para uso por parceiros específicos no setor privado. O objetivo é fornecer aos destinatários inteligência a ser usada para ajudar os profissionais de

segurança cibernética e os administradores de sistemas a se protegerem contra as ações maliciosas persistentes dos criminosos cibernéticos Caso você identifique alguma atividade suspeita na sua empresa ou tenha informações pertinentes, entre em contato imediatamente com o FBI CYWATCH. Para relatórios PIN ou FLASH sobre ameaças cibernéticas relacionadas à RPDC, entre em contato com cywatch@fbi.gov.

- Divisão Cibernética do FBI: https://www.fbi.gov/investigate/cyber
- Programa de Adido Jurídico do FBI: a principal missão do Adido Jurídico do FBI é estabelecer uma ligação contínua com os principais serviços responsáveis pela aplicação da lei e de segurança em países estrangeiros designados. https://www.fbi.gov/contact-us/legal-attache-offices

Divulgação de Informações sobre Malware do Comando Cibernético dos E.U.A. As forças cibernéticas do Departamento de Defesa buscam permanentemente por atividades cibernéticas maliciosas da RPDC, incluindo malware da RPDC que explora instituições financeiras, realiza espionagem e permite atividades cibernéticas maliciosas contra os EUA e seus parceiros. O Comando Cibernético dos EUA publica informações periódicas sobre malware, identificando vulnerabilidades para a indústria e o governo na defesa das suas infraestruturas e redes contra atividades ilícitas da RPDC. Informações sobre malware para reforçar a segurança cibernética podem ser encontradas nas seguintes contas do Twitter: @US_CYBERCOM e @CNMF_VirusAlert.

Informação sobre Sanções do Departamento do Tesouro dos EUA e Consultas sobre Financiamento Ilícito. O Centro de Recursos on-line do ***Escritório de Controle de Ativos Estrangeiros*** (OFAC's) fornece uma gama de informações sobre sanções impostas à Coreia do Norte e sanções relativas a atividades cibernéticas maliciosas, incluindo assessorias sobre sanções, estatutos relevantes, ordens executivas, normas e regulamentos relacionado à RPDC e sanções cibernéticas. O OFAC também publicou várias perguntas frequentes (FAQs) relacionadas às sanções à RPDC, sanções cibernéticas e moeda digital. Para questões ou esclarecimentos relacionados aos regulamentos e requisitos de sanções do OFAC, entre em contato pelo telefone direto 1-800-540-6322 ou pelo e-mail OFAC_Feedback@treasury.gov.

- Sanções impostas à RPDC
    - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
    - Perguntas frequentes - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- Sanções contra atividades cibernéticas maliciosas
    - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
    - Perguntas frequentes - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber
    - Perguntas frequentes sobre moeda virtual - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

A Rede de Execução de Crimes Financeiros (FinCEN) emitiu um parecer sobre o uso do sistema financeiro internacional pela Coreia do Norte (https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008). O FinCEN também emitiu orientações específicas para instituições financeiras das quais se exige

notificação de atividades suspeitas, aconselhando-as sobre quando e como denunciar crimes cibernéticos e/ou atividades criminosas relacionadas a moedas digitais.

- Crime cibernético
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- Atividades ilícitas em moeda digital
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- E-mails de empresas comprometidos por atividades fraudulentas
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

O ***Conselho Federal de Exame de Instituições Financeiras (FFIEC)*** desenvolveu a Ferramenta de Avaliação de Segurança Cibernética para ajudar instituições financeiras a identificar riscos e determinar se estão devidamente preparadas quanto à segurança cibernética. A ferramenta de avaliação pode ser encontrada em https://www.ffiec.gov/cyberassessmenttool.htm.

ANEXO II: Relatórios do painel de especialistas da ONU sobre ameaças cibernéticas da RPDC

Relatórios do Painel de Especialistas do Comitê de Sanções da ONU 1718 (RPDC). O Comitê de Sanções do Conselho de Segurança das Nações Unidas 1718 sobre a RPDC é assessorado por um Painel de Especialistas, que "reúne, examina e analisa informações" dos Estados Membros da ONU, órgãos relevantes da ONU e outras partes sobre a implementação das medidas delineadas nas Resoluções do Conselho de Segurança da ONU contra a Coreia do Norte. O Painel também faz recomendações sobre como aperfeiçoar a implementação de sanções, fornecendo um Relatório Intercalar e Final ao Comitê 1718. Os relatórios podem ser encontrados em https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports.