Métodos digitais para contornar as sanções da ONU
Um estudo de caso da Cyber Force da República Popular Democrática da Coreia

Por Ashley Taylor

Introdução

A ciberesfera é uma nova linha da frente na implementação e contorno das sanções da ONU. Como a Internet fornece um espaço virtual para comunicação e transação instantâneas, ela abre inerentemente caminhos mais baratos e não regulamentados para os intervenientes desonestos violarem as normas internacionais. Os usos ilícitos das tecnologias digitais superam os avanços dos tecnólogos lícitos, que geralmente não dão prioridade à segurança internacional nos seus negócios.

A República Popular Democrática da Coreia (RPDC), em particular, tornou-se cada vez mais adepta da utilização de instrumentos digitais para contornar as sanções. Desenvolveram técnicas digitais para gerar receitas para financiar os seus esforços ilegais de proliferação, adquirir informações e conhecimentos técnicos e prejudicar os negócios e a reputação dos seus adversários estrangeiros, nomeadamente para perturbar os que acompanham a aplicação do regime de sanções da RPDC adotado com a Resolução 1718 da ONU em outubro de 2006. Kim Jong-un vangloriou-se recentemente afirmando que "A guerra cibernética, juntamente com armas nucleares e mísseis, é uma 'espada para todos os fins' que garante a capacidade dos nossos militares de atacar implacavelmente"[1] Um desertor militar norte-coreano relatou que a força cibernética é vista como a arma mais forte na "Guerra Secreta" e[2] os seus membros são considerados parte da elite, sendo uma das poucas posições bem pagas.

Até onde eles irão no futuro? Evidências sugerem que intervenientes estatais norte-coreanos e representantes não-estatais estão cada vez mais a fazer uso de novas tecnologias de anonimato, como cibermoeda, a dark web, criptografia e ciberataques avançados difíceis de detetar. O relatório do Painel de Peritos da ONU sobre a RPDC estimou que eles ganharam 571 milhões de dólares dos EUA apenas em roubos de cibermoeda.

Este estudo de caso concentrar-se-á primeiramente nas origens da força cibernética da Coreia do Norte, analisando ataques documentados realizados usando métodos tradicionais de hacking, delineando táticas observadas a partir de intrusões e ataques passados e analisando relatórios sobre adaptações norte-coreanas a tecnologias mais avançadas. Este artigo concluirá com recomendações de medidas de cibersegurança e orientações regulamentares a adoptar.

Sanções cibernéticas e da ONU: O contexto regulamentar

[1] de acordo com um relatório do think tank sedeado em Washington, o Centro de Estudos Estratégicos e Internacionais

[2] https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205

Empresários de tecnologia que exploram o potencial perturbador e transformador ricamente gratificante das tecnologias digitais foram historicamente incentivados por normas regulatórias suaves. No entanto, o reconhecimento do impacto potencialmente prejudicial dessas novas tecnologias para questões políticas, sociais e de segurança está agora a mobilizar reguladores europeus e norte-americanos para intervir contra, e disciplinar, empresas de tecnologia que estão a violar normas nacionais e internacionais.

Embora as estruturas ciber-regulatórias nacionais tenham sido adotadas por 138 países, a maioria concentra-se na prevenção do crime doméstico, mantendo-se felizmente separada das implicações de segurança internacional[3] de uma ciberesfera armada. O Conselho de Segurança da ONU abordou as ameaças cibernéticas apenas de forma irregular e inconsistente, apesar de ter 20 anos de relatórios e evidências sobre como a tecnologia digital tem impulsionado conflitos e beneficiado os intervenientes sancionados. Até à data, apenas o Grupo de Acção Financeira Internacional (GAFI) está a alterar gradualmente as suas 40 recomendações para prevenir e proteger contra as variações digitais do combate ao branqueamento de capitais (AML), ao financiamento da luta contra o terrorismo (CTF) e ao financiamento da não proliferação.

Houve alguns passos unilaterais no sentido de sanções cibernéticas. Por exemplo, os EUA sancionaram duas contas de criptomoeda pertencentes a indivíduos iranianos, e a UE divulgou algumas orientações, incluindo um conjunto de ferramentas para a ciberdiplomacia. No entanto, estas medidas estão longe da abordagem global que é necessária.

Conforme descrito nas secções a seguir, o uso diversificado de tecnologias digitais pela Coreia do Norte exemplifica o desafio multifacetado de aplicar sanções na esfera cibernética. A capacidade demonstrada da RPDC para realizar ataques cibernéticos monumentais, mas pouco percetíveis e baratos a dados ou ativos financeiros pertencentes a governos, empresas e indivíduos é um enorme motivador para adotar ferramentas ofensivas de guerra digital e de informação. Também é necessário que os líderes da indústria e os decisores políticos abordem o papel que aplicações civis aparentemente inócuas, como criptomoeda ou escudos de identidade online, desempenham.

A nível internacional, as sanções existentes contra a Coreia do Norte não classificam os abusos da ciberinfra-estrutura internacional como atos sancionáveis. Considerando a natureza nebulosa de lidar com ameaças cibernéticas relacionadas à Coreia do Norte, os líderes passivos do governo e da indústria correm o risco de:
(1) norte-coreanos atacam ou se preparam para atacar os seus sistemas de computador, levando à perda de receitas, dados críticos e capacidades operacionais;
(2) falhas de conformidade e perda de reputação por permitir ações norte-coreanas que resultam em violações de sanções; e
(3) serem deixados para trás nos esforços e iniciativas para regular a indústria tecnológica, com implicações potencialmente abrangentes para a sua economia e segurança nacional.
Além disso, em regiões onde a indústria de cibersegurança e a supervisão governamental não têm caminhos bem estabelecidos para o compartilhamento de conhecimento e a colaboração, há menos potencial para responder de forma eficaz e/ou responsável aos ciberataques.

Força cibercética da RPDC

Estima-se que a Coreia do Norte tenha até 6.000 guerreiros cibernéticos, organizados em diferentes grupos conhecidos como Lazarus, Bureau 121, Hidden Cobra, Bluenoroff, Apt 38, TEMP.Hermit e Andariel. Um dos principais contribuintes para o arsenal cibernético da Coreia do Norte é a canalização pelo sistema educacional da Coreia do Norte, desde tenra idade, das melhores mentes técnicas em ciência e

[3] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

matemática para cursos de ciência da computação e engenharia e, eventualmente, para a Universidade de Ciência e Tecnologia de Pionguiangue (PUST), a única universidade estrangeira financiada no país. A PUST foi aberta em 2010 com um contrato entre o governo norte-coreano e a Fundação para a Educação e Cultura do Nordeste Asiático (NAFEC). Alguns voluntários estrangeiros trabalham na universidade, enquanto outros vêm durante algumas semanas para ensinar um curso.

Em 2015, o desertor norte-coreano Jang Se-yul, que diz fazer parte do comando de guerra cibernética de Pyongyang, informou que as formações na PUST preparam os alunos para hackear. A PUST rejeita estas alegações, alegando provas inadequadas. Independentemente disso, é verdade que um subproduto da aprendizagem de engenharia e segurança informática está a adquirir a base para a forma de hackear. Noções básicas de ciência da computação, como escrever programas de computador, criar algoritmos (procedimentos para análise de dados) e interface com um sistema operacional de computador também fazem parte integrante do hacking. Qualquer estudante legítimo de cibersegurança eventualmente realizará experiências de hacking "white hat", onde tentam invadir redes de informação para expor as suas vulnerabilidades.

Assim que estiverem devidamente treinados, alguns alunos juntam-se à força cibernética localizada na Coreia do Norte, enquanto outros se juntam a equipas estrangeiras para realizar esforços de hacking ou vão para o estrangeiro para iniciar empresas de fachada para ajudar a contornar as sanções[4]. Empresas de segurança privada analisaram as atividades de internet de utilizadores com sede na RPDC para entender a rede de apoiantes no estrangeiro e encontraram evidências de apoiantes fisicamente localizados ou residentes no Bangladesh, na China, na Índia, na Indonésia, no Quénia, em Moçambique, no Nepal e na Tailândia[5].

Uma arma importante para este pipeline de talentos é o uso das tecnologias mais avançadas, como técnicas de anonimato que permitem ataques anónimos e criptomoeda, que permitem novas formas de gerar fundos e transferir secretamente ganhos hackeados. Demonstrando a sua capacidade de adotar as últimas tendências cibernéticas, a RPDC organizou uma conferência de blockchain e criptomoeda na PUST em abril de 2019, organizada com a ajuda de um empresário do Reino[6] Unido.

As tecnologias de anonimização mais importantes que a Coreia do Norte usa, e as auxiliares, são explicadas na tabela a seguir.

Tecnologias para ataques anónimos e tecnologias de evasão às sanções

Descrição e utilização pela RPDC
Intranet	uma rede de fechada não ligada à rede mundial livre e aberta; uma coleção interna de servidores e computadores em rede que só permite o acesso a determinadas páginas e ficheiros (por exemplo, a infraestrutura de Internet da RPDC é uma Intranet chamada Kwangmyong que só é acessível a partir do interior das fronteiras da Coreia do Norte)

[4] https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205

[5] https://www.recordedfuture.com/north-korea-internet-usage/

[6] https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-cryptocurrency-blockchain-conference-pyongyang-a8643391.html

evasão às sanções	Descrição e utilização pela RPDC
dark web	a parte da Internet que não é indexada por mecanismos de busca populares, como o Google ou o Yahoo, o que significa que as páginas não são fáceis de descobrir, exceto se o utilizador souber onde procurar; onde a atividade ilegítima pode ocorrer sem ser detetada, como fóruns e mercados para a aquisição de armas, propriedade intelectual roubada, etc.
Tor	um navegador que permite o acesso à dark web. Pode ser descarregado gratuitamente por qualquer pessoa que tenha acesso à Internet
encriptação	codificação de dados com códigos secretos apenas possuídos pelos participantes pretendidos. Ela é usada para mensagens encriptadas, para que as informações possam passar por protocolos da Internet sem serem detetadas e também é usada como um elemento fundamental de design na criação de criptomoeda. Os norte-coreanos usaram a aplicação chinesa de mensagens encriptadas WeChat para coordenar transferências de navio para navio
criptomoedas	um tipo de moeda digital, em que cada versão tem regras específicas sobre a forma como as moedas surgem e como podem ser utilizadas. Utiliza encriptação para tornar as moedas difíceis de falsificar e fornecer anonimato aos utilizadores, o que significa que a identidade do mundo real não é necessária para adquiri-las ou comercializá-las. Cada criptomoeda, da qual há milhares, tem as suas próprias regras e procura de mercado para a obtenção de moedas. As transações são registadas num registo partilhado, chamado blockchain
blockchain	uma base de dados que é composta por um livro razão de transações de uma criptomoeda específica. Assim que as entradas são feitas, elas são muito difíceis/dispendiosas de mudar, portanto, é uma maneira útil de rastrear dados "confiáveis" ao longo do tempo. Cada transação é sempre visível para toda a rede. A moeda nativa de cada blockchain geralmente é necessária para interagir na rede. Essas redes de blockchain e as suas moedas podem ser públicas, como a Bitcoin, ou privadas, apenas utilizáveis por um grupo selecionado
rede privada virtual (VPN)	um serviço que permite a um utilizador criar um portal privado para aceder anonimamente à Internet pública, pelo que os seus dados, informações e acesso à Web não podem ser controlados e/ou o conteúdo não pode ser observado ou censurado
servidor privado virtual (VPS)	um serviço para hospedar aplicações da web que não requer o uso de um servidor de terceiros, como Google, Microsoft ou Amazon
segurança da camada de transporte (TLS)	um nível adicional de criptografia adicionado às redes de informação para garantir que todos os dados transferidos através da rede sejam difíceis de obter/observar
redes sociais	vizinhanças online, ou os lugares na esfera digital onde as pessoas interagem. No caso da RPDC, as redes sociais são úteis para promover a sua propaganda junto dos seus apoiantes no estrangeiro, bem como para criar contas fraudulentas para promover empresas de fachada e realizar outras táticas de pirataria informática sem revelar a sua verdadeira identidade

A partir de abril de 2018, os pesquisadores de segurança encontraram um aumento de 1.200% no uso desses serviços privados de Internet, que ajudam os norte-coreanos nas suas pesquisas e ataques. Estas ferramentas, combinadas com a altamente censurada Intranet Kwangmyong da RPDC, limitam a capacidade das agências estrangeiras de inteligência cibernética e segurança para compreender plenamente a força cibernética da Coreia do Norte.[7]

Os norte-coreanos ainda usam a web pública, especialmente as redes sociais, para coordenar as evasões a sanções. Eles têm vindo a afastar-se das redes sociais e meios de comunicação ocidentais desde o fim de 2017 a favor das versões chinesas, onde se assimilam mais facilmente sem serem identificados. Uma exceção notável é o uso contínuo do LinkedIn, que provavelmente continua a ser útil para criar falsas personas (ou seja, uma pessoa sem afiliações norte-coreanas) para promover empresas de fachada, criar relacionamentos com potenciais vítimas de ciberataques e entender como melhor hackeá-las e promover oportunidades de negócios, como novas moedas digitais. Estas incidências são descritas mais detalhadamente nas próximas secções.

