RELATÓRIO DO GAFI

COMBATE AO FINANCIAMENTO DE RANSOMWARE

Março 2023

O Grupo de Ação Financeira Internacional (GAFI) é um organismo intergovernamental independente que desenvolve e promove políticas para proteger o sistema financeiro mundial contra o branqueamento de capitais, o financiamento do terrorismo e o financiamento da proliferação de armas de destruição massiva. As recomendações do GAFI são reconhecidas como normas globais de combate ao branqueamento de capitais (ABC) e ao financiamento do terrorismo (CFT).

Para mais informações sobre o FATF, visite www.fatf-gafi.org

O presente documento e/ou qualquer mapa nele incluído são sem prejuízo do estatuto ou da soberania de qualquer território, da delimitação de fronteiras e limites internacionais e do nome de qualquer território, cidade ou zona.

Referência para citação:

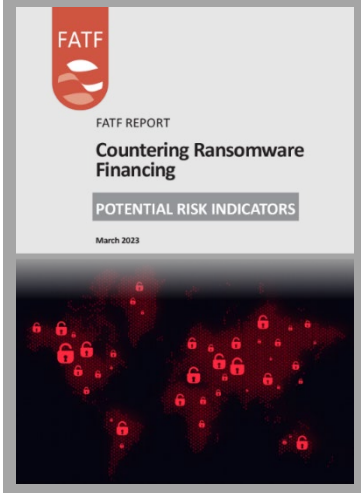
FATF (2023), Countering Ransomware Financing, FATF, Paris,

http://www.fatf-gafi.org/publications/Methodsandtrends/countering-ransomware-financing.html

Índice

Ver também:

Combate ao Financiamento de Ransomware: Indicadores potenciais de risco



Esta lista de potenciais indicadores de risco complementa o relatório do GAFI sobre o Combate ao Financiamento de Ransomware e pode ajudar as entidades dos setores público e privado a identificar atividades suspeitas relacionadas com o ransomware..

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

Acrónimos

AEC	Criptomoedas de Anonimato Acrescido
ABC/CFT	Anti-branqueamento de Capitais e Combate ao Financiamento do Terrorismo
CERT	Equipas de Resposta a Emergências Informáticas
DeFi	Financiamento Descentralizado
DNFBP	Empresas e Profissões Não Financeiras Designadas
UIF	Unidade de Informação Financeira
IP	Internet Protocol
LEA	Autoridades policiais
BC	Branqueamento de Capitais
OTC	Comércio ao Balcão
PPP	Parceria Público-privada
RaaS	Ransomware como Serviço
COS	Comunicação de Operação Suspeita
VACG	Grupo de Contacto sobre Ativos Virtuais
VASP	Virtual Asset Service Provider (Prestador de Serviços de Ativos Virtuais)
VPN	Virtual Private Network

Sumário

A escala mundial dos fluxos financeiros relacionados com ataques de ransomware aumentou drasticamente nos últimos anos. As estimativas do setor apontam para uma quadruplicação dos pagamentos de ransomware em 2020 e 2021, em comparação com 2019. As novas técnicas aumentaram a rentabilidade dos ataques e a probabilidade de êxito. Estas incluem como alvo entidades de elevada dimensão e valor, bem como o ransomware enquanto serviço, em que os criminosos de ransomware vendem kits de software de fácil utilização a afiliados. As consequências dos ataques de ransomware podem ser dramáticas e representar ameaças à segurança nacional, incluindo danos e perturbações nas infraestruturas e serviços críticos.

Através deste estudo, o GAFI visa melhorar a compreensão global dos fluxos financeiros associados ao ransomware e destacar as boas práticas para fazer face a esta ameaça. O relatório apresenta igualmente uma lista de potenciais indicadores de risco que ajudarão as autoridades e o setor privado a detetar esses fluxos financeiros. As conclusões do presente relatório baseiam-se na experiência e nos conhecimentos especializados de todo o setor público e privado, incluindo contributos e estudos de casos de mais de 40 delegações da rede global do GAFI.

Um ataque de ransomware é uma forma de extorsão e os padrões do GAFI requerem que seja criminalizado como infração subjacente ao branqueamento de capitais. O presente relatório conclui que os pagamentos e o subsequente branqueamento das receitas do ransomware são realizados quase exclusivamente através de ativos virtuais. Os criminosos de ransomware exploram a natureza internacional dos ativos virtuais para facilitar operações transfronteiriças em grande escala, quase instantâneas, por vezes sem a participação de instituições financeiras tradicionais que dispõem de programas de luta contra o branqueamento de capitais e o financiamento do terrorismo (ABC/CFT). Os criminosos complexificam ainda mais as suas operações através da utilização de tecnologias, técnicas e tokens (criptoativos) que promovem o anonimato no processo de branqueamento, como as criptomoedas e os mixers [*Serviços prestados por entidades que visam impedir ou dificultar o rastreamento de ativos virtuais*] de anonimato acrescido.

A utilização quase exclusiva de ativos virtuais no branqueamento relacionado com o ransomware reforça ainda mais a importância de acelerar a aplicação da Recomendação 15 do GAFI, que exige que as jurisdições apliquem medidas para atenuar os riscos associados aos ativos virtuais e regulamentem o setor dos VASP. Estes esforços são fundamentais para impedir que os criminosos acedam facilmente aos VASP localizados em jurisdições com controlos ABC/CFT fracos ou inexistentes para branquear os lucros dos seus crimes.

O presente relatório conclui igualmente que os ataques de ransomware são, de um modo geral, subdenunciados, quer devido a desafios na deteção pelo setor privado, a impactos negativos nos negócios da vítima, quer a um receio de retaliação por parte de criminosos, caso uma vítima denuncie um ataque. Tal explica, em parte, a falta de experiência na investigação do branqueamento de capitais relacionado com ransomware. As jurisdições devem continuar a trabalhar para aumentar e reforçar as fontes de deteção e comunicação. As autoridades devem agir rapidamente para recolher informações essenciais e devem dispor dos instrumentos e competências necessários para rastrear e recuperar eficazmente os ativos virtuais.

O ransomware atravessa uma vasta área de domínios e as investigações podem envolver intervenientes exteriores às autoridades tradicionais ABC/CFT, incluindo agências de cibersegurança e proteção de dados. Como tal, é necessária uma abordagem multidisciplinar para combater eficazmente o ransomware e o branqueamento de capitais associado. Devido à natureza intrinsecamente descentralizada e transnacional dos ativos virtuais, é imperativo criar e alavancar os mecanismos de cooperação internacional existentes para combater com êxito o branqueamento relacionado com o ransomware.

A fim de reforçar a resposta mundial contra o ransomware e o branqueamento com ele relacionado, o GAFI propõe que as jurisdições tomem as seguintes medidas.

Ações propostas

As informações recolhidas para este estudo forneceram alguns exemplos práticos de medidas que os países podem tomar para melhorar a sua capacidade de combater os fluxos financeiros ilícitos relacionados com ransomware. A presente secção resume estas boas práticas e apresenta sugestões sobre a forma como as jurisdições poderiam desmantelar de forma mais eficaz o branqueamento de capitais relacionado com o ransomware.

Implementar os padrões pertinentes do GAFI, nomeadamente em matéria de VASP, e melhorar a deteção

- As jurisdições devem acelerar o cumprimento dos padrões pertinentes do GAFI sobre o setor dos VASP mediante a aplicação da Recomendação 15 (incluindo a "Travel Rule") o mais rapidamente possível. Tal garante que os VASP cumprem as obrigações necessárias em matéria de ABC/CFT para captar informações financeiras críticas e comunicar operações suspeitas.
- As jurisdições devem assegurar que o ransomware é criminalizado como infração principal do branqueamento de capitais, em conformidade com a Recomendação 3 do GAFI (por exemplo, como um tipo de extorsão).
- As jurisdições devem melhorar a deteção de ransomware através das seguintes ações:
    - Apoiar as entidades regulamentadas a detetarem ransomware e branqueamento de capitais conexo e a comunicarem operações suspeitas, nomeadamente através da partilha de tendências, guias de deteção e indicadores de alerta (como os contidos no Combate ao Financiamento do Ransomware: Potenciais indicadores de risco) com as entidades obrigadas relevantes.
    - Incentivar as vítimas a comunicarem voluntariamente incidentes, por exemplo sensibilizando para o apoio e os recursos disponíveis ou criando canais seguros para a denúncia.
- As jurisdições devem também ponderar a criação de canais de comunicação com intervenientes não

tradicionais que possam não estar sujeitos a requisitos em matéria de ABC/CFT (tais como empresas de seguros cibernéticos e de resposta a incidentes), a fim de aumentar as fontes de deteção.

Promover as investigações financeiras e os esforços de recuperação de bens

- As autoridades competentes devem utilizar e adaptar, se necessário, as técnicas tradicionais de aplicação da lei, bem como as técnicas especificamente relacionadas com a utilização de ativos virtuais, para realizar investigações de branqueamento de capitais relacionadas com o ransomware. As autoridades competentes devem possuir as competências e os conhecimentos especializados necessários para o êxito das investigações financeiras relacionadas com ransomware. Tal inclui o desenvolvimento, o acesso e a formação em matéria de análise de blockchain e ferramentas de monitorização.
- As jurisdições devem assegurar que as autoridades responsáveis pela aplicação da lei dispõem e mantêm as capacidades e os poderes necessários para apreender e confiscar, de forma rápida e eficaz, os ativos, em especial os ativos virtuais. As jurisdições devem assegurar a existência de mecanismos especializados para gerir adequadamente os ativos virtuais apreendidos

Adotar uma abordagem multidisciplinar para combater o ransomware

- As jurisdições devem assegurar que identificam e avaliam os riscos de branqueamento de capitais criados pelo ransomware nas suas avaliações de risco nacionais. Dada a natureza descentralizada dos ativos virtuais e grupos criminosos de ransomware, incluem-se jurisdições com setores de ativos virtuais em que o ransomware não é atualmente uma ameaça interna. Essas conclusões podem ainda ajudar a apoiar as estratégias cibernéticas nacionais, obtendo uma visão holística nacional dos riscos associados ao ransomware.
- As jurisdições devem desenvolver mecanismos de coordenação entre as autoridades competentes relevantes, desde as autoridades responsáveis pela aplicação da lei, autoridades ABC/CFT e de combate ao cibercrime a parceiros não tradicionais, como as agências de cibersegurança ou de proteção de dados. Isto promove a partilha de dados e informações e proporciona uma plataforma útil para a partilha cruzada de vários conhecimentos técnicos especializados.

Apoiar parcerias com o setor privado

- As jurisdições devem identificar e estabelecer mecanismos de apoio à cooperação público-privada. As jurisdições devem considerar a inclusão de VASP e de

outros parceiros não tradicionais nesses mecanismos de cooperação. Tal cria plataformas úteis para aumentar a sensibilização, trocar conhecimentos especializados e perspetivas, bem como apoiar os objetivos de aplicação da lei.

Melhorar a cooperação internacional

- As jurisdições devem estabelecer e participar ativamente em mecanismos bilaterais, regionais e multilaterais, nomeadamente através da utilização de gabinetes de ligação e da criação de pontos de contacto claros 24/7, a fim de facilitar a cooperação internacional rápida e intercâmbio de informações. Tal ajuda a apoiar eficazmente o rastreio rápido de fundos transfronteiriços e a recuperação eficaz de bens e ajuda as autoridades a conseguirem desmantelar as redes transnacionais envolvidas em ransomware e no branqueamento de capitais associado.

Introdução

Âmbito de aplicação

1. O ransomware é um tipo de software malicioso (malware) que os criminosos desenvolvem e/ou utilizam para recusar o acesso a dados, sistemas ou redes, exigindo simultaneamente um pagamento de resgate em troca. Os métodos comuns de ataque incluem a encriptação de dados, a exfiltração de dados e a perturbação das operações das vítimas. Os ataques envolvem frequentemente mais do que um método e podem incluir uma ameaça de publicação dos dados da vítima[1].

2. Os incidentes com ransomware aumentaram significativamente nos últimos anos[2], tanto em número como em escala. O ransomware é essencialmente uma tentativa de obtenção de lucro e o aumento dos ataques conduziu a um consequente aumento das receitas do ransomware e do branqueamento de capitais com ele relacionado. As estimativas do setor indicam que os pagamentos de ransomware aumentaram pelo menos quatro vezes em 2020 e 2021, em comparação com 2019[3]. Embora os dados mais recentes do setor sugiram uma

[1] FBI "Scams and Safety: Ransomware" (acedido em setembro 2022), disponível em: www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware ; Australian Cyber Security Centre "Ransomware" (acedido em setembro 2022), disponível em: www.cyber.gov.au/ransomware .

[2] ENISA Threat Landscape 2022 (outubro 2022), disponível em www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[3] Chainalysis, "Chainalysis Crypto Crime Report 2022" (fevereiro 2022), disponível em: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

tendência descendente em 2022 (possivelmente devido à recusa de pagamento por parte das vítimas), o valor dos ativos virtuais recebidos pelos atacantes de ransomware continua a ser significativamente mais elevado do que antes de 2019[4]. O número total real de ataques e perdas conexas é suscetível de aumentar significativamente, uma vez que os ataques com ransomware muitas vezes não são comunicados.

3. Os ataques causaram graves perturbações e danos aos governos, às instituições públicas, às empresas e aos cidadãos, afetando, em alguns casos, os cuidados de saúde e ameaçando a segurança nacional, nomeadamente exigindo a interrupção de infraestruturas e serviços críticos ou comprometendo dados sensíveis[5]. Os criminosos de ransomware desenvolveram técnicas para aumentar a rentabilidade dos seus ataques e a probabilidade de êxito. Consequentemente, a ameaça de fluxos financeiros ilícitos relacionados com ransomware continuará provavelmente a aumentar.

4. Os criminosos exigem pagamentos de ransomware quase exclusivamente em ativos virtuais. As vítimas, ou terceiros relacionados que atuam sobre uma vítima, recorrem frequentemente a (VASPs)[6] para pagar resgates. Os criminosos de ransomware também utilizam os VASPs para branquear fundos ilícitos e trocar receitas por moeda fiduciária, que pode ser mais facilmente trocada por bens e serviços e é uma reserva de valor mais estável.

5. Em 2018, o GAFI alterou as suas recomendações para abranger os ativos virtuais e os VASPs. Desde então, o GAFI emitiu várias orientações para ajudar as jurisdições e o setor privado a acompanhar e atenuar os riscos neste setor, incluindo indicadores de alerta de branqueamento de capitais (BC) e financiamento do terrorismo (FT)[7]. Embora este trabalho tenha frequentemente incidido sobre o ransomware, o presente relatório é a primeira vez que o GAFI se centrou especificamente nas tendências e técnicas de branqueamento associadas a ataques de ransomware.

6. Sob a Presidência de Singapura, o GAFI está a tirar partido da sua experiência em investigações financeiras que envolvam ativos virtuais, a fim de identificar desafios e partilhar boas práticas para combater o financiamento de ransomware e o BC conexo. O presente relatório centra-se nos seguintes aspetos: como identificar e comunicar os pagamentos relacionados com o ransomware; como prevenir, detetar e investigar os fluxos financeiros do ransomware; e a forma como essas receitas são branqueadas. O presente relatório não se centra na utilização de ransomware para o financiamento do terrorismo, dada a falta de utilização significativa ou notável do ransomware para este efeito na informação e nos estudos de casos apresentados para o presente relatório.

---

[4] Chainalysis, "Ransomware Revenue Down As More Victims Refuse to Pay" (janeiro 2023), disponível em: https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

[5] Os ataques aos hospitais, por exemplo, colocaram em risco os cuidados prestados aos doentes, e os ataques aos serviços de polícia afetaram a segurança.

[6] VASP – *Virtual Assets Service Provider* (Prestador de Serviços de Ativos Virtuais) é qualquer pessoa singular ou coletiva não abrangida noutra parte das Recomendações e que, enquanto empresa, realize uma ou mais das seguintes atividades ou operações por conta ou em nome de outra pessoa singular ou coletiva: troca entre ativos virtuais e moedas fiduciárias; troca entre uma ou mais formas de ativos virtuais; transferência de ativos virtuais; guarda e/ou administração de ativos virtuais ou instrumentos que permitam controlar os ativos virtuais; e participação e prestação de serviços financeiros relacionados com a oferta e/ou venda de um ativo virtual por parte de um emitente.

[7] Ver: GAFI/FATF (Junho 2022) *Targeted Update on Implementation of the FATF Padrões on Virtual Assets And Virtual Asset Service Providers*; (setembro 2020) *Virtual Assets Red Flag Indicators*; e (agosto 2019) *Confidential FATF Guidance on Financial Investigations Involving Virtual Assets*

7. Uma vez que um ataque de ransomware é uma forma de extorsão, as recomendações do GAFI exigem que todas as jurisdições criminalizem o branqueamento de capitais relacionado com o ransomware (R.3). O GAFI também exige que as jurisdições identifiquem, avaliem e tomem medidas para atenuar os seus riscos de BC (R.1-2); assegurem que o setor privado, incluindo os VASP, aplica medidas preventivas adequadas, como a comunicação de operações suspeitas (R.9-23); assegurem que as autoridades policiais investiguem, localizam e confiscam os produtos do crime (R.4, 29-31); e cooperam a nível internacional para combater o branqueamento de capitais e as infrações subjacentes, bem como os proventos associados (R.36-40).

8. Embora o ransomware seja um tipo de cibercriminalidade, as informações constantes do presente relatório centram-se no ransomware e podem ou não ser aplicáveis a outros tipos de cibercriminalidade, tais como programas maliciosos, phishing, BEC – *Business Email Compromise* ou comprometimento e venda de informações financeiras.

