RELATÓRIO DO GAFI

COMBATE AO FINANCIAMENTO DE RANSOMWARE

INDICADORES POTENCIAIS DE RISCO

Março 2023

COMBATE AO FINANCIAMENTO DE RANSOMWARE: INDICADORES POTENCIAIS DE RISCO

Os seguintes indicadores potenciais de risco baseiam-se na experiência e nos dados recebidos das jurisdições em toda a rede global. Estes indicadores visam melhorar a deteção de transações suspeitas relacionadas com *ransomware.* A lista varia de acordo com as diferentes perspetivas que vão ocorrendo ao longo do processo de pagamento do resgate.

Antes de utilizar os indicadores de risco, os leitores são incentivados a ler a nota infra e o relatório de 2023 do GAFI sobre a luta contra o financiamento de ransomware.

Combate ao Financiamento de Ransomware

Este relatório analisa os métodos utilizados pelos criminosos para levar a cabo os seus ataques com ransomware e a forma como procedem ao branqueamento dos resgates.

O relatório salienta que as autoridades devem tirar partido dos mecanismos de cooperação internacional existentes e tirar partido dos mesmos para combater com êxito o branqueamento do pagamento de resgates. Devem também desenvolver as competências e os instrumentos necessários para recolher rapidamente informações essenciais, rastrear transações virtuais quase instantâneas e recuperar ativos virtuais antes de se dissiparem.

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

A existência de um único indicador em relação a um cliente ou transação pode não justificar, por si só, a suspeita de uma infração de ransomware, nem um indicador único poderá necessariamente fornecer uma indicação clara dessa atividade. No entanto, poderá exigir um acompanhamento e uma análise mais aprofundados, se necessário.

A lista de indicadores complementa os Indicadores de Alerta sobre Ativos Virtuais do GAFI[1], e a mesma é relevante tanto para o setor público como para o setor privado. Relativamente a estes últimos, os indicadores podem ser relevantes para os VASP, os bancos e outras instituições financeiras e de pagamento.

Bancos/Outras instituições financeiras e de pagamento que identifiquem pagamento de ransomware por parte de uma vítima

- Transferências eletrónicas para empresas de consultoria em cibersegurança ou de resposta a incidentes especializadas na reparação de ransomware
- Transferências eletrónicas invulgares provenientes de companhias de seguros especializadas na reparação de ransomware
- Comunicação pelo próprio cliente de um ataque ou pagamento de resgate de ransomware
- Informações de fonte aberta sobre ataques de ransomware a clientes
- Elevado volume de operações da mesma conta bancária para várias contas num VASP
- A descrição do pagamento contém palavras como «resgate» ou nomes de grupos de ransomware
- Pagamentos efetuados a VASP em jurisdições de alto risco (ver caixa)

VASP que identificam o pagamento de ransomware por parte da vítima

- Pedido de aquisição de ativos virtuais por uma empresa de resposta a incidentes ou uma companhia de seguros em nome de um terceiro.
- O cliente declara ao VASP que está a comprar ativos virtuais para pagamento de ransomware.
- Utilizador que, sem historial de transações de ativos virtuais, envia fundos fora da prática comercial normal
- Um cliente que aumenta o limite de uma conta e envia a um terceiro
- Um cliente parece ansioso ou impaciente com o tempo necessário para um pagamento
- Compras ou transferências de criptomoedas que promovem o anonimato
- Pagamentos efetuados a VASP em jurisdições de alto risco
- Um novo cliente adquire ativos virtuais e transmite a totalidade do saldo da sua conta para um único endereço

VASP que identificam o recebimento de pagamentos/contas de ransomware criminosas

- Um cliente que, após uma grande transferência inicial de ativos virtuais, tem pouca ou nenhuma atividade em moeda digital

[1] Ver "FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorism Financing" (setembro 2020), disponível em: www.fatfgafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-FlagIndicators.pdf

- A análise de blockchains nos endereços das carteiras revela ligações a ransomware
- Levantamento imediato após a conversão de fundos em ativos virtuais
- Envio de ativos virtuais para carteiras ligadas a ransomware
- Utilização de um VASP numa jurisdição de alto risco
- Transferência de ativos virtuais para um serviço de mixing
- Utilização de redes encriptadas
- A informação de verificação é uma fotografia de dados num ecrã de computador, ou tem um nome de ficheiro que contém "imagem do WhatsApp"ou semelhante
- A sintaxe do cliente não corresponde à demografia do cliente
- A informação sobre o cliente mostra que o mesmo tem uma conta de correio eletrónico conhecida pela privacidade elevada, como o correio proton ou Tutanota
- Dados de identificação incoerentes ou tentativa de criar uma conta com uma identidade falsa
- Contas múltiplas associadas aos mesmos dados de contacto; endereços partilhados sob diferentes nomes
- O cliente parece utilizar uma VPN
- Transações que envolvem criptomoedas que promovem o anonimato.

Caixa: 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 profundamente 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 neles operam; (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 sistemas de governação, de aplicação da lei e de supervisão deficientes, incluindo os países identificados pelas declarações do GAFI como tendo regimes ABC/CFT fracos, especialmente no que toca aos VASP, e nos países em relação aos quais os VASP e outras entidades obrigadas devem prestar especial atenção em termos de relações de negócio e transações.

Fonte: "FATF (2021) Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs", par. 154

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 complementam 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.