Técnicas utilizadas pela RPDC para contornar sanções

A tabela a seguir é uma descrição das técnicas utilizadas eplos norte-coreanos numa variedade de ataques.

Técnicas	Descrição
malware	hackers instalam um programa de computador prejudicial no computador das vítimas, que pode realizar qualquer número de metas, como dar ao hacker acesso ao computador
botnet	quando hackers se apoderam de muitos computadores e constroem uma infraestrutura para coordenar ataques que precisam de grandes quantidades de poder de processamento, como DDOS (próximo)
negação de serviços distribuída (DDOS)	usando muitos computadores (geralmente botnets) para tentar aceder a uma determinada página da Web para que ela fique sobrecarregada e deixe de funcionar. O ataque geralmente visa prejudicar o negócio (por exemplo, incapacidade de funcionamento normal do comércio)
phishing	envio de comunicações falsas, como emails falsos, que enganam os utilizadores para inserir as suas palavras-passe numa página da Web de propriedade dos hackers e/ou fazer o download de um ficheiro falso que contenha malware
Spearphishing	semelhante ao phishing, exceto que as vítimas são mais cuidadosamente visadas, depois de uma pesquisa de antecedentes pelos invasores, para determinar que vítima será mais suscetível, como criar uma conta falsa e fazer amizade com ela nas redes sociais.

[7] https://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/#more-29249
relatório de utilização da Internet

Técnicas	Descrição
exploração de vulnerabilidade do sistema	encontrar lacunas na infraestrutura/nos sistemas operacionais, como o Microsoft Windows, que dará aos hackers acesso ao computador. Essas brechas são úteis para os hackers coordenarem ataques generalizados a muitas vítimas de uma só vez, todas usando o mesmo software com essa vulnerabilidade.
vírus	um programa de computador projetado para infetar computadores e causar um resultado específico (por exemplo, destruir ficheiros, roubar informações) que se auto-propaga, o que significa encontrar uma maneira de infetar tantos computadores quanto possível através do computador infetado, causando danos em larga escala num computador num curto período de tempo
negociação/troca de criptomoedas	uma próspera indústria de serviços que permite aos utilizadores transferir criptomoedas para outras criptomoedas e fiat (moeda produzida pelo estado). Relativamente aos norte-coreanos, essas transferências podem transformar moedas roubadas em dinheiro e/ou facilmente ofuscar uma trilha de propriedade de moedas roubadas, passando de uma criptomoeda para outra. Existem muitas trocas de criptomoedas que permitem negociar sem qualquer regulação.
mineração de criptomoedas	Cada criptomoeda tem regras especificadas sobre como novas moedas podem ser obtidas, o que geralmente requer o uso de computadores especializados com poderosas GPUs para processar dados constantemente enquanto eles competem para ganhar novas moedas libertadas num determinado período de tempo.
oferta inicial de contribuição (ICO)	a criação de uma nova criptomoeda com um fundraiser conduzido para pré-venda de uma parte das moedas, com promessas de como os utilizadores poderão usar as moedas, muitas vezes com o subtexto de um retorno financeiro
ataque watering hole	o invasor compromete um site de interesse do(s) destino(s) pretendido(s) e adiciona código para enganar o utilizador para aceder a uma nova página da Web que os levará a instalar malware
ransomware (tipo de vírus)	um malware que criptografa o disco rígido das vítimas e exige resgate num período de tempo limitado, se quiser que os seus dados sejam devolvidos e não destruídos

Métodos específicos empregues para evasão de sanções

Embora as técnicas descritas acima possam ser componentes autónomos de um ataque ou aquisição, muitas vezes elas são combinadas nos seguintes métodos e repetidas em múltiplas incidências.

Métodos para prejudicar adversários, roubar informações e, por vezes, exigir resgate

Os norte-coreanos têm um histórico de ataques cibernéticos para prejudicar os seus adversários. Eles foram capazes de causar danos massivos, como no caso do ataque à Sony Pictures. Em resposta ao próximo lançamento de um filme que retratou o assassinato de Kim Jong-un, hackers da RPDC destruíram ficheiros, vazaram informações confidenciais, como informações de pagamento de funcionários que levaram a uma crise de igualdade de género para a empresa e causaram cerca de 100 milhões de dólares dos EUA em danos cibernéticos relacionados à empresa.