Objetivos e estrutura

9. A parte I do presente relatório demonstra a forma como os criminosos de ransomware recebem, branqueiam e despendem as suas receitas ilícitas. Visa aumentar a sensibilização e a compreensão a nível global da dimensão da ameaça do ransomware a nível mundial, da forma como são feitos os pagamentos de ou relacionados com o ransomware e da forma como os proventos relacionados com os ataques de ransomware são disponibilizados aos cibercriminosos.

10. A Parte II identifica os desafios e as boas práticas na identificação, investigação e perturbação dos fluxos financeiros relacionados com o ransomware.

11. O presente relatório visa ajudar as autoridades operacionais a produzir informações financeiras de elevada qualidade, a realizar investigações financeiras e a identificar, rastrear e apreender proventos ilícitos. Os reguladores nacionais e os decisores políticos podem utilizar as informações constantes do presente relatório para identificar vulnerabilidades e atenuar os riscos. Ajudará igualmente as i**nstituições financeiras, VASP** e as **empresas e profissões não financeiras designadas (DNFBPs**) a conceberem e implementarem controlos para detetar, comunicar e prevenir a circulação ilícita de proventos relacionados com o ransomware.

Metodologia

12. Este projeto foi coliderado por peritos de Israel e dos Estados Unidos. Além disso, as seguintes jurisdições e entidades contribuíram para o trabalho no âmbito da equipa do projeto: Austrália, Canadá, Comissão Europeia, França, Alemanha, Japão, Luxemburgo, México, Filipinas, Singapura, África do Sul, Espanha, Suíça, Turquia, Reino Unido, o Grupo Ásia-Pacífico sobre BC e Grupo Egmont de Unidades de Informação Financeira.

13. As conclusões do presente relatório baseiam-se nos seguintes elementos:

• Uma análise da literatura existente e do material de fontes abertas sobre este tema.

• Um pedido de informações à Rede Global do GAFI de mais de 200 jurisdições sobre a perceção dos riscos, a legislação e as competências nacionais, os desafios e as boas práticas,

bem como estudos de casos relacionados com ransomware. No total, a equipa do projeto recebeu contributos de mais de 40 delegações.

• Debates no Grupo de Contacto sobre os Ativos Virtuais do GAFI (VACG).[8]

• Compromisso específico com o setor privado através do VACG.

[8] Em junho de 2019, o Grupo de Desenvolvimento de Políticas do GAFI acordou em criar o Grupo de Contacto de Ativos Virtuais para comunicar os requisitos do GAFI ao setor privado e assegurar que a indústria desenvolva rapidamente soluções tecnológicas adequadas para a respetiva aplicação.

PARTE I. FLUXOS FINANCEIROS DO RANSOMWARE

Escala dos fluxos financeiros

14. A escala dos ataques de ransomware e dos fluxos financeiros conexos aumentou drasticamente em todo o mundo. Muitas jurisdições registaram um aumento da frequência de ataques de ransomware nos últimos anos, variando entre 10 % e várias centenas de percentagem, consoante a jurisdição. Verificou-se um aumento correspondente das denúncias das vítimas e um aumento das comunicações de operações suspeitas relacionadas com o ransomware em várias jurisdições. Numa jurisdição, os COS apresentados nos primeiros seis meses de 2021 identificaram o equivalente a 590 milhões de USD (552 milhões de EUR) em operações relacionadas com o ransomware, um aumento de 42 % em comparação com 2020, quando o total atingiu 416 milhões de USD (389 milhões de EUR)[9]. Os recentes relatórios anuais das organizações responsáveis pela aplicação da lei revelam um crescimento substancial da atividade de ransomware[10], e as estimativas da indústria mostram um crescimento semelhante em termos do número de ataques e de tipos ativos de ransomware. Em 2021, o número estimado de ataques com ransomware foi de cerca de 623,3 milhões, mais do dobro dos 304,6 milhões de ataques estimados em 2020[11]. Do mesmo modo, o número estimado de tipos ativos de ransomware duplicou em relação ao número de 2019[12].

15. Embora algumas jurisdições tenham comunicado níveis baixos de ataques com ransomware, as informações recolhidas para o presente relatório mostram que os ataques com ransomware continuam a ser sub-reportados, apesar de o número de comunicações de operações suspeitas e de denúncias das vítimas ter aumentado em algumas jurisdições. O que torna difícil estimar com exatidão o número total de incidentes e os montantes pagos em resgates. Os estudos de casos apresentados para o presente relatório demonstraram que o ransomware pode constituir um risco para as jurisdições desenvolvidas e em desenvolvimento, independentemente da região.

16. Várias jurisdições identificaram que o aumento dos ataques de ransomware e dos fluxos financeiros conexos estava associado ao desenvolvimento de técnicas por criminosos de ransomware como alvos de grande dimensão, o ransomware como serviço (RaaS), táticas de dupla/tripla/multi-extorsão para maximizar a eficácia dos ataques e a rentabilidade daí resultante (ver caixa 1).

---

[9] FINCEN, "Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021" (junho 2021), disponível em: www.fincen.gov/sites/default/files/2021-10/Financial Trend Analysis Ransomware 508 FINAL.pdf

[10] FBI, "Internet Crime Report 2021" (acedido em 1 Dezembro 2022), disponível em: www.ic3.gov/Home/AnnualReports ; EUROPOL, "Internet Organised Crime Threat Assessment (IOCTA) 2021" acedido em 1 Dezembro 2022), disponível em: www.europol.europa.eu/publications-events/main-reports/iocta-report

[11] SonicWall, "2022 SonicWall Cyber Threat Report" (2022), disponível em: www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

[12] Chainalysis, "Chainalysis Crypto Crime Report 2022" (fevereiro 2022), disponível em: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

Caixa 1. Desenvolvimento de técnicas de ransomware

Com o ***Big Game Hunting*** [alvos de grande dimensão], os criminosos de ransomware focam-se em organizações grandes de elevado valor ou entidades de grande visibilidade que consideram ser mais suscetíveis de pagar um resgate para retomar as operações comerciais ou evitar o escrutínio público. Os criminosos de ransomware também visam seletivamente organizações que operam em cadeias de abastecimento «just-in-time», que são mais suscetíveis de ter custos mais elevados de inatividade, bem como infraestruturas críticas, e organizações que detêm informações sensíveis ou valiosas. Os atacantes podem avaliar que estas organizações têm uma maior propensão para pagar resgates do que outras vítimas.

O **RaaS** refere-se a um modelo de negócio criminoso em que os criminosos de ransomware fornecem kits de ransomware na Dark Web ou recorrem a recursos externos em ataques de ransomware, incluindo a distribuição de programas maliciosos, o compromisso de segurança inicial da rede informática da vítima, a exfiltração de dados ou a negociação de resgates para as filiais em troca de uma taxa e/ou de uma percentagem do resgate. Os criminosos também podem adquirir credenciais roubadas para aceder e explorar os sistemas das vítimas que permitem a distribuição de ransomware e obter informações sobre indústrias específicas em jurisdições específicas para informar o seu alvo e maximizar a eficácia do seu ataque. O modelo RaaS reduziu os custos e os conhecimentos técnicos necessários para levar a cabo ataques com ransomware, reduzindo os obstáculos à entrada e permitindo que criminosos menos sofisticados realizem ataques de ransomware.

A **Dupla Extorsão** refere-se a uma prática em que os operadores de ransomware exfiltram os dados de uma vítima antes de os codificarem e, em seguida, ameaçam publicar os dados roubados se os pedidos de resgate não forem satisfeitos. Esta ameaça de publicação acresce à ameaça relacionada com o sistema perturbado. Esta tática pode exercer pressão adicional sobre as vítimas para que paguem pedidos de resgate, mesmo que sejam capazes de restabelecer as operações.

A **Tripla Extorsão** refere-se a uma prática em que os operadores de ransomware procuram dinheiro não só da vítima visada pela primeira vez, mas também de uma vítima que pode ser afetada pela divulgação dos dados originais da vítima visada, tais como informações protegidas em matéria de saúde, informações pessoais identificáveis, credenciais de contas e propriedade intelectual.

A **Multi-Extorsão** refere-se a uma prática que envolve mais de dois métodos de extorsão. Baseia-se na dupla extorsão utilizando a encriptação e a exfiltração, mas inclui táticas de pressão adicionais, como a negação da distribuição do serviço (DDoS), o contacto com os clientes das vítimas, a venda a descoberto das existências das vítimas e a perturbação dos sistemas de infraestruturas.

17. Mais de metade de todos os ataques de ransomware relatados são contra vítimas no setor do governo/setor público, dos cuidados de saúde e do setor dos bens e serviços industriais, de acordo com informações públicas[13], [14]. É provável que tal se deva, em parte, à procura de grandes empresas, que pode ser responsável por grandes pagamentos e por um aumento global dos pagamentos de ransomware. Nos últimos anos, os criminosos do ransomware também visaram instituições no setor da energia, financeiro, comunicações e educação. Embora os criminosos de ransomware que utilizam táticas de *Big Game Hunting* se foquem em grandes empresas, as organizações e indústrias de média e pequena dimensão são também fortemente visadas por ataques de ransomware. Com efeito, os ataques de ransomware continuam a visar predominantemente pequenas e médias empresas. Estes alvos mais pequenos podem ter um rácio risco/recompensa mais consistente do que os ataques de perfil mais elevado contra vítimas de maiores dimensões. No segundo trimestre de 2020, quase 55 % do total de ataques ocorreram contra empresas com menos de 100 trabalhadores e cerca de 75 % dos ataques ocorreram em empresas com menos de 50 milhões de USD (47 milhões de EUR) em receitas[15].

18. Os montantes dos resgates variam entre centenas de dólares ou euros de ativos virtuais em casos de pequena escala destinados a pessoas singulares ao equivalente a milhões de dólares ou euros nos casos que visam grandes empresas, especialmente infraestruturas críticas ou organizações que detêm informações sensíveis ou valiosas. A experiência das jurisdições indica que o montante dos resgates solicitado pelos criminosos também aumentou nos últimos anos. Em 2021, o pagamento médio de resgate foi aproximadamente o equivalente a 800 000 USD (748 000 EUR) de ativos virtuais, quase cinco vezes mais elevado do que em 2020. Este aumento está provavelmente relacionado com a utilização de técnicas de *Big Game Hunting*, acima referidas. Em alguns casos, os pedidos de resgate atingiram dezenas de milhões de dólares em ativos virtuais; por exemplo, de acordo com notícias da imprensa, em 2021, uma companhia de seguros sediada nos Estados Unidos foi atacada por um «Phoenix CryptoLocker» (alegadamente a terceira maior RaaS em termos

[13] Sophos, "The State of Ransomware in State and Local Government" (setembro 2022), disponível em: https://assets.sophos.com/X24WTUEQ/at/rbjqpp5wwm6v5h3wj9v3733/sophos-state-of-ransomware-government-2022-wp.pdf

[14] Digital Shadows, "Ransomware: Analyzing The Data From 2020" (janeiro 2021), disponível em: www.digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from-2020/

[15] Coveware, "Q2 Quarterly Report" (agosto 2020), disponível em: www.coveware.com/blog/q2-2020-ransomware-marketplace-report

de receitas em 2021, após a Conti e a DarkSide[16]) e, alegadamente, pagou 40 milhões de USD (37 milhões de EUR) para recuperar o controlo da sua rede[17].

Características e tendências geográficas

19. O ransomware é geralmente um fenómeno internacional, em parte devido à natureza da cibercriminalidade e dos ativos virtuais. As informações da Rede Global do GAFI, os estudos de casos e os dados da indústria apontam para determinadas características e tendências geográficas nos ataques de ransomware. Muitas redes de ransomware têm estado ligadas a jurisdições com riscos de BC mais elevados (ver caixa 2). Em muitos casos, os criminosos de ransomware depositam ou levantam dinheiro nessas jurisdições. Noutros casos, os ataques de ransomware foram perpetrados a partir dessas jurisdições ou por elas potencialmente patrocinados[18].

[16] Chainalysis, "Chainalysis Crypto Crime Report 2022" (fevereiro 2022), disponível em: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

[17] Mehrotra, Kartikay and Turton, William, "CNA Financial Paid $40 Million in Ransom After March Cyberattack," Bloomberg, 20 May 2021 (acedido em 1 Dezembro 2022), disponível em: www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

[18] Ver Alerta (AA22-187A) da U.S. Cybersecurity & Infrastructure Security Agency (julho 2022), disponível em at: www.cisa.gov/uscert/ncas/alerts/aa22-187a

Caixa 2. Jurisdições com riscos mais elevados de branqueamento de capitais

Embora não exista um consenso universal quanto à definição ou metodologia para determinar se uma jurisdição representa um risco mais elevado para o BC/FT, a consideração dos riscos específicos de cada país, em conjugação com outros fatores de risco, fornece informações úteis para determinar mais aprofundadamente os potenciais riscos de BC/FT. Os indicadores de risco mais elevado incluem: a) Países ou zonas geográficas identificados por fontes credíveis como fornecendo financiamento ou apoio a atividades terroristas ou que tenham designado organizações terroristas que operam no seu interior; (b) Países identificados por fontes credíveis como apresentando níveis significativos de criminalidade organizada, corrupção ou outras atividades criminosas, incluindo países de origem ou de trânsito de drogas ilegais, tráfico de seres humanos, contrabando e jogo ilegal; (c) Países sujeitos a sanções, embargos ou medidas semelhantes emitidas por organizações internacionais como as Nações Unidas; e d) Países identificados por fontes credíveis como tendo regimes de governação, de aplicação da lei e regulamentares fracos, incluindo os países identificados pelas declarações do GAFI como tendo regimes de ABC/CFT fracos, especialmente para os VASP, e em relação aos quais os VASP e outras entidades obrigadas devem prestar especial atenção às relações de negócio e às operações..

Fonte: GAFI (2021) Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs, parágrafo 154

20. A escala dos ataques com ransomware difere por geografia. Os relatórios especializados de 2022 indicam que a região do Médio Oriente e de África foi a menos visada por ataques de ransomware (4 %), seguida da América Latina (6 %), da Ásia-Pacífico (10 %), da Europa (28 %) e da América do Norte (52 %)[19]. A variação de escala entre regiões geográficas teve um impacto na forma como estas regiões percecionam o risco que enfrentam devido ao ransomware. As informações fornecidas pela Rede Global do GAFI mostram que as jurisdições que testemunham um aumento da procura por grandes alvos e resgates associados de elevado valor são mais suscetíveis de avaliar como elevados os riscos de BC relacionados com o ransomware.

21. Muitos grandes grupos de ransomware utilizam uma versão do RaaS denominada modelo de filial, na qual externalizam elementos do ataque de ransomware em troca de uma taxa e/ou de uma percentagem do resgate. Nesses casos, estes criminosos estão frequentemente dispersos geograficamente e pode ser difícil identificar e localizar grupos envolvidos em ataques de ransomware. Por exemplo, tal como ilustrado no estudo de caso do EMOTET infra, os criminosos de ransomware podem cooperar na condução de ataques ou utilizar infraestruturas partilhadas quando operam em diferentes jurisdições. A

[19] Group-IB, "Ransomware Uncovered Report. Group-IB" (May 2022), disponível em: https://spiresolutions.com/wp-content/uploads/2021/07/ransomware_uncovered_2020.pdf

variedade de criminosos envolvidos em várias jurisdições pode também complicar a deteção dos fluxos de dinheiro associados aos principais criminosos de ransomware.

Caixa 3. Estudo de caso EMOTET [1]

O EMOTET é uma das mais significativas campanhas de malware nos últimos anos. Foi descoberto pela primeira vez como um Trojan bancário em 2014, transformando-se num instrumento fundamental para outros malwares e ransomware. Quando foi eliminado, em janeiro de 2021, o EMOTET tinha permitido até 70 % dos malwares mundiais, incluindo o Ryuk e o DoppelPaymer, que tiveram um impacto económico significativo nas empresas do Reino Unido. A eliminação envolveu um trabalho estreito entre as autoridades policiais do Canadá, da França, da Alemanha, da Lituânia, dos Países Baixos, da Ucrânia, do Reino Unido e dos EUA, com atividades internacionais coordenadas pela Europol e pela Eurojust. Através desta parceria colaborativa, as autoridades policiais nacionais conseguiram identificar e analisar dados que ligam os dados relativos ao pagamento e registo aos criminosos que utilizaram o EMOTET. O caso ilustra a dimensão e a natureza da cibercriminalidade, demonstrando a forma como a cooperação internacional é essencial para combater a ameaça.

Fonte: Reino Unido

Notas:

1. Ver também o comunicado da Europol sobre EMOTET, disponível em: www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

1. Um Trojan bancário refere-se a um malware que tenta roubar as credenciais dos clientes de uma instituição financeira ou obter acesso às suas informações financeiras.

22. O branqueamento de pagamentos de ransomware também é transnacional, dada a natureza transfronteiriça dos ativos virtuais, em que os pagamentos de ransomware são quase sempre efetuados. Os utilizadores de ativos virtuais podem transacionar entre pares — transacionar diretamente entre si, utilizando apenas a sua chave privada e uma ligação à Internet, independentemente das fronteiras geográficas e sem o envolvimento de instituições com obrigações ABC/CFT. Os criminosos, incluindo os criminosos de ransomware com acesso à Internet, podem explorar estas características dos ativos virtuais para facilitar operações transfronteiriços em grande escala, quase instantâneas, sem intermediários financeiros tradicionais que tenham programas ABC/CFT. Têm também acesso a VASP sediados em todo o mundo em jurisdições com controlos ABC/CFT fracos ou inexistentes, que os criminosos de sequestro utilizam para trocar os seus proventos ilícitos para moeda fiduciária.