Tal como ilustrado no quadro seguinte, os ataques da RPDC estão a evoluir no sentido de incorporar formas de gerar receitas, para além de causarem danos. O vírus Wannacry em 2017 espalhou-se por todo o mundo, infetando computadores e criptografando todos os seus dados. O Wannacry ativou então

uma exigência urgente de um pagamento de resgate em bitcoin, se os utilizadores quisessem os seus dados de volta. Como as bitcoins são difíceis de associar aos seus proprietários do mundo real, é muito difícil saber o quanto os norte-coreanos realmente geraram a partir deste ataque. Pelo menos 140.000 dólares dos EUA foram rastreados, embora o número real seja provavelmente muito superior. No entanto, os danos causados às empresas infetadas foram de milhões e muitas vezes causaram resultados catastróficos, como desligar computadores críticos em hospitais do Reino Unido.

Incidências (ordem temporal)	**Técnicas utilizadas**	**Danos provocados conhecido**
DDOS (2009)	botnet, ddos	31 milhões a 46 milhões de dólares dos EUA em danos
DDOS (20011)	botnet, ddos	40 sites, 820 discos duros afetados
320 Dark Seoul (2013)	especulação, malware	dados destruídos, 75 milhões de dólares dos EUA em reparações
Sony Pictures (2014)	especulação, malware	tentativa mal sucedida de resgate de informações confidenciais roubadas, em seguida, vazou a informação causando danos à reputação e custo para reparar sistemas de computador ~100 milhões de dólares dos EUA
Korea Hydro & Nuclear Power Attack (2014)	especulação, malware	atacaram 3.571 funcionários da Korea Hydro e tentaram destruir os seus discos de PC. Os hackers obtiveram e divulgaram plantas de seis fábricas nucleares em seis ocasiões diferentes no Twitter e exigiram 10 mil milhões de dólars dos EUA
Interpark (2016)	malware	vazou informações privadas de 10,3 milhões de utilizadores, tentou pedido de resgate em Bitcoin de 2,7 milhões de dólares dos EUA
empresas não divulgadas na indústria de defesa (2016)	exploração de vulnerabilidade do sistema	dados classificados obtidos e vazados, como plantas de aeronaves
Autoridade de Supervisão Financeira polaca (2017), entre outros alvos	ataque watering hole, malware	enviou bancos em visita ao site para uma página alternativa onde foi pedido às vítimas que descarregassem malware. Talvez tenha sido usado nos ataques Swift (próxima secção)
Vírus Wannacry (2017)	exploração de vulnerabilidade do sistema para inserir um ransomware que encriptava ficheiros de computadores de destino e exigia resgate de	pelo menos 140.000 dólares dos EUA ganhos em criptomoedas, danos críticos causados a empresas e instituições como hospitais do Reino Unido

Incidências (ordem temporal)	Técnicas utilizadas	Danos provocados conhecido
	bitcoin para os mesmos	
Painel de Peritos da ONU para a RPDC	desconhecido	sabotou a comissão atrasando a publicação do seu relatório sobre a RPDC

Métodos puramente geradores de receita

Nos últimos anos, os norte-coreanos têm mostrado preferência pela geração de fundos com a sua experiência cibernética. Em fevereiro de 2016, hackers norte-coreanos fizeram spearphishing em funcionários do Banco Central do Bangladesh e instalaram malware para obter as suas credenciais legítimas para o sistema global de mensagens interbancárias SWIFT. Eles então comprometeram a conta do Bangladesh na Reserva Federal dos EUA e tentaram transferir 951 milhões de dólares dos EUA dos fundos do banco para contas em todo o mundo, enquanto apenas conseguiam adquirir 81 milhões de dólares dos EUA. O dinheiro foi para uma conta nas Filipinas e foi branqueado através de várias contas bancárias, um negócio de remessa de dinheiro e casinos[8]. Este mesmo ataque foi tentado muitas outras vezes em bancos em todo o mundo, com outros hacks bem sucedidos ganhando 10 a 15 milhões de dólares dos EUA cada.

Após esses ataques, os hackers norte-coreanos começaram a concentrar os seus esforços em trocas de criptomoeda, os serviços que atuam como bancos online para trocar a multitude de criptomoedas. Os perpetradores visam as carteiras digitais onde as trocas de criptomoeda armazenam os fundos mantidos entre transações para clientes. Estas carteiras são alvos muito lucrativos porque contêm enormes volumes de fundos de clientes. Roubar as assinaturas digitais (palavras-passe) que controlam essas carteiras e reapropriar os fundos gera ganhos muito significativos.