Caixa 4. O que é um ativo virtual?

Um ativo virtual é uma representação digital de valor que pode ser negociado ou transferido digitalmente e que pode ser utilizado para fins de pagamento ou investimento. Os ativos virtuais não incluem representações digitais de moedas fiduciárias, valores mobiliários e outros ativos financeiros que já estejam abrangidos noutras partes das recomendações do GAFI.

Os ativos virtuais mais frequentemente utilizados são um meio de troca, para o qual os registos de produção ou de propriedade são suportados através de uma tecnologia de registo distribuído baseada na criptografia, como uma blockchain. Tal como referido a seguir, muitos ativos virtuais populares operam em blockchains públicas, onde podem ser visualizadas informações sobre operações sob pseudónimo.

Fonte: GAFI

Métodos e tendências comuns

23. A realização de uma investigação financeira bem-sucedida sobre um ataque de ransomware exige uma boa compreensão dos métodos e técnicas utilizados para o branqueamento de fundos. Uma vez que os ataques de ransomware são geralmente subdenunciados, o presente relatório recolheu informações de várias fontes abertas, bem como experiências de jurisdições, a fim de obter uma melhor compreensão da forma como os pagamentos de resgate são efetuados, branqueados, recebidos e, em alguns casos, trocados por moeda fiduciária.

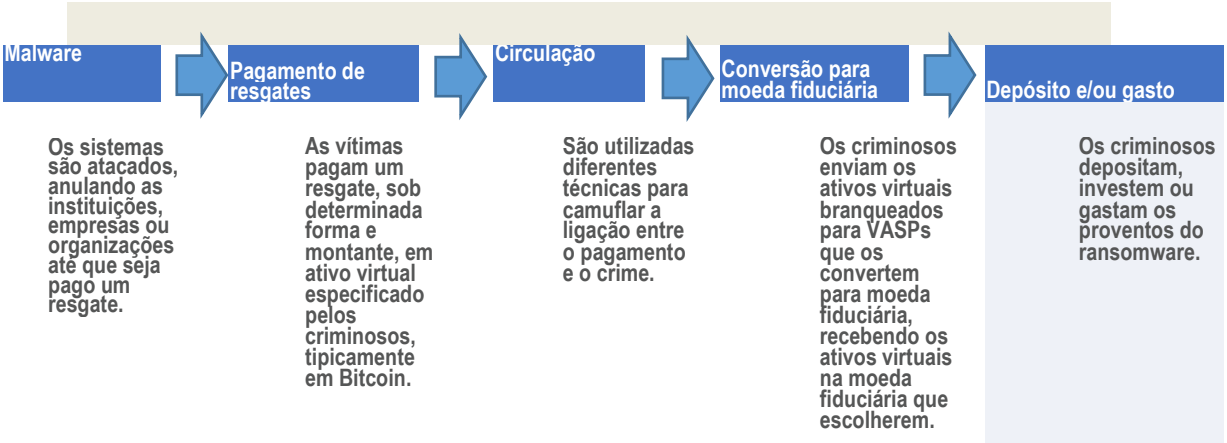
24. Os fluxos financeiros relacionados com o ransomware envolvem frequentemente várias instituições financeiras tradicionais, bem como VASP. Outros terceiros, tais como companhias de seguros cibernéticos, empresas de resposta a incidentes ou empresas de cibersegurança, podem também participar na resposta a um ataque de ransomware, incluindo o processo de pagamento às vítimas.

25. Embora os ativos virtuais sejam o principal método para os pagamentos de ransomware, os fluxos financeiros globais relacionados com o ransomware envolvem múltiplas instituições financeiras tradicionais, bem como VASP e outros terceiros.

Quadro 1. Tipos de setores que podem estar envolvidos nos fluxos financeiros do ransomware

Instituições Financeiras	As instituições financeiras atuam normalmente como intermediários que as vítimas de ransomware (ou um terceiro que opera em nome da vítima) utilizam para transmitir fundos a um VASP para a aquisição de ativos virtuais.
VASPs	As vítimas de ransomware (ou um terceiro que atue em nome da vítima) utilizam os VASP para adquirir e transferir o tipo e a quantidade específicos de ativos virtuais especificados pelo criminoso de ransomware.
Companhias de seguros	As companhias de seguros podem cobrir e, por vezes, pagar resgates como parte da cobertura de seguro cibernético.
Empresas de resposta a incidentes	As empresas de resposta a incidentes contratadas por vítimas de ransomware negoceiam frequentemente o pagamento de resgate com os atacantes. No âmbito do seu serviço, estas empresas podem adquirir os ativos virtuais às VASP para pagamento de resgates e transferi-los para os atacantes em nome das vítimas.
Empresas de cibersegurança	Empresas que são responsáveis pela proteção dos dados, sistemas, redes e dispositivos conectados do cliente contra qualquer acesso não autorizado e ilegal.

Caixa 5. Fluxos financeiros típicos relacionados com pagamentos de ransomware



Na sequência da receção do pedido de resgate por parte da vítima, esta ou um terceiro que atue em seu nome transmite normalmente fundos através de transferência eletrónica, de um centro de compensação automático ou de um pagamento por cartão de crédito a um VASP para adquirir o tipo e o montante do ativo virtual especificado pelo criminoso do ransomware. Os terceiros que atuam em nome da vítima podem incluir empresas de resposta a incidentes ou companhias de seguros cibernéticas.

Em seguida, a vítima ou terceiro envia o resgate, muitas vezes a partir de uma carteira alojada num VASP, para o endereço virtual do autor do crime. Trata-se geralmente de uma carteira não alojada (software ou hardware que permite aos utilizadores deter,

armazenar e transferir ativos virtuais para fora de um terceiro, como um VASP; também referida como uma carteira sem custódia) controlada por um criminoso de ransomware, ou mula ou carteira alojada num VASP situado fora da jurisdição onde ocorreu o ataque e que, normalmente, não coopera com as autoridades policiais ou as UIF.

Em muitos casos, o criminoso de ransomware utilizará técnicas diferentes que podem facilitar a circulação (descritas mais pormenorizadamente abaixo). Por último, os criminosos de ransomware utilizam frequentemente VASP localizados em jurisdições fora da sua sede para trocar ativos virtuais por moeda fiduciária, embora também possam deixar fundos em carteiras não alojadas durante longos períodos de tempo ou utilizar ativos virtuais para pagar a terceiros envolvidos nos ataques

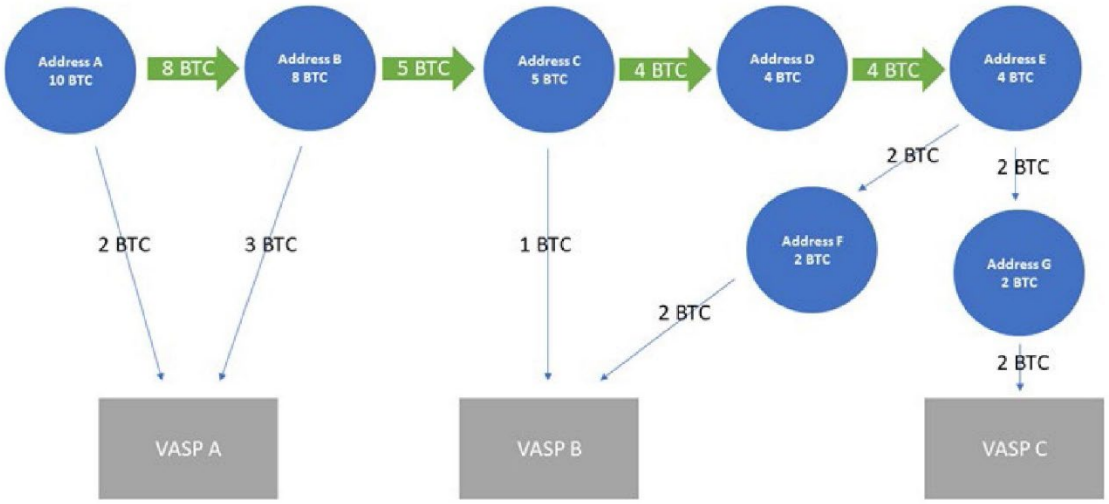
26. Os criminosos de ransomware utilizam frequentemente tecnologias, técnicas e tokens que reforçam o anonimato no processo de branqueamento, incluindo um ou mais dos abaixo indicados. Os criminosos de ransomware podem não utilizar os mesmos elementos de cada vez ou seguir a mesma ordem ao branquear os seus proventos.

• Os atacantes de ransomware exigem frequentemente que os pagamentos às vítimas em ativos virtuais sejam enviados para os endereços da carteira que controlam, e muitas vezes **diferentes endereços de carteiras** para receber proventos ilícitos de cada ataque.

• Depois de os atacantes receberem fundos, podem utilizar vários endereços intermediários para transferir os ativos virtuais de um endereço de carteira, utilizando uma série de operações em que transferem pequenos montantes de ativos virtuais para novos endereços sucessivos. Os fundos são frequentemente enviados para endereços de carteira alojados em mais de um VASP. Estes padrões de transação são designados por *"**peel chains***" que não são exclusivamente utilizados para ocultar o movimento de ativos virtuais[20]. Contudo, podem também ser explorados por criminosos para branquear uma grande quantidade de ativos virtuais através de uma série de operações menores com o objetivo de reduzir a oportunidade deste comportamento ser rastreado. Em especial, o rasto dos ativos virtuais pode ser ocultado se as operações forem executadas com uma rapidez e frequência elevadas.

Figura 1. Ilustração das "*peel chains*"

[20] As *peel chains* observam-se com bastante frequência, e podem ocorrer naturalmente devido à forma como as carteiras de ativos virtuais são concebidas.



Legenda: "Address" – Endereço

• Os criminosos de ransomware muitas vezes também branqueiam ativos virtuais através de ***mixers* ou *tumblers*** (por exemplo, Wasabi), que utilizam vários métodos para ocultar a ligação entre o endereço que envia ativos virtuais e os endereços que recebem ativos virtuais, quer em alternativa quer como complemento da transferência de ativos virtuais através de peel chains. Em alguns casos, os cibercriminosos utilizam operações CoinJoin, nas quais os vários remetentes e destinatários dos fundos combinam os seus pagamentos numa única transação agregada. Tal exige frequentemente um serviço específico, como por exemplo o JoinMarket, que faz corresponder utilizadores interessados e os apoia na criação dessa transação.

• Além disso, os atacantes de ransomware também utilizam **criptomoedas de anonimato acrescido** (**AEC, também denominadas moedas de privacidade**), apesar de a maioria exigir o pagamento em Bitcoin. As experiências das jurisdições e os relatórios do setor indicam que as AEC são utilizadas para pagar aos atacantes de ransomware, uma vez que podem ocultar carteiras de envio e receção. Por exemplo, as AEC podem utilizar uma combinação de tecnologias de reforço da privacidade, tais como *mixers*, assinaturas angulares, endereço "*stealth*" e operações confidenciais, todas elas suscetíveis de ocultar o envio e a receção de carteiras. Cada vez mais atacantes de ransomware solicitam pagamentos exclusivamente em Monero, embora o ativo virtual mais comummente utilizado em casos de ransomware seja a Bitcoin (99 %)[21]. Algumas jurisdições assistiram a casos em que os atacantes aceitaram pagamentos tanto em Bitcoin como em Monero. No entanto, cobrariam uma taxa adicional que variaria entre 10 a 20 % do resgate exigido para os pagamentos da Bitcoin, com base no facto de tais operações serem mais facilmente detetáveis. Como tal, os criminosos pagarão taxas adicionais para utilizar tecnologias de anonimato acrescido, como os serviços de *mixing*, para tornar mais difícil às autoridades para rastrear ou qualificar operações.

• Várias jurisdições observaram também que os cibercriminosos convertem frequentemente o pagamento de resgates da Bitcoin em outros ativos virtuais através de

[21] Coveware, "Q3 Ransomware Marketplace Report" (novembro 2019), disponível em: www.coveware.com/blog/q3-ransomware-marketplace-report

VASP ou de protocolos DeFi[22], [23]. Esta ação é frequentemente designada como «**chain-hopping**», que se refere à transição de um ativo virtual para outra blockchain diferente, muitas vezes numa sucessão rápida e com o objetivo de contornar as tentativas de seguir estes movimentos. Uma jurisdição comunicou que os criminosos de ransomware utilizam cada vez mais protocolos DeFi para montar nas chamadas criptomoedas estáveis (*stablecoins*)[24] antes de trocarem fundos em moeda fiduciária. As plataformas DEFI são atrativas para os criminosos, uma vez que muitas não aplicam controlos ABC/CFT, embora possam estar sujeitas a obrigações em matéria de ABC/CFT em função dos factos e circunstâncias dos seus modelos de negócio. Uma jurisdição comunicou que os protocolos e mixers de DeFi são utilizados de forma coerente por criminosos de ransomware, por vezes utilizados em sucessão várias vezes no processo de branqueamento de capitais.

• Durante o processo de branqueamento, os criminosos de ransomware recorrem frequentemente a VASP centralizados, incluindo os comerciantes ao balcão (OTC) para trocar o dinheiro dos seus lucros. Os criminosos de ransomware enviam frequentemente os ativos virtuais para um VASP em jurisdições de alto risco ou para um VASP com controlos ABC/CFT fracos ou inexistentes para conversão em moeda fiduciária. Os criminosos estabelecidos em jurisdições de alto risco poderão utilizar os VASP centralizados a nível local para estes fins, como no caso dos VASPs americanos Suex[25], [26]Chatex, Garantex[27] e Bitzlato Limited (ver Caixa 6, abaixo)[28]. Várias jurisdições comunicaram que as entidades de troca e levantamento de fundos estão fortemente concentradas em locais urbanos e centrais. Em alguns casos, os criminosos de ransomware de vários grupos utilizaram os mesmos VASP para receber ou branquear os seus ativos virtuais.

• Nos casos em que estejam envolvidas várias partes, os criminosos de ransomware têm normalmente de pagar aos parceiros criminosos e aos hospedeiros de infraestrutura. Cada vez mais, os operadores de infraestruturas criminosas estão dispostos a aceitar pagamentos em ativos virtuais e os criminosos de ransomware efetuam frequentemente esses pagamentos utilizando receitas provenientes dos seus ataques. Em muitos casos, as empresas de análise de blockchains observaram desvios diretos de pagamentos de

---

[22] O termo "decentralised finance"- DeFi (financiamento descentralizado) é utilizado quando aplicações descentralizadas ou distribuídas, ativadas por uma "*smart-contract provisioned blockchain*", oferecem serviços financeiros, como os oferecidos pelos VASP. Uma aplicação DeFi (ou seja, um software) não é um VASP à luz dos padrões do GAFI, uma vez que os padrões não se aplicam ao software ou à tecnologia subjacentes. No entanto, os criadores, proprietários e operadores ou outras pessoas que mantenham um controlo ou influência suficiente nos serviços DeFi podem ser abrangidos pela definição de VASP do GAFI sempre que prestem ou facilitem ativamente serviços VASP.

[23] Para além de serem utilizados para branquear pagamentos de ransomware, os próprios protocolos DeFi, em especial *cross-chain bridges*, têm sido cada vez mais visados por cibercriminosos que procuram explorar lacunas de segurança e roubar ativos virtuais.

[24] Nota sobre a terminologia: O GAFI considera que o termo «criptomoedas estáveis» não é uma categoria jurídica ou técnica clara, mas antes um termo comercial utilizado pelos promotores dessas moedas. Para evitar uma validação não intencional de tal presunção, referimo-nos às mesmas como as "chamadas criptomoedas estáveis".

[25] Ver Comunicado do U.S. Treasury, disponível em: https://home.treasury.gov/news/press-releases/jy0364

[26] Ver Comunicado do U.S. Treasury, disponível em: https://home.treasury.gov/news/press-releases/jy0471

[27] Ver Comunicado do U.S. Treasury, disponível em: https://home.treasury.gov/news/press-releases/jy0701

[28] Ver Comunicado do U.S. Treasury, disponível em: www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million

ransomware para endereços de ativos virtuais associados a operadores maliciosos "enquanto infraestrutura como um serviço".

Caixa 1. Bitzlato Limited[1]

Em janeiro de 2023, uma operação transnacional determinou que a Bitzlato Limited, um Exchange de moeda virtual com operações significativas na Rússia, desempenhou um papel fundamental no branqueamento de moeda virtual convertível (CVC). A operação foi conduzida pelas autoridades francesas e norte-americanas, com o apoio da Europol, e com a participação de autoridades da Bélgica, Chipre, Portugal, Espanha e Países Baixos. A Bitzlato foi suspeita de facilitar várias operações ilícitas, nomeadamente no caso de criminosos de ransomware, como o Conti, um grupo de *Ransomware-as-a-Service* associado à Rússia. O Departamento de Justiça dos EUA alegou igualmente que a Bitzlato recebeu mais de 15 milhões de dólares em produtos de ransomware. Paralelamente, a UIF dos EUA (Financial Enforcement Network) emitiu uma decisão que identifica a plataforma como uma «preocupação principal em matéria de branqueamento de capitais».

Estas investigações permitiram o desmantelamento da plataforma de exchange, incluindo a apreensão de infraestruturas digitais e de bens de origem criminosa no valor de 18 milhões de EUR em carteiras cripto em França, bem como a detenção de indivíduos importantes em várias jurisdições.

A Bitzlato tornou-se conhecida como necessitando de uma identificação mínima por parte dos seus utilizadores e, em resultado destes procedimentos deficientes relativamente ao conhecimento do seu cliente (KYC), a Bitzlato tornou-se alegadamente um refúgio para proventos criminosos e fundos destinados a ser utilizados em atividades criminosas.

Fonte: França e Estados Unidos

1. Ver também o comunicado da Gendarmerie francesa, disponível em: www.gendarmerie.interieur.gouv.fr/gendinfo/enquetes/2023/demantelement-d-une-plateforme-de-cryptomonnaies-servant-au-blanchiment ; bem como o comunicado da Europol, disponível em: www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested

27. Algumas jurisdições observaram igualmente que os criminosos de ransomware utilizavam **mulas de dinheiro** com contas em VASP para converter os proventos em moeda fiduciária através da utilização de "rampas de lançamento" que são serviços/plataformas que permitem a troca de ativos virtuais por moeda fiduciária (por vezes designada por «troca/ levantamento»). Essas contas podem ser criadas utilizando uma identidade roubada ou falsa ou podem ser uma conta legítima detida por outra parte cúmplice na utilização da conta. As mulas são normalmente terceiros não associados envolvidos na fase final do processo de branqueamento de capitais e são responsáveis por uma parte da

globalidade dos fundos que circulam através de um processo de branqueamento. O seu afastamento da entidade criminosa e as suas transferências de valor mais reduzido podem torná-los mais difíceis de identificar.

Caixa 7. Exemplo de recrutamento de uma "mula" de dinheiro

Os criminosos de ransomware recrutam mulas de dinheiro e fornecem-lhes dispositivos móveis. Na maioria dos casos, estas mulas não têm qualquer presença na Internet e pouca literacia de Internet. As contas de correio eletrónico são então criadas em prestadores de serviços de correio eletrónico anónimos fora da jurisdição, o que dificulta a identificação dos utilizadores das contas. As mulas utilizam um dispositivo móvel fornecido pelo «facilitador» criminoso para os processos de registo e para criar uma conta na instituição financeira ou no VASP. Após registo, as mulas devolvem o dispositivo ao «facilitador» criminoso. Os «facilitadores» criminosos utilizam estes dispositivos em nome da mula para realizar operações online. Em alguns casos, os criminosos tiram partido dos serviços de VPN, o que torna anónimo o endereço IP do dispositivo utilizado. Em consequência, a localização geográfica real do criminoso que realiza as operações permanece oculta.

Fonte: África do Sul

PARTE II. DESAFIOS E BOAS PRÁTICAS PARA PERTURBAR O BC DO RANSOMWARE

Quadro jurídico

28. Um quadro jurídico sólido serve de base para permitir que as autoridades competentes desenvolvam políticas eficazes de atenuação dos riscos do ransomware. A presente secção analisa a relevância dos padrões do GAFI para i) criminalizar o ransomware para efeitos de branqueamento de capitais (BC) e ii) aplicar medidas preventivas aos setores regulamentados relevantes.

Ransomware como infração subjacente ao BC

29. Embora a maioria das jurisdições não disponha de legislação penal específica em matéria de ransomware, tal não impede, de um modo geral, as jurisdições de perseguirem criminalmente ataques com ransomware como infração subjacente[29].

30. Com base nos contributos dos participantes no projeto, as jurisdições tendem a perseguir o crime precedente de ransomware através de acusações de extorsão ou, mais frequentemente, como crime informático, como danos a dados, intrusões ou danos em programas e sistemas informáticos. A Recomendação 3 do GAFI requer que as jurisdições criminalizem o branqueamento de capitais relacionado com infrações relacionadas com a extorsão. As infrações de extorsão tipicamente têm a vantagem de ser tecnologicamente neutras, o que significa que podem captar ataques de ransomware, independentemente do método ou da forma. As jurisdições que utilizam infrações de extorsão devem assegurar que a sua legislação continua a ser pertinente para permitir às autoridades competentes investigar e recuperar eficazmente os fluxos ilícitos de ativos virtuais (ver secção 6).

31. Ao contrário da extorsão, os crimes informáticos não estão incluídos na lista mínima de infrações subjacentes[30] do GAFI. No entanto, não parece que tal tenha conduzido na prática a lacunas na luta contra o branqueamento de capitais decorrentes da atividade de ransomware.Com base numa amostra de jurisdições, aquelas que usam os crimes informáticos para perseguir o ransomware encaram estas infrações como subjacentes (quer estejam na lista de infrações subjacentes, quer seja através de uma abordagem de "todos os crimes"). Durante este estudo, nenhuma jurisdição comunicou problemas relacionados com o ransomware. No entanto, as jurisdições devem assegurar que a sua escolha da infração subjacente imputada não inibe a sua capacidade de combater o BC relacionado com o ransomware.

Aplicação de medidas preventivas aos intervenientes relevantes

32. Os padrões do GAFI exigem que as jurisdições apliquem medidas para prevenir o branqueamento de capitais, nomeadamente através de instituições financeiras, entidades não financeiras e VASPs. Estas medidas asseguram que estas entidades compreendem e atenuam os seus riscos de BC, aplicam controlos adequados, incluindo a identificação dos seus clientes; e detetam e comunicam operações suspeitas, em conformidade com as Recomendações 9 a 23 do GAFI.

[29] As jurisdições também comunicaram, na sua maioria, que não criminalizaram as vítimas que efetuam pagamentos de resgate aos autores de ataques com ransomware, embora algumas jurisdições desaconselhem fortemente os pagamentos de ransomware pelas vítimas.
[30] Ver Categorias de infrações designadas definidas no Glossário das Recomendações do GAFI.

33. Dada a relação entre o ransomware e os ativos virtuais, a alteração de 2018 aos padrões do GAFI para aplicar estas medidas aos VASP constituiu um passo importante no reforço do regime global ABC/CFT contra os riscos colocados pelo ransomware. No entanto, em janeiro de 2023[31], das 86 jurisdições que foram avaliadas à luz dos padrões revistos (recomendação 15), 63 (73 %) cumprem parcialmente ou não cumprem estes requisitos[32]. Apenas uma das 86 jurisdições foi considerada plenamente conforme.

34. Tendo em conta o leque de jurisdições avaliadas à luz da revista Recomendação 15, é provável que estes valores sejam largamente representativos da situação em toda a rede global do GAFI. Esta avaliação é ainda corroborada pelas conclusões de um inquérito do GAFI de março de 2022, que concluiu que, em 2022, menos de metade dos inquiridos tinha um regime de licenciamento ou um registo para ativos virtuais e VASP. Como tal, existem provavelmente lacunas na aplicação das obrigações em matéria de ABC/CFT por parte dos VASP, incluindo a identificação de clientes ou a comunicação de operações suspeitas, na maioria das jurisdições. Dada a natureza transfronteiriça dos ativos virtuais, é importante que as jurisdições de toda a rede global acelerem o cumprimento da Recomendação 15 (incluindo a "Travel Rule").

Ações propostas

- As jurisdições devem acelerar o cumprimento dos padrões pertinentes do GAFI sobre o setor VASP mediante a aplicação da Recomendação 15 (incluindo a "Travel Rule") o mais rapidamente possível. Tal garante que os VASP cumprem as obrigações necessárias em matéria de ABC/CFT para captar informações financeiras críticas e comunicar operações suspeitas.
- As jurisdições devem assegurar que o ransomware é criminalizado como infração subjacente ao branqueamento de capitais, em conformidade com a Recomendação 3 do GAFI (por exemplo, como um tipo de extorsão).

Deteção e comunicação de informações

35. Devido à distribuição geográfica dos criminosos de ransomware, à utilização por estes de técnicas de BC e às atuais características dos ataques de ransomware (como referido na parte I supra), é difícil estimar a escala dos fluxos financeiros derivados deste fenómeno. Na maioria das jurisdições, os ataques de ransomware continuam a ser pouco comunicados, o

[31] Ver as avaliações consolidadas, disponíveis em: www.fatfgafi.org/en/publications/Mutualevaluations/Assessment-ratings.html. Note-se que nem todas as jurisdições foram avaliadas à luz da metodologia revista da Recomendação 15.

[32] Esta análise baseia-se na avaliação mútua e nos relatórios de acompanhamento das jurisdições que foram avaliadas de acordo com a metodologia revista da Recomendação 15.

que dificulta a formação de uma imagem cabal dos ganhos e dos fluxos financeiros relacionados com o ransomware.

36. A deteção e a comunicação sólidas constituem uma base para o êxito das investigações financeiras (ver secção 6 infra). Com base na experiência das jurisdições e nos estudos de casos apresentados, existem duas fontes principais para detetar os fluxos financeiros relacionados com o ransomware: comunicações de operações suspeitas (COS) e denúncia das vítimas. A presente secção analisa os desafios e as boas práticas em relação ao âmbito dos requisitos de comunicação de COS; a identificação de operações suspeitas; o encorajamento da denúncia por parte das vítimas; e outras fontes de deteção.

Âmbito das obrigações de comunicação de COS

37. As autoridades competentes utilizam habitualmente as COS para detetar ataques de ransomware e como fonte de informação durante as investigações. Até à data, a grande maioria das COS relativas a pagamentos de ransomware são comunicadas por VASP e bancos.

38. Um pequeno número de jurisdições identificou setores que não estão tipicamente sujeitos a obrigações em matéria de ABC/CFT como potenciais fontes adicionais para a deteção de receitas ilícitas relacionadas com o ransomware. Incentivar ou exigir que estes setores não tradicionais comuniquem operações suspeitas pode ser útil, em especial quando estes setores estão diretamente envolvidos na resolução de ataques de ransomware em nome dos clientes.

39. Por exemplo, o setor dos seguros em geral, em especial as instituições envolvidas em ransomware e ciberseguros, pode dispor de informações diretas sobre ataques de ransomware que envolvam clientes segurados que apresentem pedidos de reembolso. Estas entidades não são abrangidas pela definição de «instituição financeira» do GAFI, que abrange a subscrição de seguros de vida e outros seguros relacionados com investimentos. No entanto, ao dialogar com o setor para incentivar ou solicitar a comunicação, algumas jurisdições registaram um impacto inicial positivo na comunicação relativa a ransomware.

Caixa 8. Sensibilização específica para o setor dos seguros, a fim de melhorar a comunicação relativa a ransomware

O setor dos seguros não vida está sujeito a requisitos ABC/CFT em França. Em 2021, foram realizadas ações de sensibilização para este setor através de grupos de trabalho específicos, que reuniram representantes dos setores público e privado. Estes grupos de trabalho procuraram estudar a possibilidade de segurar os ciber-riscos e reforçar a resiliência das empresas contra ciberataques. Um produto fundamental que surgiu destes grupos de trabalho foi um relatório publicado[1] que abrange, entre outros, a evolução do risco de BC relacionado com o ransomware, bem como as obrigações em matéria de ABC/CFT e as boas práticas em matéria de pagamento e reembolso de resgates efetuados.

A "Autorité de Contrôle Prudentiel et de Résolution - ACPR" (Autoridade de Supervisão Prudencial e Resolução) procedeu a um escrutínio de supervisão específico das companhias de seguros, nomeadamente durante inspeções no local. Posteriormente, a ACPR recordou às entidades regulamentadas os seus requisitos em matéria de ABC/CFT quando contratam esses serviços, incluindo a necessidade de monitorizar e obter quaisquer informações financeiras pertinentes (especialmente para o rastreio de pagamentos).

Desde então, a TRACFIN tem observado um aumento das COS relacionadas com pagamentos de ransomware apresentados pelo setor dos seguros, passando de 28 em 2020 e 19 em 2019 para 66 em 2021. O aumento em 2021 deve-se, em parte, a uma única companhia de seguros e os volumes ainda não são suficientemente significativos para tirar quaisquer conclusões ou resultados.

Fonte: França

1. Disponível em Francês em: www.banque-france.fr/sites/default/files/rapport_45_f.pdf

40. As empresas de resposta a incidentes também têm acesso a informações pertinentes relacionadas com ataques e pagamentos de ransomware. Estas empresas, como as empresas forenses digitais de resposta a incidentes e as sociedades de advogados, ajudam as vítimas a responder a ataques de ransomware. Podem facilitar os pagamentos de ransomware a cibercriminosos através da negociação de montantes de pagamentos de ransomware, da conversão da moeda fiduciária dos clientes em ativos virtuais e da transferência dos fundos para contas controladas pelos criminosos. Incentivar ou exigir a comunicação por parte deste setor permite a deteção e comunicação atempadas de ataques de ransomware, especialmente porque é provável que os clientes informem estas entidades do ataque em primeira instância (em alguns casos antes das autoridades). Dependendo do modelo de negócio e dos serviços que prestam, estas empresas podem também ser abrangidas pela definição de VASP (e, por conseguinte, estar sujeitas a obrigações de declaração ABC/CFT e COS) se operarem como uma empresa por conta ou em nome de

outra pessoa singular ou coletiva, trocarem ativos virtuais por outros ativos virtuais ou moeda fiduciária, transferirem ativos virtuais, ou guardarem ou administrarem ativos virtuais.

Caixa 9. Regulamentação das empresas forenses digitais e de resposta a incidentes (DFiR)

As empresas DFiR e as empresas de ciberseguros (CIC) podem ajudar as vítimas de ataques com ransomware no decurso da prestação de serviços, facilitando o pagamento de ransomware. Em 2020 e 2021, a FinCEN (UIF dos EUA) esclareceu nas recomendações sobre ransomware[1] que, dependendo dos factos e circunstâncias, esta atividade poderia constituir uma transferência de dinheiro. As entidades envolvidas na transferência de fundos são obrigadas a registar-se como empresas de serviços de pagamento e estão sujeitas a obrigações em matéria de ABC/CFT. As recomendações incluíam também indicadores de alerta financeiro ou ransomware e pagamentos associados a DFIR e CIC como suporte à identificação de atividades suspeitas e à Comunicação de atividades suspeitas (SAR).

Durante o primeiro semestre de 2021, as comunicações apresentadas por empresas DFiR sediadas nos EUA representaram cerca de 63 % das SAR relativas ao ransomware[2]. Globalmente, as comunicações relacionadas com o ransomware recebidas pela FinCEN em 2021 também aumentaram 188 %. Estas comunicações permitiram à FinCEN analisar e descobrir padrões e informações sobre tendências para apoiar os esforços de toda a administração pública para prevenir e combater os ataques de ransomware. Por exemplo, em 2021, a análise da FinCEN concluiu que o ransomware continua a representar uma ameaça significativa para os setores das infraestruturas críticas dos EUA, para as empresas e para o público. Além disso, a análise salientou que as variantes de ransomware relacionadas com a Rússia foram responsáveis pela maioria das atividades de ransomware comunicadas, representando 69 % do valor de incidentes com ransomware e 75 % dos incidentes relacionados com o ransomware durante o segundo semestre de 2021[3].

Fonte: Estados Unidos

Notas
1. Disponível em Francês em:www.banque-france.fr/sites/default/files/rapport_45_f.pdf
2. Ver o FinCEN Financial Trend Analysis, disponível em: www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
3. Ver o FinCEN Financial Trend Analysis, disponível em: www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

41. A caixa acima ilustra a utilidade de incentivar ou solicitar a comunicação de informações por parte de um vasto leque de entidades que comunicam informações não tradicionais, em

consonância com o risco e o contexto. Tal permite que as atividades suspeitas sejam comunicadas e captadas de acordo com as perspetivas dos diferentes setores, o que reforça a capacidade das autoridades para descobrir e detetar incidentes de outro modo desconhecidos, congregando informações de diferentes setores.

Medidas para melhorar a deteção de operações suspeitas

42. As jurisdições reconhecem que as atividades suspeitas relacionadas com o ransomware são, em geral, pouco comunicadas em todos os setores. Podem surgir problemas de deteção devido à natureza geograficamente descentralizada dos grupos criminosos de ransomware, à variedade de criminosos envolvidos e à utilização de diferentes técnicas de branqueamento de capitais. Nenhum dos setores poderá conseguir ver o cenário completo.

43. Para melhorar a frequência e a qualidade da comunicação de informações pelas entidades regulamentadas e a deteção de um modo mais geral, as jurisdições recorreram a métodos variáveis, como a participação do setor privado, bem como o desenvolvimento e a partilha de indicadores de alerta e de guias de deteção (ver também a secção 8.3 infra).

Caixa 10. Documento de orientação da UIF de Israel (IMPA)

O IMPA, UIF de Israel, realizou uma análise estratégica das comunicações de atividades atípicas para identificar as características dos pagamentos de ransomware. Tal incluiu informações sobre a frequência e o tipo de entidades atacadas, os montantes pagos, o tipo de ativos virtuais utilizados e o envolvimento de terceiros. Tal resultou na publicação de um documento de orientação centrado no ransomware, que incluía sinais de alerta e estudos de casos. O documento foi publicado no site da IMPA, transmitido a todas as entidades comunicantes pertinentes e acompanhado de um comunicado de imprensa oficial.

Os resultados da investigação foram também apresentados em diversas ocasiões em fóruns públicos e conferências profissionais. A publicação promoveu, nomeadamente, a colaboração com o setor israelita de resposta a incidentes, abrindo assim caminho a uma maior expansão dessas relações e à exploração de oportunidades de cooperação e partilha de informações futuras.

Fonte: Israel

1. Apenas disponível em Hebraico em: www.gov.il/BlobFolder/dynamiccollectorresultitem/red-flags-typology-ransomware-impa-140222/he/professional-docs_red_flags_typology_ransomware_impa_140222.pdf

44. Na maior parte dos casos em que um VASP envia uma COS relacionada com ransomware, esta é apresentada com base numa suspeita de que foram adquiridos ativos virtuais para pagar um pedido de resgate. Os indicadores úteis em que os VASP se baseiam incluem as próprias declarações da vítima ao VASP, as aquisições efetuadas por uma empresa conhecida de resposta a incidentes, bem como os pagamentos efetuados direta ou indiretamente relacionados com um endereço virtual com exposição a ransomware provavelmente identificado através da análise de blockchains. Uma vez que os VASP atuam como intermediários diretos em muitos pagamentos de resgate, são uma fonte essencial de COS sobre os fluxos financeiros ilícitos relacionados com o ransomware. Por favor consultar o documento "*Combate ao Financiamento de Ransomware: Potenciais indicadores de risco"*, para uma compilação dos indicadores de risco relevantes em que os VASP podem basear-se.