A RPDC foi responsável por 75% dos hacks de câmbio de criptomoeda comunicados globalmente (um total de 882 milhões de dólare s dos EUA) do fim de 2016 até ao outono de 2018. Este rendimento digital é difícil de localizar e pode, por conseguinte, ser utilizado para contornar ou contrariar o congelamento de bens e outras sanções da ONU.

Incidências dignas de nota (ordem temporal)	Técnicas utilizadas	Danos realizados / impactos estimados
Assalto cibernético ao Banco do Bangladesh (2016)	spearphishing, malware, transferência bancária fraudulenta de Swift	roubou 81 milhões de dólares dos EUA

[8] https://www.thecipherbrief.com/kim-digs-cybercrime-coin-sanctions-cant-snatch

Incidências dignas de nota (ordem temporal)	Técnicas utilizadas	Danos realizados / impactos estimados
Casinos online pirateados (2016, 2017)	malware, inseriu uma fraude em jogos de azar	desconhecido
Banco Internacional do Extremo Oriente (2017)	spearphishing, malware, transferência bancária fraudulenta de Swift	60 milhões de dólares dos EUA transferidos, mas a maioria recuperada
Standard Chartered Plc - Bancomext (2018)	spearphishing, malware, transferência bancária fraudulenta de Swift	tentativa infrutífera de hackear 110 milhões de dólares dos EUA, embora 15 milhões de dólares dos EUA tenham sido roubados de outros ataques a bancos mexicanos
Banco do Chile (2018)	spearphishing, malware, transferência bancária fraudulenta de Swift	10 milhões de dólares dos EUA adquiridos, transferidos em grande parte para contas em Hong Kong
Loja Open Bazar para produtos norte-coreanos - (desde 2016)	criou uma loja para vender itens especiais norte-coreanos, como cigarros, dinheiro e selos	desconhecido
Câmbio de criptomoeda Yazipon (2017)	spearphishing para obter palavra-passe para a conta de câmbio, troca de criptomoedas	5,3 milhões de dólares dos EUA roubados
Malware de mineração Andariel (2017)	malware instalado que minerava criptomoeda no computador dos destinatários	70 moedas onero, 26.000 dólares dos EUA ganhos
Câmbio de criptomoeda exchange (2017)	spearphishing para obter palavra-passe para a conta de câmbio, troca de criptomoedas	7 milhões de dólares dos EUA roubados
Câmbio de criptomoeda Youbit (2017)	spearphishing para obter palavra-passe para a conta de câmbio, troca de criptomoedas	5,6 milhões de dólares dos EUA roubados
Câmbio de criptomoeda Coincheck (2018)	spearphishing para obter palavra-passe para a conta de câmbio com uma nova criptomoeda NEM Coin, troca de criptomoeda	534 milhões de dólares dos EUA roubados

Incidências dignas de nota (ordem temporal)	Técnicas utilizadas	Danos realizados / impactos estimados
Câmbio de criptomoeda Bitthumb (2018)	spearphishing para obter palavra-passe para a conta de câmbio, troca de criptomoedas	32 milhões de dólares dos EUA roubados
Interstellar, Stellar, HOLD, ou HUZU (2018)	uma Oferta Inicial de Moedas (ICO) para uma nova criptomoeda; o nome foi alterado muitas vezes para tentar ofuscar as origens	desconhecido
MarineChain (2018)	uma ICO para uma nova criptomoeda que alegava fraudulentamente vender a propriedade de grandes navios.	fundos desconhecidos obtidos à medida que o projeto se dissipava quando exposto. No entanto, aponta para um novo meio de contornar as sanções aplicáveis ao transporte marítimo, criando uma nova forma de ofuscar a propriedade de um navio
Mineração/troca de criptomoedas (2015 até ao presente)	usar computadores na Coreia do Norte para minerar várias criptomoedas e depois convertê-las em moeda utilizável ou negociar por outros bens	Estimativa de 150.000 a 200.000 dólares americanos ganhos por ano

É claro que, ao longo do tempo, os hackers norte-coreanos estão a movimentar-se para ataques geradores de receita, especialmente aqueles que tiram proveito de normas regulatórias fracas à volta das criptomoedas. Os norte-coreanos mostram claramente que estão preparados para tirar partido das tendências tecnológicas. Os seus hacks de câmbio de criptomoedas e ICOs coincidem perfeitamente com uma mania especulativa no fim de 2017 até ao início de 2018, quando o valor de mercado das moedas digitais atingiu o seu pico mais alto até agora. O mercado total dessas moedas em 2018 oscilou entre 128,9 mil milhões de dólares dos EUA e 818,1 mil milhões de dólares dos EUA.[9]

Medidas de recomendação de cibersegurança

Em termos de resposta a estas ameaças, podem ser adotadas medidas de cibersegurança e, se for caso disso, exigidas por regulamentação. As duas áreas mais importantes a serem abordadas para prevenir ataques cibernéticos são:

Formação de funcionários sobre a forma de reconhecer tentativas de invasão, como spearphishing e anexos suspeitos

[9] https://coinmarketcap.com/charts/

Independentemente do nível de segurança de uma nova tecnologia como o blockchain, técnicas como o spearphishing prevalecerão como um método de comprometer sistemas. A autenticação de dois fatores pode reduzir o impacto de uma violação, mas não substitui a necessidade de educação[10]. O melhor programa de educação inclui um currículo mostrando exemplos passados com testes onde os funcionários podem identificar arquivos / e-mails que aparecem fraudulentos. Finalmente, o pessoal de TI deve se envolver continuamente com ataques rotineiros de "chapéu branco", onde eles tentam enganar os funcionários com uma tentativa de hacking simulada.

(2) Manter os protocolos do sistema de TI atualizados com os padrões do setor de segurança cibernética, inclusive mantendo-se atualizado com os ataques cibernéticos recentes.

Como mencionado neste relatório, muitos ataques norte-coreanos se concentram em vulnerabilidades nos protocolos do sistema operacional. As equipas de TI/ segurança devem manter-se actualizadas até:

- Criar palavras-passe fortes[11] e implementar um sistema que exija a troca regular de palavras-passe e, se possível, utilizar um sistema de gestão de palavras-passe;
- Manter-se a par de todas as edições de patch e aplicá-las rapidamente;
- Substituir os sistemas operativos mais antigos pelas versões mais recentes;
- Manter atualizado o software antivírus, quando apropriado, e digitalizar todos os softwares descarregados da internet antes de executar;
- Restringir as capacidades (permissões) dos utilizadores para instalar e executar aplicações de software indesejadas e aplicar o princípio do menor privilégio a todos os sistemas e serviços;
- Procurar e remover anexos de email suspeitos. Empresas e organizações podem bloquear mensagens de email de fontes suspeitas que contenham anexos;[12] e
- Ativar um firewall pessoal nas estações de trabalho da organização e configurá-lo para negar solicitações de ligação não solicitadas.

Abordagem de Ransomware

- Faça backup de sistemas regularmente e mantenha uma cópia criptografada de backups recentes off-site e off-line
- Existem softwares que afirmam interromper o ransomware bloqueando a criptografia não autorizada de ficheiros. Peça ao pessoal de segurança para avaliar essas ferramentas.

Regulamentação e Jurisdição

[10] autenticações de dois fatores é um procedimento de segurança que exige que o utilizador verifique a sua identidade, além de introduzir uma palavra-passe introduzindo um código recebido no seu dispositivo móvel. É melhor usar uma aplicação para autenticação em vez de um número de telemóvel, porque os números de telemóvel podem ser mais facilmente transferidos para o controlo dos hackers.

[11] consultar https://www.us-cert.gov/ncas/tips/ST04-002 para obter mais informações sobre como criar palavras-passe fortes.

[12] Para obter informações sobre como lidar com segurança com anexos de e-mail, consulteTer Cuidado com Anexos de Email. Siga práticas seguras ao navegar na web. ConsultarBons Hábitos de Segurança e Proteção dos Seus Dados para obter detalhes adicionais. Restringir esses privilégios pode impedir que malware seja executado ou limitar a sua capacidade de se espalhar pela rede

Na cibersegurança, na guerra da informação e na elaboração de políticas relacionadas, a melhor estratégia é estar à frente da ameaça. Para os países e líderes do setor que aguardam orientação sobre a componente cibernética das sanções, é aconselhável tomar medidas para garantir que as empresas de tecnologia digital estejam a trabalhar para garantir que as violações das sanções não estejam a acontecer no ciberespaço e, assim, preparar uma forma para a indústria progredir de acordo com as normas já definidas de paz e segurança humanas. É igualmente necessário que as empresas de tecnologia comuniquem as medidas que estão a tomar para seguir as sanções da ONU.