Caixa 11. Envolvimento de uma empresa de gestão de crises

A IMPA recebeu uma COS através de um VASP israelita relativa a uma empresa de gestão de crises (resposta a incidentes) que adquiriu ativos virtuais (avaliados em dezenas de milhares de dólares na altura) destinados a serem utilizados para um pagamento de ransomware, em nome de uma vítima (não revelada) de ataque. Segundo a COS, foi também comprada uma quantidade adicional de criptomoeda de forma independente por um representante do suspeito alvo de ataque ao mesmo VASP israelita.

A investigação financeira da IMPA revelou que o endereço da carteira que recebeu a maior parte dos fundos tinha ligações a outros ataques de ransomware e recebeu fundos de outros endereços. Os fundos acumulados foram depois transferidos para um VASP localizado numa jurisdição de alto risco. Além disso, os fundos que foram adquiridos de forma independente pela empresa foram transferidos através de vários endereços, tendo uma grande parte acabado por ser financiada através de um "mixer". Foi partilhado um relatório de *intelligence* com as autoridades de polícia competentes para uma investigação mais aprofundada.

Fonte: Israel

45. Ao contrário do que acontece com os VASP, os bancos e outras instituições financeiras e de pagamento podem observar uma vítima que transfira moeda fiduciária para um VASP ou um terceiro que atue em nome da vítima relacionado com um pagamento de resgate e podem enviar uma COS sobre isso. No entanto, podem não ter uma visão direta dos pagamentos relacionados com o ransomware ou do BC relacionado, uma vez que a maioria dos pagamentos é efetuada em ativos virtuais e não em moeda fiduciária. Consequentemente, estas instituições financeiras e de pagamento podem dispor de informações muito limitadas sobre os endereços dos ativos virtuais ou a fonte de fundos, o

que lhes dificulta a utilização de análise de *blockchain*. Para atenuar estes desafios, estas instituições exigem, em muitos casos, indicadores de "proxy" para identificar potenciais pagamentos de ransomware. Com base em estudos de casos, os indicadores comuns incluem transferências invulgares para os VASP (especialmente quando a empresa não negoceia normalmente ativos virtuais), a aquisição de ativos virtuais por empresas de cibersegurança, de seguros e de resposta a incidentes, as declarações dos clientes de que uma transferência de fundos está a ser utilizada para pagar um pedido de resgate, bem como informações de fonte aberta que corroborem ataques (por exemplo, notícias, relatórios de incidentes, etc.). Uma lista pormenorizada dos indicadores de risco relevantes pode ser consultada no documento *Combate ao Financiamento de Ransomware: Potenciais indicadores de risco.*

Denúncia das vítimas

46. Devido aos baixos níveis de comunicação de operações suspeitas sobre pagamentos de ransomware na maioria das jurisdições, as COS continuam a ser uma fonte insuficiente de deteção e compreensão de todo o âmbito dos ataques de ransomware e do branqueamento de capitais conexo, e ainda como suporte às investigações. Por conseguinte, a denúncia das vítimas é também uma importante fonte de informação para detetar e investigar os fluxos financeiros relacionados com o ransomware. A comunicação atempada das vítimas é importante para permitir que as autoridades policiais atuem rapidamente para rastrear os fluxos financeiros e aumentar a probabilidade de resultados positivos em matéria de execução.

47. Os requisitos de comunicação de incidentes variam consoante a jurisdição e dependem do quadro jurídico de cada jurisdição. Na maioria dos casos, a comunicação de incidentes é voluntária. Quando fazem denúncias, as vítimas fazem-no normalmente à polícia, às agências de cibersegurança ou a unidades especiais de comunicação de ciberincidentes ou às equipas locais de resposta a emergências informáticas (CERT).

48. No entanto, a denúncia das vítimas também é limitada, uma vez que os ataques não são todos denunciados. Existem várias razões que podem dissuadir as vítimas de se apresentarem voluntariamente para denunciar ataques de ransomware devido a perceções de potenciais conflitos contra os seus próprios interesses comerciais. Tal inclui preocupações com os danos reputacionais, o desejo de restaurar rapidamente as operações ou o receio de retaliação por parte dos criminosos do ransomware. A natureza do ransomware envolve normalmente o acesso ilícito a dados pessoais e sensíveis dos clientes. Considera-se que uma falha de segurança ou fuga de dados para as autoridades policiais ou público afeta negativamente as empresas e pode resultar em ações cíveis. As vítimas também podem ser ameaçadas por revelações públicas de dados por parte de criminosos se as autoridades policiais forem avisadas.

49. Além disso, as vítimas podem não ter incentivos para comunicar voluntariamente incidentes após o resgate. Nos casos em que as vítimas tenham um ciberseguro, a vítima pode não ter motivação financeira para denunciar um ataque, uma vez que a companhia de seguros pode cobrir o custo do pagamento. Em algumas jurisdições, as vítimas também podem não se manifestar após terem pago resgates por receio de violarem a regulamentação nacional (por exemplo, pagamentos efetuados a uma entidade sancionada) ou serem consideradas cúmplices dos grupos criminosos.

50. As jurisdições adotaram uma série de métodos para incentivar as vítimas a denunciar ataques. Por exemplo, algumas jurisdições implementaram políticas ou realizaram atividades, como campanhas públicas para aumentar a sensibilização para os ataques de ransomware e incentivar a denúncia. Estas políticas e atividades também envolvem normalmente o setor privado e servem para salientar a forma como as autoridades podem ajudar a atenuar o impacto dos ataques de ransomware. Tal inclui a devolução de bens às vítimas e a partilha de códigos de desencriptação para recuperar dados, quando disponíveis.

Caixa 12. "No more Ransom" (Fim ao Resgaste)

O site «No More Ransom» é uma iniciativa da Unidade Nacional de Criminalidade de Alta Tecnologia da polícia neerlandesa, do Centro Europeu da Cibercriminalidade da Europol e de dois parceiros industriais com o objetivo de ajudar as vítimas de ransomware a recuperar os seus dados encriptados sem terem de pagar aos criminosos. O site contém um repositório de chaves e aplicações que podem decifrar dados bloqueados por diferentes tipos de ransomware. Isto ajuda as vítimas a restabelecer o seu acesso aos seus ficheiros encriptados ou aos seus sistemas bloqueados sem terem de pagar.

A iniciativa reúne inúmeros parceiros dos setores público e privado em várias jurisdições, incluindo autoridades e empresas de segurança informática. Visa educar os utilizadores sobre o funcionamento do ransomware e sobre as contramedidas que podem ser tomadas para prevenir eficazmente a infeção. O site incentiva ainda as vítimas a não pagarem quaisquer resgates e fornece ligações para redirecionar as vítimas para o site de denúncia do seu país, a fim de apresentarem uma queixa.

Fonte: No More Ransom

Para mais informação ver: www.nomoreransom.org/en/index.html

51. Para fazer face às preocupações quanto ao risco para a reputação associado à denúncia, algumas jurisdições procuraram criar ambientes seguros para as empresas vítimas de um ataque de ransomware se manifestarem sem receio de danos à reputação, por exemplo, através de contactos regulares e da participação em conferências empresariais. Outra boa prática é a criação de portais de «balcão único» como fonte única para as vítimas comunicarem incidentes, servindo simultaneamente de plataforma de recursos para aconselhamento especializado e medidas de reparação. Embora estes esforços se centrem frequentemente na deteção do ataque de ransomware propriamente dito, as informações obtidas a partir da denúncia de uma vítima são vitais para as investigações financeiras, incluindo a deteção dos fluxos financeiros associados e do branqueamento de capitais.

Caixa 13. Centro Canadiano para a Cibersegurança

O Centro Canadiano para a Cibersegurança (Cyber Centre) abriu em 2018 como uma iniciativa fundamental no âmbito da Estratégia Nacional de Cibersegurança do Canadá. O Cyber Centre é a fonte única de aconselhamento especializado, orientação, serviços e apoio em matéria de cibersegurança para governo, proprietários de infraestruturas críticas e operações, o setor privado e o público canadiano. Disponibiliza recursos aos indivíduos e às empresas, incluindo orientações sobre a forma de prevenir e recuperar de incidentes de ransomware e emite comunicados sobre o cenário de ameaça em termos de ransomware. O Cyber Centre recolhe comunicações de ciberincidentes de partes envolvidas no setor público e no setor privado, tanto nacionais como internacionais. As comunicações podem ser feitas online, por correio eletrónico ou por telefone. O Centro incentiva a comunicação à polícia caso considerem que um ciberincidente constitui uma ameaça iminente à vida ou seja de natureza criminosa.

Fonte: Canadá

52. Algumas jurisdições adotaram a abordagem que consiste em identificar determinadas indústrias ou instâncias em que a denúncia das vítimas é obrigatória, por exemplo, ataques a infraestruturas críticas (como energia, comunicações, cuidados de saúde, etc.) ou fugas de dados. Em muitas jurisdições, estes setores podem também incluir setores financeiros sujeitos a requisitos em matéria de ABC/CFT (por exemplo, no setor bancário), em que as entidades regulamentadas são obrigadas a comunicar incidentes significativos às autoridades competentes, como as autoridades de supervisão, no âmbito do quadro regulamentar. Os quadros legais de proteção de dados podem também incentivar ou exigir a comunicação obrigatória de violações de dados que envolvam informações pessoais, o que pode conduzir a deteção atempada. Para melhorar a deteção de fluxos financeiros ilícitos, é uma boa prática transmitir informações financeiras relevantes durante essa comunicação (como o endereço da wallet, ou o tipo de ativo virtual).

Outras fontes de deteção

53. Tal como acima referido, os intercâmbios e a colaboração com partes interessadas fora das instituições financeiras, dos setores não-financeiro e dos VASPs, como por exemplo os fornecedores de serviços Internet e o setor da cibersegurança, podem constituir uma fonte de informação potencialmente valiosa. No entanto, estes setores podem não estar sujeitos a requisitos regulamentares em matéria de ABC/CFT, incluindo a comunicação de COS. Em alguns casos, pode existir um potencial conflito de interesses (por exemplo, empresas de cibersegurança que atuam em nome das vítimas), o que pode limitar a comunicação proactiva. Nessas circunstâncias, as informações podem ser obtidas através de mecanismos informais, tais como parcerias público-privadas que envolvam estas entidades, ou através de um envolvimento direto.

Caixa 14. Colaboração com empresa de cibersegurança

Uma empresa vítima contratou uma empresa de cibersegurança após ter sofrido um ataque de um grupo de ransomware. Foi exigido um resgate em Bitcoin ou em Monero. A vítima acabou por pagar o resgate ao grupo criminoso através da empresa de cibersegurança.

Posteriormente, a empresa de cibersegurança informou a autoridade competente acerca deste incidente, o que permitiu rastrear os fluxos ilícitos. A autoridade competente colabora frequentemente com empresas de cibersegurança. A colaboração visa uma interferência mínima no trabalho de recuperação das empresas de cibersegurança para com os seus clientes, mas assegura que os elementos essenciais, como os endereços IP e cripto, são fornecidos para a investigação criminal.

Neste caso, as autoridades policiais observaram a utilização de técnicas de anonimato, como a utilização de mixers e inúmeros endereços de wallets não alojados. Na altura da investigação, uma parte significativa dos ativos era mantida em carteiras não alojadas e, por conseguinte, não pôde ser identificada. Uma parte significativa dos fundos terá sido canalizada através de dois VASPs em jurisdições estrangeiras.

Fonte: Suíça

54. As autoridades competentes também detetam ataques e pagamentos de ransomware através de investigações financeiras independentes, utilizando análises de blockchains em carteiras conhecidas por terem ligações a ransomware. Tal inclui também o acompanhamento de ataques conhecidos, blogues e análises de fontes abertas partilhadas por empresas de análise de blockchains, bem como o contacto proactivo com potenciais vítimas após a análise.

55. Estes esforços podem revelar outras causas de ataques anteriores de ransomware. Pode também revelar informações sobre a magnitude de um ataque atribuível a um criminoso de ransomware, bem como as tendências, tipologias e infraestruturas que os criminosos utilizam para branquear, receber e utilizar os seus produtos ilícitos.

Caixa 15. Análise de fontes abertas para identificar criminosos RaaS

A UIF Turquia recebeu uma COS de um VASP relativa a um endereço de carteira de ativos virtuais ligado a uma pessoa registada como «Nome 1» pelo VASP. Uma pesquisa online do nome concluiu que existe um site com o mesmo nome. Uma investigação mais aprofundada revelou que o site estava a realizar atividades relacionadas com a Darknet e funcionava como intermediário na venda de ransomware e de outro software malicioso.

Uma análise mais aprofundada através de fontes abertas concluiu que:

- A pessoa envolvida na transação mencionada na COS utilizou um pseudónimo diferente («Nome 2»), o que levou à identificação do nome real da pessoa («Pessoa X»), que era anteriormente uma pessoa de interesse para o Departamento de Combate ao Cibercrime da Polícia.
- O suspeito (Pessoa X) oferecia serviços e produtos, tais como acesso não autorizado, acesso a informações confidenciais, credenciais de identidade falsas, pirataria informática de contas nas redes sociais, venda de hiperligações informáticas e páginas de phishing.
- Os pagamentos relativos a estes produtos/serviços ilegais foram efetuados com Bitcoin e outros ativos virtuais.

Posteriormente, a UIF Turquia solicitou informações adicionais ao VASP relacionadas com a pessoa incluída na COS, em especial os endereços da carteira de ativos virtuais, as operações financeiras (ativos virtuais e moeda fiduciária) e outras informações pessoais. Foi elaborado e apresentado um relatório de análise aos departamentos de cibercriminalidade da Polícia Nacional Turca, suspeitando-se que a pessoa referida na COS era intermediária na venda de ransomware e de outros programas informáticos maliciosos. As investigações estão a decorrer.

Fonte: Turquia

56. As jurisdições também podem ser alertadas para ataques e pagamentos de ransomware através de informações partilhadas por outras jurisdições. A cooperação internacional, o auxílio judiciário mútuo e o intercâmbio informal de informações com jurisdições estrangeiras podem fornecer informações sobre fundos obtidos através de exchanges nacionais ligadas a ataques/vítimas estrangeiros.

Ações propostas

- As jurisdições devem ajudar as entidades regulamentadas a detetar ransomware e o BC conexo e a comunicar operações suspeitas, nomeadamente através da partilha de tendências, guias de deteção e indicadores de alerta (como os contidos no documento Combate ao Financiamento de Ransomware: Potenciais Indicadores de Risco) com as entidades obrigadas relevantes.
- As jurisdições devem incentivar as vítimas a comunicarem voluntariamente incidentes, por exemplo sensibilizando para o apoio e os recursos disponíveis ou criando canais seguros para a denúncia.
- As jurisdições devem ponderar a criação de canais de comunicação com intervenientes não tradicionais que possam não estar sujeitos a requisitos em matéria de ABC/CFT (tais como empresas de seguros cibernéticos e de resposta a incidentes), a fim de melhorar as fontes de deteção.

Estratégias de investigação financeira

57. O objetivo de quase todos os ataques de ransomware é gerar lucros. A maioria das jurisdições reconhece que as investigações de ransomware têm uma componente financeira significativa. Estudos de casos mostram que o rastreio de ativos virtuais é uma parte essencial das investigações de ransomware. Nas jurisdições que comunicaram que investigam ataques com ransomware, existe normalmente uma investigação financeira paralela que deteta o pagamento de resgates.

58. A nível mundial, verifica-se uma falta de experiência em investigações de BC relacionados com ransomware. Muito poucas jurisdições instauraram acusações de BC em casos de ransomware. Tal pode, em parte, ser atribuível aos desafios em matéria de deteção e comunicação, tal como referido na secção 5 supra.

59. A presente secção explora desafios específicos e boas práticas em investigações financeiras bem-sucedidas de ransomware e de branqueamento de capitais conexos, incluindo i) trabalhar com as vítimas para aceder a informações; II) técnicas e mecanismos de investigação; e iii) recuperação de ativos.

Agir rapidamente e trabalhar com as vítimas para aceder à informação

60. Dada a natureza dos cibercrimes como o ransomware, os resultados bem-sucedidos das autoridades dependem da capacidade de avançar rapidamente e recolher informações essenciais relacionadas com o ataque e o pagamento do ransomware. Tal inclui os endereços de ativos virtuais, o montante total do resgate e o tipo de ativo virtual utilizado,

as datas das transferências, os tipos de serviços envolvidos, a identidade da vítima, as comunicações entre a vítima e os criminosos de ransomware, bem como quaisquer terceiros envolvidos no pagamento de resgates.

61. Em muitos casos, a recolha dessas informações depende da cooperação das vítimas ou de terceiros envolvidos na resposta ao incidente e/ou no processo de pagamento de resgates. No entanto, tal como referido anteriormente, as vítimas podem mostrar-se relutantes em denunciar incidentes às autoridades responsáveis (ver secção 5.3 supra). As vítimas também podem mostrar-se relutantes em cooperar devido à perceção de interesses concorrentes com a aplicação da lei; muitas vezes, as vítimas pretendem retomar as operações comerciais o mais rapidamente possível e podem preferir pagar o resgate. Podem também temer retaliações por parte de criminosos por implicarem a aplicação da lei. Por outro lado, as autoridades policiais podem necessitar de tempo para obter provas forenses, desenvolver operações controladas e tomar outras medidas de investigação, o que pode atrasar a retoma dos serviços.

62. As denúncias tardias ou incompletas, bem como a falta de cooperação por parte das vítimas, podem comprometer a qualidade das informações disponíveis para prosseguir com êxito as investigações. A ausência de um plano de ação claro sobre a forma de atuação das vítimas após o ataque e/ou o pagamento, pode comprometer os elementos de prova disponíveis devido à falta de preservação dos dados. As boas práticas debatidas na secção 5.3, como as campanhas públicas e outros esforços para incentivar a participação das vítimas, são importantes para atenuar estes desafios.

63. Algumas jurisdições salientaram ainda a importância da partilha de informações entre os investigadores dos cibercrimes (subjacentes) e dos investigadores de BC. Durante a recolha de provas forenses para a investigação subjacente ao ransomware, as autoridades responsáveis pela aplicação da lei irão inevitavelmente recolher informações relevantes para a investigação de branqueamento de capitais. Essas informações permitem às autoridades policiais estabelecer ligações entre diferentes grupos e afiliados de atacantes de ransomware, e permitem dar seguimento a uma investigação financeira mais ampla. Ver secção 8.2 para mais informações sobre a forma como várias autoridades nacionais competentes podem cooperar de forma eficaz.

Caixa 16. Fontes de prova pertinentes para as investigações financeiras obtidas durante investigações subjacentes

Provas forenses: Exemplos de provas forenses incluem — vetores de ataque (ou seja, a forma como os criminosos conseguem o acesso não autorizado); informações sobre o tipo de ransomware; Endereços IP; nomes ou pseudónimos utilizados; e os dispositivos do atacante. Essas informações podem ser recolhidas diretamente junto das vítimas, dos fornecedores de serviços Internet, das empresas de cibersegurança e de resposta a incidentes e da utilização de tecnologia forense.

Provas diretas do setor privado: As empresas do setor privado relevantes incluem as que são proprietárias da tecnologia ou infraestrutura que foi utilizada de forma abusiva num ataque de ransomware. Os investigadores podem obter informações sobre assinantes junto de empresas de correio eletrónico ou de redes sociais junto das quais o autor do crime tenha tido contas para comunicar com a vítima.

Informação de fonte aberta: A análise de informações de fonte aberta, incluindo redes sociais, fóruns online, mercados da Darknet e comunicações por criminosos de ransomware pode ajudar a identificar potenciais autores.

Técnicas e mecanismos de investigação

Relevância das técnicas de investigação tradicionais

64. As tecnologias utilizadas pelos criminosos de ransomware para ocultar as suas localizações, identidades e fluxos financeiros podem dificultar as investigações. Os desafios específicos incluem a utilização de VPNs, «The Onion Router»[33], ou correio eletrónico encriptado para permitir uma maior privacidade e segurança, bem como atividade anónima à medida que o tráfego passa através de uma rede. Estes desafios podem aumentar devido à rapidez com que essas tecnologias evoluem.

65. A Recomendação 31 do GAFI estabelece as bases para conferir às autoridades policiais os poderes necessários para investigações financeiras eficazes. Estas técnicas de investigação tradicionais continuam a ser pertinentes para superar estes desafios, a fim de permitir a recolha e análise de informações essenciais relacionadas com os fluxos financeiros do ransomware. Tal inclui a vigilância, a interceção de comunicações e as operações encobertas. No entanto, estas técnicas tradicionais terão de ser adaptadas no contexto de investigações financeiras que envolvam ativos virtuais. Exemplos de como tal pode ser feito para alcançar resultados de investigação bem-sucedidos:

[33] Também conhecido por TOR, um software de fonte aberta que permite aos utilizadores navegar na Internet de forma anónima.

• *Vigilância*: Determinar os tipos de dispositivos eletrónicos que um suspeito utiliza; detetar quaisquer carteiras virtuais utilizadas, bem como os seus métodos preferidos de comunicação eletrónica.

• *Interceção de comunicações e operações encobertas*: Desenvolver informação sobre as atividades do suspeito visado e dos trabalhos da organização criminal, identificar as pessoas associadas ao suspeito visado e informações e bens financeiros relevantes, bem como infiltrar em comunidades criminosas (como os fóruns Darknet) para anular o anonimato dos autores e beneficiários finais.

• *Produção de prova*: Obtenção de informações de VASPs ou de outras instituições financeiras envolvidas em pagamentos de resgates, etc.

66. A utilização destes instrumentos nas investigações financeiras pode ser mais esclarecida através de detalhes de COS ou denúncias das vítimas (ver secção 5 supra). As autoridades responsáveis pela aplicação da lei podem identificar as instituições financeiras e os VASP pertinentes através de COS e análises de blockchains (ver secção 6.2.2), a fim de obter a prova necessária através de meios de obtenção de prova. Os VASP podem fornecer informações de identificação úteis como suporte às investigações financeiras relacionadas com ransomware, no sentido de obter informações básicas sobre o beneficiário efetivo e sobre operações (por exemplo, identidade do utilizador e informações conexas, endereços IP, cartões de crédito ou contas bancárias, etc.).

67. No entanto, tal como referido na secção 3, algumas redes de ransomware foram também ligadas a jurisdições de alto risco em que os requisitos em matéria de ABC/CFT são fracos ou inexistentes para os VASP ou em que, muitas vezes, estes não cumprem os requisitos. Por conseguinte, as investigações podem enfrentar complicações se os fundos circularem ou forem detidos nesses VASPs. Nesses casos, os VASP podem não recolher informações pertinentes ou não responder a pedidos das autoridades.

68. Os investigadores enfrentam desafios semelhantes quando os criminosos utilizam carteiras não alojadas. Tal proporciona aos utilizadores o controlo dos ativos virtuais sem o envolvimento de um VASP, o que coloca desafios à deteção e prevenção da atividade de BC. A falta de ligação a uma entidade terceira (que tenha de ser registada/licenciada ao abrigo dos padrões do GAFI) pode complicar a capacidade das autoridades para identificar o proprietário da carteira, uma vez que não existe uma entidade externa junto da qual se possa procurar informações.

69. A aplicação limitada da «"Travel Rule"» do GAFI pelos VASP oferece igualmente oportunidades para os cibercriminosos evitarem a deteção e dificultarem as investigações. A "Travel Rule" exige que os VASP e outras instituições financeiras que efetuem transferências de ativos virtuais partilhem informações sobre o remetente (origem) e o destinatário (beneficiário) juntamente com qualquer transferência. Tal aumenta a transparência das operações para prevenir a utilização abusiva e constitui uma fonte de informação a que as autoridades policiais podem ter acesso para identificar as partes envolvidas numa determinada transação. No entanto, um relatório do GAFI de 2022 concluiu que apenas um terço das jurisdições comunicou ter aprovado legislação para aplicar a "Travel Rule" para os VASP, e ainda menos estão realmente a aplicar estes requisitos[34]. Esta falta de regulamentação consistente reduz a quantidade de informação de

[34] Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (junho 2022) do GAFI. Esta *Targeted Update* cobre apenas países cujos MERs [*Mutual Evaluation Report*]/FURs [*Follow-Up Report*] foram publicados entre junho 2021 e maio 2022.

VASPs disponível às autoridades em jurisdições sem obrigações em matéria de "Travel Rule". Significa também que os VASP em jurisdições conformes que efetuem operações com VASPs em jurisdições não conformes não conseguirão provavelmente obter essas informações, limitando as informações disponíveis para os investigadores, mesmo nas jurisdições que aplicam a "Travel Rule".

Caixa 17. Técnicas tradicionais e financeiras de investigação contra um Grupo de ransomware

Uma empresa vítima italiana apresentou uma queixa policial após ter efetuado um pagamento de resgate em Bitcoin e assim desbloquear com êxito os seus dados infetados por um ataque de ransomware. O pagamento foi efetuado através de um VASP mencionado no pedido de resgate.

As investigações policiais contra o VASP revelaram que o respetivo site estava formalmente registado em Itália. Posteriormente, foi identificado um indivíduo italiano que se revelou ter facilitado os fluxos de Bitcoin ligados ao pagamento do resgate. Posteriormente, a polícia revistou o seu apartamento e apreendeu cartões de pagamento, telemóveis, bem como artigos de hardware, como discos rígidos, unidades USB e tablets. As escutas telefónicas e a análise das mensagens de telemóvel trocadas resultaram na identificação de um grupo de outros indivíduos italianos (o «Grupo») que desempenharam um papel semelhante na facilitação dos fluxos de Bitcoin relacionados com o ransomware. Investigações financeiras concluíram que os fundos fiduciários enviados pelas vítimas de ransomware foram transferidos pelo Grupo para contas bancárias estrangeiras mantidas por VASP estrangeiros, incluindo as localizadas em jurisdições de alto risco

Com base nas investigações financeiras, bem como na análise forense dos telefones e dos artigos de hardware, as autoridades concluíram que o Grupo estava a espalhar ransomware pelas vítimas, com montantes de resgate de várias centenas de euros por cada ataque. O Grupo foi acusado de extorsão relacionada com o ransomware e subsequente branqueamento dos proventos, que se estima ascenderem a cerca de 300 000 EUR referentes a várias vítimas. As investigações estão ainda em curso.

Fonte: Itália

Técnicas Específicas para ativos virtuais

70. Para além das técnicas tradicionais, as autoridades devem basear-se em técnicas específicas para ativos virtuais para realizar investigações financeiras relacionadas com o «ransomware». A maioria dos ativos virtuais opera numa blockchain pública, que funciona como uma base de dados visualizável através da qual podem ser rastreadas informações sob pseudónimo associadas a operações de ativos virtuais, utilizando ferramentas de

análise de blockchains de fonte aberta ou de subscrição (ver secção 7 infra). A análise de blockchains, combinada com as técnicas de investigação tradicionais, poderá permitir que os investigadores obtenham as informações necessárias para identificar os criminosos de ransomware online e os seus afiliados, bem como rastrear a circulação de produtos ilícitos.

71. O rastreio dos proventos através da análise de blockchains exige normalmente a identificação de um endereço inicial da carteira, o que faz da deteção e recolha de informações sobre o pagamento de resgates um primeiro passo fundamental. Uma vez fornecido um endereço inicial da carteira, os investigadores podem identificar os pagamentos efetuados e recebidos por esse endereço, entre outras possibilidades. No entanto, as informações disponíveis podem depender do serviço utilizado. Embora a blockchain pública contenha informações úteis para as investigações financeiras, algumas operações de ativos virtuais também ocorrem fora da blockchain. Certas análises de blockchains dependem ainda mais de algoritmos de agregação *[clustering*] e de outras técnicas para agrupar endereços de carteiras digitais ou operações que possam estar associadas à criminalidade, como o ransomware.

72. As informações provenientes da análise de blockchains podem reforçar o recurso a técnicas de investigação tradicionais. Por exemplo, a análise de blockchains pode ajudar a identificar um VASP que aloja um endereço de carteira que recebeu um pagamento enviado de ou para criminosos de ransomware, o que poderia levar as autoridades policiais a utilizar métodos obrigatórios para solicitar informações sobre o endereço da carteira ao VASP em questão.

Caixa 18. Investigações de carteiras conhecidas de ransomware que revelem mais vítimas desconhecidas

Estava em curso uma análise da ameaça de blockchains online relativa a um endereço Bitcoin, que se sabia ter recebido aproximadamente 20 Bitcoin entre 12 de maio de 2017 e 27 de maio de 2021. Descobriu-se que o referido endereço Bitcoin podia estar diretamente ligado a ransomware que infetou várias entidades empresariais e departamentos governamentais na África do Sul. A análise revelou que um endereço local de Bitcoin separado, pertencente a um VASP na África do Sul, forneceu, em fevereiro de 2018, 0.06 Bitcoin para o endereço acima sob investigação.

Após obtenção de informações sobre os subscritores junto do VASP, identificou-se uma vítima sendo que o VASP reconheceu que a mesma tinha sofrido um prejuízo financeiro. Preferiu não comunicar o incidente às autoridades de investigação locais, uma vez que temia embaraço público por falta de segurança dos dados dos clientes. A questão foi remetida pela UIF África do Sul às autoridades locais de investigação. Uma vez que a vítima identificada não quis instaurar qualquer acusação, o processo foi retirado e encerrado pelas autoridades policiais locais.

Fonte: África do Sul

73. Os métodos de branqueamento que reforçam o anonimato utilizados pelos criminosos de ransomware (discutidos na secção 3 supra) também colocam desafios às autoridades responsáveis em termos de rastreamento e atribuição de operações feitas através da análise de blockchains, embora algumas empresas de análise de blockchain tenham desenvolvido tecnologia para atenuar algumas destas medidas. Os modelos associados ou os fornecedores de RaaS, bem como o envolvimento de "mulas" de dinheiro, também aumentam a complexidade das investigações financeiras relacionadas com o ransomware. Como os pagamentos nem sempre podem ser rastreados até à vítima, torna-se difícil identificar os endereços utilizados para o pagamento inicial de ativos virtuais que normalmente servem de base para a análise dos blockchains.

74. Para além de utilizarem a análise de blockchains para rastrear o pagamento do resgate e do seu subsequente branqueamento, os investigadores devem também rastrear as operações anteriores associadas ao grupo de ransomware. Esta etapa adicional permite que as autoridades policiais identifiquem potenciais tendências e tipologias e/ou formas adicionais de criminalidade.

75. Como boa prática, as autoridades em algumas jurisdições desenvolveram bases de dados de informações essenciais sobre mulas, ou endereços de carteiras envolvidas em casos de ransomware. Estas bases de dados incluem geralmente dados sobre incidentes que identificam informações de mulas, montante dos danos e criminosos do ransomware (por exemplo, número de conta, endereços de carteiras, nomes de utilizador). Essas bases de dados ajudam a identificar e rastrear os pagamentos de ransomware e o BC conexo, fornecendo um repositório para fazer corresponder os resultados de investigações anteriores (incluindo informações sobre pagamentos) a incidentes atuais e futuros. Tal permite às autoridades policiais compreender a rede de branqueamento mais vasta que pode abranger várias entidades e setores regulamentados.

Recuperação de ativos

76. Para além do reforço das capacidades de deteção e investigação financeira, as autoridades necessitam também de poderes legislativos e de capacidade para apreender e confiscar ativos virtuais. As operações de ativos virtuais são quase instantâneas. Isto significa que, logo que as autoridades competentes tenham conhecimento de um ataque de ransomware e de um pagamento de resgate, devem poder localizar rapidamente o pagamento do resgate e ter acesso rápido a poderes de congelamento/suspensão, idealmente numa questão de horas, para evitar a dissipação. Em conformidade com a Recomendação 4 do GAFI, esses poderes já devem existir em muitas jurisdições e podem variar de forma.

77. Várias jurisdições salientaram igualmente a utilidade de instrumentos alternativos para intercetar proventos ilícitos, como os poderes de suspensão das UIFs, no que toca a suspeitas de bens de origem criminosa identificados nas COS. A fim de acompanhar a natureza dinâmica dos ativos virtuais, pode também ser necessário equacionar a atualização de legislação, regulamentação, políticas e procedimentos existentes em matéria de perda de ativos.

Caixa 19. "Colonial Pipeline" (Gasoduto colonial)

Em junho de 2021, o Departamento de Justiça dos EUA anunciou que tinha apreendido 63.7 bitcoins no valor aproximado de 2,3 milhões de dólares. Estes fundos representavam alegadamente o produto do pagamento de resgates em 8 de maio de 2021 a pessoas singulares de um grupo conhecido como DARKSIDE, que tinha visado o Colonial Pipeline, o que resultou na inoperacionalidade de infraestruturas críticas. O mandado de apreensão foi autorizado por um juiz da Califórnia logo no início desse dia.

Por volta de 7 de maio de 2021, o Colonial Pipeline foi vítima de um ataque de ransomware amplamente publicitado, que levou a empresa a inoperacionalizar partes da sua infraestrutura. O Colonial Pipeline informou o FBI que uma organização denominada DARKSIDE acedeu à sua rede informática e que tinha recebido e pago um pedido de resgate de cerca de 75 bitcoins. Tal como alegado na declaração sob compromisso de honra, ao rever o registo público da Bitcoin, as autoridades policiais conseguiram rastrear múltiplas transferências de bitcoin e identificar que cerca de 63.7 bitcoins, que representam o produto do resgate da vítima, tinham sido transferidos para um endereço específico. Esta bitcoin representa os proventos que se detetaram estarem ligados a uma intrusão informática e a bens envolvidos em BC, e poderá ser apreendida ao abrigo de leis penais e cíveis de perda de ativos.

Fonte: Estados Unidos

Ações propostas

- As autoridades competentes devem utilizar e adaptar, se necessário, as técnicas policiais tradicionais, bem como técnicas específicas para ativos virtuais, para realizar investigações de BC relacionadas com o ransomware.
- As jurisdições devem assegurar que as autoridades dispõem e mantêm as capacidades e os poderes necessários para apreender e confiscar de forma rápida e eficaz os bens, em especial os ativos virtuais

Aptidões e conhecimentos especializados

78. Tal como referido na secção 6.2, embora as técnicas policiais tradicionais continuem a ser fundamentais para as investigações de BC relacionadas com o ransomware, são também necessários conhecimentos técnicos especializados para o êxito das investigações e ações penais em matéria de branqueamento de capitais, bem como para a recuperação de bens relacionados com ativos virtuais. Tal inclui o conhecimento tecnológico e jurídico do ecossistema dos ativos virtuais.