A principal prioridade é que as melhores práticas em atividades cibernéticas sejam tratadas como seu equivalente no mundo real. Em última análise, não há diferença entre branqueamento de capitais com ativos convencionais ou cibernéticos. O anonimato e a novidade dessas tecnologias aumentam o potencial de práticas enganosas e ações arriscadas por entidades já sancionadas e novos intervenientes de ameaças. Devido aos riscos aumentados, as práticas de due diligence devem ser mais resolutas. Os intervenientes que preferem operar dentro de redes de informação baseadas em blockchain ou altamente criptografadas estão se desviando das práticas prevalecentes no setor e dos requisitos de relatórios existentes. Por conseguinte, é necessária uma vigilância acrescida para qualquer entidade envolvida em armamento ou transações financeiras, transporte marítimo ou aéreo e interações com trabalhadores ou diplomatas norte-coreanos, sempre que seja sugerida a utilização dessas plataformas tecnologicamente avançadas.

As medidas de proteção recomendadas incluem:

- Insistir na divulgação integral da identificação verificável, finalidade das transações propostas e quaisquer outras informações relevantes que seriam consideradas numa transação do mundo real;
- Esclarecer a fundamentação da atividade proposta para garantir que todas as etapas económicas sirvam a propósitos razoáveis, lógicos e legítimos;
- Verificar todas as partes envolvidas na criação de novos empreendimentos cibernéticos, garantir que o financiamento e o capital - independentemente de serem pagos sob a forma de moeda digital ou não - não estejam relacionados com qualquer violação de sanções ou derivados de ativos que devam ser bloqueados;
- Impor requisitos de divulgação para qualquer empresa ou empreendimento baseado em tecnologia blockchain para autenticar a legitimidade de ativos, conteúdos de carteiras digitais ou propósitos de contratos inteligentes;
- Partilhar informações sobre quaisquer ataques à comunidade de cibersegurança e aumentar a cooperação com a pesquisa e regulamentação;
- Insistir em proteções profissionais de segurança de rede para instituições e empresas financeiras, incluindo emissores ou trocas de criptomoedas, começando com educação e política de malware/phishing/palavra-passe para melhor proteger o sistema financeiro nacional contra intrusões não autorizadas;
- Garantir que as empresas de hospedagem na Web verifiquem se a natureza do tráfego dos sites que hospedam não contribui para violações de sanções;
- Garantir que as empresas de mídia digital/social monitorem anúncios para garantir que não estejam contribuindo para violações de sanções; e
- Impor obrigações de integridade aos operadores de instalações de computação na nuvem, para maximizar a proteção e garantir que não hospedam atividades passíveis de sanção, por exemplo, malware.

Ao lidar com indivíduos, empresas ou entidades já sob sanções da ONU:

- Bloquear todo o comércio de bens, componentes ou tecnologias embargados;
- Bloquear contas financeiras e carteiras digitais e sinalizar relatórios de transações suspeitas quando apropriado; e

- Negar todas as atividades digitais ou acesso a contas em plataformas de tecnologia digital, incluindo mídias sociais, mercados, aplicativos, computação em nuvem e e-mail, se houver indícios de que as atividades possam contribuir para violações de sanções.

Conclusão

Reconhecer os conhecimentos especializados da ciberforça norte-coreana é especialmente importante, uma vez que a comunidade internacional continua a lutar por um acordo de não proliferação nuclear com a RPDC. A compreensão da forma como a Coreia do Norte está a adquirir tecnologias e a angariar fundos secretamente terá de ser abordada em futuras negociações. Para decifrar os próximos movimentos dos norte-coreanos, será importante prestar atenção à direção da indústria de tecnologia anônima, especialmente as indústrias de criptomoeda e tecnologia criptografada, e extrapolar os tipos de vantagens que um ator desonesto poderia ganhar por ter pouca regulamentação nesses campos. Mais ideias relacionadas a como eles avançarão serão deixadas para um estudo futuro.

Sobre a Ashley Taylor

Praticante, empreendedora e pesquisadora, Ashley Taylor está profundamente imersa na interseção das tecnologias digitais e da segurança internacional. Sendo um membro da primeira geração de empreendedores de blockchain, Taylor foi atraída precocemente para as potenciais ramificações das comunicações encriptadas e tecnologias de ledger distribuídas sobre a integridade do comércio e desenvolvimento social. Trabalhando com organizações de tecnologia e finanças, ela está agora a desenvolver ativamente um quadro humanista envolvendo novas tecnologias e critérios de implementação que apoiam a manutenção da paz e segurança internacional.