79. Além disso, as equipas de investigação que trabalham em casos de BC ou na recuperação de bens relacionados com ransomware devem incluir pessoal com competências técnicas em cibersegurança, informática forense, informações online e plataformas de fonte aberta. Tal deve incluir uma tónica no reconhecimento online para recolher informações financeiras relativas a operações de ativos virtuais do domínio público, incluindo informações que possam ser identificadas a partir da análise de blockchains, da digitalização de sites, das redes sociais, de fóruns online, da Darknet e dos mercados obscuros, bem como de denúncias online de abusos.

80. Especialmente quando estão envolvidos ativos virtuais, as autoridades competentes podem necessitar de novas competências e conhecimentos especializados para interpretar e aceder à informação. Especificamente, as autoridades devem familiarizar-se com as capacidades de análise e monitorização dos blockchains, tais como a utilização de ferramentas analíticas de blockchains, incluindo software gratuito para ver a blockchain pública, e análise para rastrear fundos. Além disso, diferentes ferramentas proporcionam capacidades variáveis e complementares (análise de diferentes tipos de ativos virtuais, capacidade para analisar "chain hopping", informações de fonte aberta, etc.).

81. São necessários formação e conhecimentos técnicos especializados para desenvolver estes instrumentos variados e utilizá-los durante as investigações, e algumas jurisdições identificaram formas de integrar especialistas nas investigações pertinentes (ver secção 8.2). O acesso aos recursos necessários pode ser dispendioso e algumas jurisdições podem não dispor dos recursos necessários para apoiar o desenvolvimento destas competências, o que pode prejudicar a capacidade das autoridades para prosseguir a investigação do BC relacionado com o ransomware.

82. Se os conhecimentos especializados a nível interno não estiverem disponíveis ou forem insuficientes, as jurisdições podem ponderar a utilização de instrumentos criados por empresas do setor privado. As ferramentas de terceiros podem ajudar as autoridades a identificar, rastrear e atribuir operações de ativos virtuais em todas as grandes blockchains de ativos virtuais e na maior parte das mais pequenas. Atualmente, estes instrumentos suportam centenas de tokens e utilizam métodos como o agrupamento de algoritmos, o scraping de conteúdos Web e a monitorização de bases de dados de burlas que permitem a um investigador ligar e atribuir uma vasta gama de operações a pessoas e entidades do mundo real. As ferramentas geram gráficos de operações e permitem a análise da rede, o que permite às entidades compreender e, em seguida, apresentar estas associações complexas a júris e tribunais em ações penais subsequentes e de recuperação de ativos. Estes instrumentos podem também ajudar as autoridades a identificar os VASP que possam ter sido utilizados para o branqueamento ou para a troca de proventos ilícitos por moeda fiduciária, e que possam dispor de informações pertinentes para sustentar a investigação.

83. Em termos de recuperação de ativos, a apreensão e a gestão de ativos virtuais exigem conhecimentos técnicos e jurídicos adicionais. As autoridades devem estar preparadas para tomar as medidas adequadas e aplicar procedimentos que garantam a apreensão e o armazenamento adequados. É uma boa prática estabelecer mecanismos especializados para apreender, confiscar e alienar bens virtuais. Tal pode incluir uma apreensão adequada, planeamento, gestão de "seed phrases"[35] e "cold storage" de ativos virtuais apreendidos (ou

[35] Um conjunto de palavras gerado aleatoriamente por uma aplicação de wallet e numa ordem específica, que podem ser utilizadas para recuperar ou obter acesso a uma(s) chave(s) privada(s) por forma a contornar uma proteção (por exemplo: palavra-passe).

seja, armazenamento numa carteira não alojada offline), bem como questões relacionadas com questões de custódia da prova.

Ações propostas

- As autoridades competentes devem possuir as competências e os conhecimentos especializados necessários para o êxito das investigações financeiras relacionadas com ransomware. Tal inclui o desenvolvimento, o acesso e a formação em matéria de análise e monitorização das blockchains.
- As jurisdições devem assegurar a existência de mecanismos especializados para gerir adequadamente os ativos virtuais apreendidos.

Políticas nacionais e coordenação

Avaliação e estratégia nacionais

84. A Recomendação 1 do GAFI exige que as jurisdições identifiquem e avaliem os seus riscos de BC e apliquem uma abordagem baseada no risco para atenuar os mesmos. Esta abordagem deve também servir de base para que as jurisdições afetem eficientemente os recursos em todo o seu regime ABC/CFT.

85. O ransomware é frequentemente abordado do ponto de vista da avaliação das ameaças à cibersegurança. Por exemplo, a nível nacional, algumas jurisdições adotaram estratégias nacionais em matéria de cibersegurança ou cibercriminalidade, que suportam a coordenação interna e proporcionam o compromisso político de perseguir ativamente o ransomware e os fluxos financeiros ilícitos associados. As estratégias nacionais envolvem normalmente várias agências governamentais[36], e podem incluir autoridades competentes em matéria de ABC/CFT, como os ministérios da Justiça, das Finanças e do Interior, bem como o setor privado. No entanto, é importante notar que o objetivo de muitas destas estratégias não se centra necessariamente nos riscos financeiros ilícitos, que devem ser considerados em pormenor através de uma avaliação dos riscos.

Caixa 20. Estratégia Nacional de Cibersegurança de Espanha

A Estratégia Nacional de Cibersegurança de Espanha (atualizada pela última vez em 2019) visa reforçar as competências para combater as ciberameaças. Define as prioridades, os objetivos e as medidas adequadas para alcançar e manter um elevado nível de segurança das redes e dos sistemas de informação. Algumas das principais linhas de ação da estratégia procuram reforçar as

[36] Estas agências incluem as agências policiais, de defesa, de segurança e de comunicação da informação, tendo em conta a ameaça que o ransomware representa para a segurança nacional.

competências para combater as ciberameaças e reforçar as capacidades para investigar e reprimir os cibercrimes.

A estratégia estabeleceu a necessidade de reforçar a cooperação jurídica e policial, com recursos suficientes atribuídos aos organismos competentes e formação em matéria de competências profissionais. Tal está também ligado à criação de um quadro institucional para a cibersegurança, que criou o Conselho Nacional de Cibersegurança. Este Conselho é liderado pelo Primeiro-Ministro espanhol com o objetivo de coordenar a política nacional de segurança em matéria de cibersegurança e promover a coordenação, a colaboração e a cooperação entre os organismos das administrações públicas e o setor privado[2], que desempenha um papel importante para uma abordagem multidisciplinar.

Fonte: Espanha

Notas:
1. Ministérios dos Negócios Estrangeiros, da Justiça, da Defesa, dos Assuntos Internos, do Tesouro, da Presidência; o Centro Nacional de Intelligence, o Departamento de Segurança Nacional e outros.
2. Entre os peritos do setor privado contam-se os das associações profissionais, empresas e universidades.

86. As jurisdições devem assegurar que também têm em conta a ameaça que o ransomware representa no âmbito da sua avaliação nacional do risco de BC, em conformidade com a Recomendação 1 do GAFI. Esta avaliação fornece a base em que as jurisdições podem elaborar medidas de mitigação — incluindo a aplicação das ações sugeridas constantes do presente relatório. Ao compreender os riscos de BC associados ao ransomware, as jurisdições poderão afetar recursos em consonância com uma abordagem baseada no risco, nomeadamente para desenvolver competências técnicas e conhecimentos especializados em ativos virtuais e adquirir ferramentas analíticas de blockchains para as autoridades competentes relevantes em matéria de ABC/CFT.

87. As jurisdições em que o ransomware e o branqueamento de capitais conexo não representam atualmente uma ameaça interna significativa devem também ter em conta os riscos de financiamento ilícito colocados pelo ransomware, em especial devido à relação única entre o ransomware e os ativos virtuais. As jurisdições devem ter em conta não só a ameaça de ataques de ransomware a vítimas domésticas, mas também o potencial que os criminosos de ransomware têm estabelecido nas suas jurisdições, ou que os VASP na sua jurisdição estão a ser utilizados para branquear ou trocar os proventos do ransomware. Por exemplo, muitos VASP podem ter distribuído arquiteturas por várias jurisdições, como o registo estar numa jurisdição, ter pessoal localizado noutra jurisdição e o alojamento de infraestruturas técnicas ou chaves privadas em jurisdições distintas. Isto significa que essas jurisdições podem ainda estar expostas aos movimentos financeiros ilícitos associados ao ransomware, em especial através do setor VASP.

Caixa 21. Avaliação do ransomware nas avaliações nacionais de risco de BC

Em março de 2022, os Estados Unidos publicaram a sua terceira avaliação nacional do risco de branqueamento de capitais (NMLRA), que destaca as ameaças financeiras ilícitas mais significativas, incluindo a cibercriminalidade, bem como vulnerabilidades relacionadas com ativos virtuais. A NMLRA identificou que os incidentes de cibercriminalidade aumentaram significativamente desde 2018 e que o ransomware representa uma ameaça financeira ilícita particularmente significativa. Por exemplo, a NMLRA concluiu que a gravidade e a sofisticação dos ataques de ransomware aumentaram durante a pandemia de COVID-19. A NMLRA fornece informações substanciais sobre as tendências de ataque de ransomware, incluindo a utilização de ransomware como modelo de serviço e táticas de dupla extorsão. A NMLRA também destaca inúmeras tipologias de BC, tais como a utilização de VASP estrangeiros com controlos ABC/CFT fracos ou inexistentes para depósitos relacionados com o ransomware. As conclusões da NMLRA serviram de base à Estratégia Nacional de Combate ao Terrorismo e Outros Financiamentos Ilícitos dos Estados Unidos referente a 2022, que formula recomendações para fazer face aos riscos financeiros ilícitos, e ao Plano de Ação para Combater os Riscos de Financiamento Ilícito de Ativos Digitais

Fonte: Estados Unidos

Cooperação e coordenação nacionais

88. A Recomendação 2 do GAFI exige que as jurisdições disponham de mecanismos nacionais para que os decisores políticos, as UIF, as autoridades policiais e outras autoridades competentes cooperem, coordenem e troquem informações. O ransomware atravessa uma vasta gama de domínios e as investigações podem envolver intervenientes exteriores às autoridades tradicionais em matéria de ABC/CFT, incluindo as agências de cibersegurança e de proteção de dados. Mecanismos de coordenação internos eficazes são vitais para reunir informações pertinentes e peritos diferentes, incluindo do setor privado, a fim de assegurar uma resposta holística para atenuar a ameaça colocada pelo ransomware e pelo branqueamento de capitais associado. Tal permite ainda o intercâmbio crítico de informações entre as autoridades que realizam investigações forenses e investigações de financiamento paralelas.

89. Uma boa prática é a criação de equipas policiais ou de organismos multidisciplinares dedicados à cibercriminalidade (ou mesmo, especificamente, ao ransomware). Estes organismos podem coordenar as investigações de ransomware e de branqueamento de capitais com ele relacionado, que requerem uma vasta gama de conhecimentos

especializados (por exemplo, peritos das UIF ou das autoridades policiais, procuradores, engenheiros técnicos, negociadores, etc.). Esta abordagem inclui normalmente funcionários policiais com conhecimentos especializados em matéria de rastreio de ativos virtuais e pode ser uma forma útil de centralizar conhecimentos técnicos especializados, em especial face a recursos ou capacidades limitadas.

Caixa 22. Mecanismos de coordenação para centralizar informação e experiência investigatória

Para fazer face à evolução do desafio cibernético, o Governo dos EUA criou a Task Force Conjunta Nacional de Ciberinvestigação (NCIFTJ) em 2008. O NCIFTJ é composto por mais de 30 agências parceiras entre as policias, os serviços de informações e o Departamento de Defesa, com representantes que estão co-localizados e trabalham em conjunto para cumprir a missão da organização numa perspetiva de todo o governo.

Enquanto único cibercentro multiagências, o NCIFTJ é o principal responsável pela coordenação, integração e partilha de informações de suporte às investigações de ciberameaças, pelo fornecimento e apoio à análise de informações para os decisores da comunidade, bem como acrescentar valor a outros esforços em curso na luta contra a ciberameaça à nação.

No final de 2014, o NCIFTJ criou a Equipa de Moeda Virtual (VCT), que centrou os seus esforços no rastreio de operações de criptomoedas relacionadas com cibercrimes. Esta equipa fornece rastreio de criptomoedas a todos os membros do NCIFTJ. No âmbito dos seus próprios esforços de investigação, membros do NCIFTJ, como o FBI e os Serviços Secretos dos EUA (USSS), criaram as suas próprias equipas individuais para rastrear ativos virtuais, à medida que a sua utilização aumentou em vários tipos de crimes.

No início de 2022, o FBI criou a Unidade dos Ativos Virtuais (VAU), um centro nevrálgico para os programas de moeda virtual do FBI, onde a informação, a tecnologia e o suporte operacional serão canalizados para outras divisões. Na VAU, os peritos em ativos virtuais e o cruzamento de recursos de outras divisões estão implantados numa task force criada para integrar sem atropelos as informações e operações em todo o FBI.

Source: United States

Cooperação e orientação para o setor privado

90. Tal como referido na secção 5.2, a colaboração com o setor privado é útil para atenuar alguns dos desafios identificados no presente relatório. Por exemplo, as entidades reguladas podem deparar-se com dificuldades na deteção e identificação de operações suspeitas relacionadas com o ransomware. Algumas jurisdições viram sucesso na frequência e

qualidade das COS relacionadas com o ransomware através do envolvimento e da prestação de orientações às entidades comunicantes, incluindo indicadores de alerta (ver Combate ao Financiamento do Ransomware: Potenciais Indicadores de Risco, GAFI, 2023) e guias de deteção.

Caixa 23. Guias de Criminalidade Financeira da Austrália

A Fintel Alliance da Austrália publica uma série de recursos, incluindo guias de criminalidade financeira, para ajudar as empresas a compreender, identificar e comunicar atividades financeiras suspeitas, para a deteção e prevenção de atividades criminosas.

Os guias de criminalidade financeira fornecem informações pormenorizadas sobre os aspetos financeiros dos diferentes tipos de criminalidade. Incluem estudos de casos e indicadores para ajudar o setor dos serviços financeiros a identificar e detetar operações suspeitas.

Para auxiliar na luta contra o ransomware, a AUSTRAC publicou, em abril de 2022, guias de criminalidade financeira centrados na utilização abusiva de moedas digitais e na deteção e fim do ransomware. Estes dois guias fornecem informações práticas e indicadores-chave de risco para ajudar a detetar e reagir quando alguém pode ser alvo de um pagamento de ransomware ou quando alguém tenta beneficiar de um pagamento do mesmo. Ambos os guias de criminalidade financeira estão disponíveis no site da AUSTRAC:

- Deteção e fim dos pagamentos de ransomware/ AUSTRAC
- Prevenção do abuso criminoso das moedas digitais/ AUSTRAC

Fonte: Austrália

Nota: A Fintel Alliance é a parceria público-privada da Austrália que reúne peritos de uma série de organizações envolvidas na luta contra o branqueamento de capitais, o financiamento do terrorismo e outros crimes graves. Os parceiros da Fintel Alliance incluem grandes bancos, prestadores de serviços de remessas e operadores de jogo, bem como agências policiais e de segurança da Austrália e do estrangeiro.

91. A forma e o grau de colaboração com o setor privado para combater o ransomware varia consoante as jurisdições. As parcerias público-privadas (PPP) são um modelo útil e comummente compreendido, embora, em muitas jurisdições, continuem a centrar-se nos intervenientes tradicionais (em especial os bancos e outras instituições financeiras, embora exista uma participação crescente das entidades não financeiras). A composição específica variará em função das finalidades e dos objetivos da PPP, mas pode incluir intervenientes não tradicionais. No contexto da prevenção e deteção eficazes de ransomware, as PPP devem ser utilizadas para mobilizar as polícias, a CERT local, as UIF e os VASP, para além das empresas de cibersegurança, dos fornecedores de telecomunicações e das empresas de análise de blockchains (por exemplo, enquanto subgrupo ou braço operacional de uma PPP existente).

92. Os objetivos comuns dessas PPP incluem a sensibilização dos participantes para o ransomware e o branqueamento de capitais conexo, a partilha de informações sobre as tendências atuais e a exploração de ameaças novas e existentes. Estes mecanismos podem também promover relações mais fortes com o setor privado e incentivar as comunicações.

93. As jurisdições também alavancaram as PPP para alcançar vários objetivos em matéria de aplicação da lei. As PPP proporcionam uma plataforma útil para a partilha de indicadores táticos para gerar informações, permitem a partilha de informações para melhorar a deteção de mulas e redes de branqueamento em vários setores regulados, e fazem avançar as investigações.

94. Uma vez que os VASP possuem informações vitais para o êxito dos resultados das autoridades (incluindo quanto à propriedade de carteiras digitais e levantamentos em moedas fiduciárias), o desenvolvimento de relações de cooperação com este setor pode também permitir que as autoridades acedam rapidamente a informações para a deteção de ativos virtuais, bem como possam apreender e confiscar ativos de forma eficaz.

Caixa 24. O projeto GATEWAY e a operação Cyclone da Interpol

O **projeto GATEWAY** é um enquadramento para a partilha de dados com entidades privadas que teve início em 2016 para intercâmbio de informações relacionadas com a cibercriminalidade. O projeto reforça as parcerias das autoridades e do setor privado para gerar dados sobre ameaças a partir de fontes múltiplas, e para permitir que as autoridades policiais impeçam ataques. As entidades que fazem parte do projeto GATEWAY são intervenientes relevantes no ecossistema da cibercriminalidade. Estas incluem as empresas de cibersegurança, as empresas de intelligence sobre ameaças, os VASP e os bancos.

O enquadramento permite o fornecimento e a receção de informações sobre cibercriminalidade entre a INTERPOL e o setor privado e permite que o setor privado preste assistência à INTERPOL para a análise da cibercriminalidade. Os parceiros do setor privado são utilizados pelos seus conhecimentos técnicos, para ajudar a determinar o tipo de infeção por ransomware, caso seja desconhecido, bem como para analisar qualquer uma das potenciais pistas de atribuição.

A **operação Cyclone** surge na sequência de investigações policiais mundiais sobre ataques contra empresas coreanas e instituições académicas dos EUA pelo grupo de ameaças de ransomware denominado Cl0p. A operação mundial em junho de 2021 resultou em detenções de seis membros da conhecida família de ransomware e foi coordenada pela INTERPOL com as autoridades coreanas, ucranianas e americanas. Pensa-se que os suspeitos facilitaram a transferência e a troca de ativos de mais de 500 milhões de USD em nome do grupo de ransomware. A Interpol desenvolveu a operação Cyclone com a assistência de informações fornecidas pelos seus parceiros privados através do projeto Gateway da Interpol.

Fonte: INTERPOL

Nota: Para mais informação, ver: www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring

Ações propostas

- As jurisdições devem assegurar que identificam e avaliam os riscos de BC colocados pelo ransomware nas suas avaliações nacionais de risco. Dada a natureza descentralizada dos ativos virtuais e dos grupos criminosos de ransomware, tal inclui jurisdições com setores de ativos virtuais em que o ransomware não é atualmente uma ameaça interna. Essas conclusões podem ainda ajudar a sustentar as ciberestratégias nacionais através de uma visão global nacional dos riscos associados ao ransomware.
- As jurisdições devem desenvolver mecanismos de coordenação entre as autoridades competentes relevantes, desde as autoridades policiais, ABC/CFT e de cibercrime até parceiros não tradicionais, como as agências de cibersegurança ou de proteção de dados. Tal promove a partilha de dados e informações e proporciona uma plataforma útil para a partilha cruzada de várias técnicas especializadas.
- As jurisdições devem identificar e estabelecer mecanismos de apoio à cooperação público-privada. As jurisdições devem ponderar a inclusão dos VASP e de outros parceiros não tradicionais nesses mecanismos de cooperação.

Cooperação internacional

95. Os ataques de ransomware e os fluxos financeiros conexos são frequentemente transnacionais e multinacionais. Os criminosos de ransomware estão geralmente estabelecidos numa jurisdição diferente das múltiplas jurisdições através das quais os fundos (em especial os ativos virtuais) são branqueados e, por fim, levantados. A complexidade e os desafios dos esquemas de BC relacionados com o ransomware exigem uma cooperação transfronteiriça contínua entre as autoridades a nível de informações, ferramentas e conhecimentos especializados pertinentes. A criação e a mobilização dos mecanismos existentes para a cooperação internacional são indispensáveis para o êxito das investigações financeiras e da recuperação de ativos, em especial no caso do ransomware.

Caixa 25. Investigação internacional conjunta contra o tipo "LockerGoga"

Em janeiro de 2019, ocorreu um ataque de ransomware contra uma grande empresa francesa. O malware LockerGoga foi identificado como o tipo de ransomware utilizado para encriptar vários ficheiros e servidores internos da empresa. Embora tenha sido solicitado um resgate de 410 Bitcoins após a negociação, a empresa não pagou o resgate. No entanto, verificou-se que o tipo LockerGoga foi também utilizado por piratas informáticos em numerosos outros ataques.

Foi constituída uma equipa de investigação conjunta sob a égide da Eurojust/Europol, juntamente com várias jurisdições europeias. Tal resultou numa partilha eficiente de informações, incluindo a cooperação jurídica através de Decisões Europeias de Investigação (DEI) e do Tratado de Acordo Judiciário Mútuo (MLAT), que ajudou a acelerar as investigações. A Europol/Eurojust também prestou apoio técnico com uma grande capacidade de hardware e financiamento. Posteriormente, foi identificada uma infraestrutura criminosa de comando e controlo, com fluxos de mensagens dos piratas informáticos a serem descodificados, tendo o grupo sido finalmente localizado numa jurisdição do Leste. Tal permitiu a realização de várias detenções na referida jurisdição.

As investigações estão em curso. Através da análise de blockchains, os investigadores descobriram as várias técnicas de peel chains utilizadas. Tal resultou na detenção de um dos principais autores de branqueamento de capitais na Suíça. Várias outras mulas foram igualmente detidas em diferentes jurisdições. As investigações revelaram ainda que os resgates pagos não eram exclusivamente para o hacker/ pirata informático. Por exemplo, tiveram de ser efetuados pagamentos ilícitos a vários parceiros criminosos, pagamentos esses que foram também utilizados para infraestruturas (engenheiros e criadores de software, servidores seguros, serviços de VPNs para ocultar comunicações ou ligações aos servidores de comando e controlo, serviços de BC para organizar movimentos de peel chains, etc.), bem como para encontrarem mulas e locais para levantamento dos valores.

Fonte: França

96. As informações solicitadas nos pedidos internacionais dizem normalmente respeito a elementos de prova forenses necessários às investigações, e dados financeiros necessários para as investigações de BC. Tal inclui endereços IP localizados no estrangeiro, nomes e pseudónimos utilizados, informações sobre subscritores, bem como informações sobre os beneficiários efetivos, dados da transação e informação de congéneres relativas a carteiras alojadas por VASP estrangeiros.

Desafios específicos colocados pela utilização de ativos virtuais

97. O envolvimento de ativos virtuais no branqueamento relacionado com o ransomware pode criar novas dificuldades na cooperação transfronteiriça. As diferenças no tratamento substantivo ou na regulação dos ativos virtuais nos vários sistemas jurídicos — e a limitada ou total falta de participação governamental ou de supervisão do setor em algumas jurisdições — podem complicar a capacidade ou a vontade das autoridades de participarem na cooperação internacional.

98. Por exemplo, as jurisdições que não registam ou não supervisionam os VASP podem ter dificuldade em identificar as empresas a quem solicitar informações. Mesmo que a entidade adequada esteja localizada, as autoridades podem só ter acesso a técnicas de investigação coercivas para executar um pedido de cooperação internacional. Tal pode limitar as informações que podem ser obtidas através de processos de cooperação informal.

99. Este desafio é agravado pela realidade de que muitas jurisdições onde estão localizados os criminosos de ransomware e respetivas mulas de dinheiro, ou onde os VASP costumavam branquear e levantar os proventos, estão sediados ou donde operam, são tolerantes com esta atividade e podem não responder a pedidos estrangeiros das autoridades policiais. Se os VASP estiverem em jurisdições sem obrigações em matéria de ABC/CFT, podem simplesmente não dispor dos registos relevantes para as autoridades policiais. Esta situação acaba por frustrar as investigações financeiras em curso e as tentativas de recuperação de ativos. Estes desafios reforçam mais uma vez a importância de acelerar a aplicação a nível mundial da Recomendação 15 do GAFI (incluindo a "Travel Rule").

Caixa 26. Desafios de investigação decorrentes de VASP estrangeiro não cooperante

A empresa X foi vítima de um ataque com ransomware, que se crê ser o tipo Caley ransomware. Após a negociação, a vítima pagou 0.25 bitcoin ao criminoso de ransomware e recebeu uma mensagem de correio eletrónico com a chave de decifragem, permitindo que as operações da vítima regressassem à normalidade após a decifragem.

As autoridades foram informadas tardiamente do caso através de uma comunicação à polícia apresentada pela vítima vários dias após o pagamento do resgate, o que levou a que o rastreamento para o pagamento se dissipasse. Com base na análise de blockchains, o rasto do pagamento dos resgates foi encaminhado para um VASP situado no estrangeiro, tendo sido observado que um saldo de 0.0081 Bitcoin foi colocado numa carteira virtual alojada pelo VASP estrangeiro, o qual tem permanecido reticente apesar dos múltiplos pedidos de informação. As investigações foram ainda dificultadas pela utilização de um mixer por parte do autor da infração para ocultar operações. Com base nas circunstâncias do caso em apreço, o autor do crime continua a ser desconhecido e não foi possível proceder à recuperação ou detenção de bens.

Fonte: Singapura

100. As arquiteturas distribuídas de alguns VASP (com operações que abrangem várias jurisdições) podem também representar um encargo de investigação significativo para as autoridades policiais, a fim de identificar a entidade adequada a abordar para pedidos de informação, ou a jurisdição adequada a quem enviar um pedido de assistência. Por exemplo, uma jurisdição citou dificuldades na identificação da jurisdição relevante para solicitar assistência com base num IBAN que, presumivelmente, pertence a uma conta bancária gerida por um VASP numa instituição financeira estrangeira. Outra jurisdição observou que alguns VASP parecem não ter presença física, o que pode dificultar a identificação das jurisdições corretas com as quais coopera.

A necessidade de uma cooperação rápida

101. Uma vez que os criminosos de ransomware podem estar amplamente espalhados por todo o mundo e que os ativos virtuais podem ser transferidos quase instantaneamente, as autoridades têm de agir rapidamente para detetar e prevenir a dissipação transfronteiriça das receitas relacionadas com o ransomware. Para o efeito, são normalmente necessários mecanismos formais de cooperação internacional (como o auxílio judiciário mútuo) para obter provas e obter apreensões no contexto de processos. No entanto, esses mecanismos formais de cooperação nem sempre são rápidos, o que pode atrasar ou mesmo dificultar significativamente as investigações. A complexidade das investigações relacionadas com o ransomware, em termos do número de jurisdições e empresas envolvidas, agrava estes desafios, uma vez que a cooperação internacional para o ransomware demora mais tempo e consome mais recursos do que outras atividades criminosas.

102. A alavancagem da cooperação informal pode ser útil para superar estes desafios e pode ajudar a racionalizar e a acelerar os pedidos de auxílio judiciário mútuo. Para facilitar a cooperação atempada, algumas jurisdições salientaram a importância dos contactos existentes e estabeleceram canais informais para contactar e dialogar com homólogos estrangeiros. Tal ajuda a facilitar o rápido intercâmbio de informações necessário para fazer avançar os casos, respeitando simultaneamente os processos necessários para proteger essas informações. Esse intercâmbio informal de informações pode ocorrer entre as UIF através do Egmont Secure Web, ao passo que a cooperação policial pode ocorrer através do I-24/7 da Interpol, bem como de outras redes informais, incluindo a Rede Interagências de Recuperação de Ativos Camden (CARIN) e as Redes Regionais de Recuperação de Bens (ARIN). As autoridades devem ter estabelecido processos e pontos de contacto disponíveis para os canais de cooperação internacional e regional, como suporte à deteção rápida de fundos e a recuperação eficaz de ativos.

103. Algumas jurisdições tiveram êxito na cooperação através do estabelecimento de relações bilaterais. A utilização de oficiais de ligação dedicados à cibercriminalidade e destacados a nível internacional pode facilitar significativamente a partilha de informações entre a jurisdição de acolhimento e a jurisdição de origem, bem como permitir que as autoridades recolham e forneçam provas do estrangeiro em investigações relacionadas com ransomware. A fim de promover a cooperação bilateral, as autoridades devem considerar a

possibilidade de divulgar os processos e os pontos de contacto para a cooperação, em especial como suporte ao rápido rastreio de fundos e recuperação de ativos.

Caixa 27. Projeto CODA

Um cibercriminoso canadiano ligado a campanhas de ransomware e ao comprometimento de departamentos governamentais e instalações médicas do governo do Alasca, foi detido em novembro de 2021, e acusado de várias infrações relacionadas com cibercrimes. Antes de contactar parceiros internacionais, o FBI investigou várias ciberintrusões criminosas conexas. Uma vez identificado e localizado o indivíduo, o FBI estabeleceu contactos bilaterais com a Polícia Provincial do Ontário (OPP).

Foram iniciadas investigações paralelas em ambas as jurisdições, com o apoio ao OPP e FBI, prestado pelo Centro Nacional de Coordenação da Cibercriminalidade do Canadá (NC3), pela Europol e pelas autoridades policiais neerlandesas. O NC3 prestou apoio operacional, análises de dados e comportamentais, informações e relatórios, serviços de rastreio de criptomoedas e análise ao longo de 23 meses, no âmbito da investigação internacional. Estes esforços contribuíram para confirmar a identificação da pessoa de interesse que conduziu à sua posterior detenção. A utilização de técnicas analíticas avançadas e de ferramentas especializadas, como o rastreio de criptomoedas, é fundamental neste tipo de investigações sobre cibercrime.

Fonte: Canadá e Estados Unidos

A importância da coordenação multilateral

104. Os estudos de casos com medidas coercivas bem-sucedidas envolvem normalmente as autoridades competentes de várias jurisdições. Tal reflete a natureza internacional e descentralizada dos ataques de ransomware e do BC associado. Um dos principais fatores de sucesso é a necessidade de coordenação internacional entre as jurisdições afetadas para, simultaneamente, desenraizar e desmantelar os cibergrupos e suas filiais. Tal também atenua os riscos de deslocalização, nos casos em que estas organizações criminosas podem facilmente transferir as suas operações digitais para outro porto seguro.

105. Existem vários mecanismos internacionais de coordenação policial que podem ser utilizados para este efeito, como a Europol/Eurojust ou a Interpol. Estas organizações acolhem bases de dados e fornecem logística e conhecimentos especializados para coordenar as partes interessadas de várias jurisdições. Esses mecanismos multilaterais podem ser úteis, especialmente para acelerar a partilha de informações críticas para as investigações financeiras e a recuperação de ativos.

Caixa 28. Operação GoldDust [1]

Em novembro de 2021, as autoridades romenas detiveram duas pessoas suspeitas de ciberataques com recurso ao ransomware Sodinokibi/REvil. Alegadamente, são responsáveis por 5 000 infeções, que, no total, deram origem a pagamentos de resgates de meio milhão de euros. Desde fevereiro de 2021, as autoridades também detiveram três outros afiliados de Sodinokibi/REvil e dois suspeitos ligados a GandCrab. Estes são alguns dos resultados da operação GoldDust, que envolveu 17 jurisdições[2], Europol, Eurojust e INTERPOL. Todas as detenções seguiram-se aos esforços internacionais conjuntos de identificação, escutas telefónicas e apreensão de algumas das infraestruturas utilizadas pela família de ransomware Sodinokibi/REvil, que é considerada a sucessora da GandCrab.

A operação GoldDust foi desenvolvida a partir de elementos relacionados com investigações anteriores que visavam a GandCrab, uma investigação conduzida pela Roménia com o apoio da Europol e das autoridades de várias jurisdições, incluindo o Reino Unido e os Estados Unidos.

A Europol facilitou o intercâmbio de informações, apoiou a coordenação da operação GoldDust e prestou apoio analítico operacional, bem como criptomoedas, malware e análises forenses. A Europol também destacou peritos para cada local e ativou um posto de comando virtual para coordenar as atividades no terreno. A cooperação internacional permitiu à Europol simplificar os esforços de mitigação das vítimas com outras jurisdições da UE. Estas atividades impediram as empresas privadas de serem vítimas de ransomware de Sodinokibi/REvil.

A Task Force Conjunta contra o Cibercrime (J-CAT) da Europol apoiou a operação. Esta equipa operacional permanente é composta por oficiais de ligação de diferentes jurisdições que trabalham a partir do mesmo gabinete em investigações de grande dimensão sobre cibercrime.

Fonte: Europol

Notas

1. 1. Para mais informação, consultar: www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
2. Jurisdições participantes: Austrália, Bélgica, Canadá, França, Alemanha, Países Baixos, Luxemburgo, Noruega, Filipinas, Polónia, Roménia, Coreia do Sul, Suécia, Suíça, Koweit, Reino Unido e Estados Unidos.

Ações propostas

- As jurisdições devem estabelecer e participar ativamente em mecanismos bilaterais, regionais e multilaterais, nomeadamente através da utilização de gabinetes de ligação e da criação de pontos de contacto claros 24 sobre 24 horas, a fim de facilitar a rápida cooperação internacional e o intercâmbio de informações.

Conclusão

106. Apesar do recente crescimento dos fluxos financeiros mundiais de ransomware, continua a verificar-se uma falta de investigações sobre o BC conexos. Este estudo demonstrou que o ransomware é um problema multidisciplinar e internacional. Tal requer uma abordagem coordenada para uma resposta eficaz contra esta ameaça. Para se conseguir tal objetivo, as jurisdições devem alavancar parcerias a três níveis: público-público; público-privado; e com jurisdições estrangeiras e organizações multilaterais.

107. Este estudo ilustra ainda a importância de uma implementação acelerada dos padrões do GAFI para se obter um quadro eficaz de combate aos proventos ilícitos provenientes de ransomware, em especial no que diz respeito aos ativos virtuais e ao setor VASP. O GAFI continuará a promover a aplicação dos padrões do GAFI neste setor.

108. Por último, o papel dos ativos virtuais no branqueamento dos produtos do ransomware, bem como a evolução das técnicas utilizadas pelos grupos criminosos de ransomware, colocam ainda mais desafios. As autoridades competentes devem assegurar que a sua legislação continua a ser pertinente e está equipada com as competências e capacidades necessárias para ser célere face a um ambiente criminoso digital dinâmico.

www.fatf-gafi.org

Março 2023

Combate ao financiamento do Ransomware: Indicadores Potenciais de Risco

Estes indicadores potenciais de risco visam auxiliar as entidades do setor público e privado a identificar atividades suspeitas relacionadas com o ransomware. Estes indicadores com3plementam o relatório do GAFI "*Combate ao Financiamento de Ransomware*", que analisa os métodos utilizados pelos criminosos para realizar os ataques de ransomware e a forma como os pagamentos são feitos e branqueados.