BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

ABRIL 2022 | nº 1/2022

DESTAQUES

Agentes de ameaça

Um dos fatores mais importantes de um incidente de cibersegurança é a ação de um agente de ameaça, isto é, uma intervenção humana individual ou em grupo que procura comprometer pelo menos um dos princípios da segurança da informação de uma potencial vítima: a confidencialidade, a integridade e/ou a disponibilidade da informação.

Imputação

Um dos problemas mais difíceis de ultrapassar no campo da cibersegurança é a dificuldade de imputar um incidente de cibersegurança a um agente de ameaça. Esta dificuldade resulta de diversas razões: a ausência de fronteiras no ciberespaço; a capacidade de anonimização que a Internet permite; o recurso a portos de abrigo em outras jurisdições; e as técnicas usadas para se adicionar uma camada acrescida de camuflagem às ações maliciosas.

Tipologia

A dificuldade de imputação não significa impossibilidade de imputação. Uma das soluções passa por utilizar modelos que identificam táticas, técnicas e procedimentos típicos em certos agentes, possibilitando associá-los a incidentes. Esta metodologia permite tipificar os agentes de ameaça (e.g., estarem associados a Estados ou não, organizarem-se segundo lógicas de espionagem ou de criminalidade, terem objetivos geopolíticos ou de monetarização).

VISUALIZAÇÃO

Dados do Observatório de Cibersegurança do CNCS identificaram como tipos de agentes de ameaça mais relevantes a atuar no ciberespaço de interesse nacional, durante 2019 e 2020, os Cibercriminosos, os Agentes Estatais, os Hacktivistas, os Cyber-offenders e os Insiders negligentes (ver Riscos & Conflitos 2020 e 2021).

Entre estes, os Cibercriminosos e os Agentes Estatais destacaram-se pela frequência e potencial de impacto. Os Hacktivistas caracterizaram-se por apresentar uma dinâmica de atividade de intensidade variável, de acordo com o surgimento de novos grupos.

Agentes de ameaça predominantes em Portugal em 2019 e 2020

Agentes de ameaça	Motivos				
	Económicos	Geopolíticos	Ideológicos	Pessoais	Sem motivo
Cibercriminosos	■	■			
Agentes Estatais	■	■			
Hacktivistas			■	■	
Cyber-offenders	■			■	
Insiders negligentes					■

Legenda: ■ Motivos predominantes ■ Outros motivos secundários

(adaptado de Riscos & Conflitos 2020 e 2021)

Os Cibercriminosos são indivíduos ou grupos que procuram ganhos económicos, ainda que possam ser financiados por Estados. Os Agentes Estatais são aqueles que mais se regem por motivos geopolíticos, ainda que por vezes também económicos. Os Hacktivistas tendem a ser motivados pela afirmação de uma mensagem ideológica, por vezes na fronteira com os motivos pessoais ligados à reputação. Os Cyber-offenders são aqueles que atuam para agredir uma vítima ou criar disrupção nos sistemas segundo motivos pessoais. Os Insiders negligentes (e não os voluntários ou comprometidos) são utilizadores que, involuntariamente, comprometem a sua organização mediante uma ação descuidada, portanto, sem um motivo consciente.

PERSPETIVA

1 Os agentes de ameaça podem ser categorizados numa tipologia com base em diferentes critérios não redutíveis apenas ao motivo (como no quadro anterior). Por exemplo, ataques que exigem muitos recursos tendem a ser atribuídos a Agentes Estatais; ataques dirigidos a cidadãos em geral tendem a ser os aplicados por Cibercriminosos e Cyber-offenders; ou ataques realizados por Hacktivistas tendem a ter níveis de especialização baixos ou médios (ver Bruijne, 2017).

2 Além desta matriz que cruza diferentes características sociais dos agentes de ameaça, são desenvolvidas metodologias de identificação dos seus modos de atuação do ponto de vista técnico, relativamente a vetores de ataque tipicamente utilizados, que permitem a associação mais fina entre determinados incidentes e certos grupos específicos. Esta metodologia é aplicada principalmente a Agentes Estatais e a Cibercriminosos organizados (ver MITRE).

3 Alguns destes agentes dizem respeito às chamadas "Ameaças Persistentes Avançadas", as quais correspondem a grupos, com alguma sofisticação de meios e de recursos, que procuram realizar intrusões em sistemas de organizações com o objetivo de realizar exfiltrações de informação crítica ou sabotagem de infraestruturas. Estas ações são realizadas de modo constante, com uma temporalidade longa e com grande capacidade de ocultação.

4 Estes métodos de imputação mantêm um certo nível de abstração enquanto processos de responsabilização, isto é, a identificação de pessoas ou organizações concretas como responsáveis pelos ataques nem sempre ocorre com níveis de precisão e prova material que permitam conclusões indubitáveis. Todavia, conseguem, no campo da troca de informações para fins geopolíticos, de defesa e por vezes judiciais, realizar aproximações que resultam em maiores certezas.

5 A capacidade de anonimização que a Internet permite é por vezes intensificada por operações de falsa bandeira realizadas por alguns agentes de ameaça. Quando aplicadas, estas operações procuram confundir as análises forenses quanto à real origem dos ataques no ciberespaço. Por exemplo, criando um grupo falso de Cibercriminosos que reivindicam o incidente, deixando uma assinatura técnica típica de outro agente ou pagando a outro grupo para realizar o ataque.

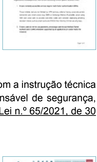
6 Este tipo de operação permite desenvolver ações típicas de ameaças híbridas, com efeitos não só em sistemas e informações com impacto social, como também na perceção das populações. A dificuldade de identificação da origem facilita a simulação de muitas origens possíveis. O facto de o ciberespaço não ter uma delimitação territorial com fronteiras claras propicia este jogo de sombras que procura modelar a opinião pública e promove a análise especulativa.

PUBLICAÇÕES E NOTÍCIAS

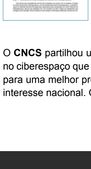
O **World Economic Forum (WEF)** publicou, no dia 11 de janeiro, o *Global Risks Report 2022*. A perceção de risco de falha de cibersegurança é o 7º risco em 10 quando se consideram os riscos mais críticos nos próximos 2 anos, passando para o 8º quando se perspetivam os próximos 2 a 5 anos e deixando de surgir entre os 10 primeiros quando a perspetiva são os próximos 5 a 10 anos. Em qualquer dos casos, o risco considerado mais crítico é o ambiental.

O **WEF** publicou, no dia 18 de janeiro, o *Global Cybersecurity Outlook 2022*, o primeiro de uma série anual. O documento apresenta os resultados de um inquérito internacional a 120 líderes da "comunidade ciber". Uma das conclusões é que 81% dos respondentes pensa que a transformação digital é uma oportunidade para melhorar a ciber-resiliência e 87% dos executivos projeta reforçar as políticas e *standards* de cibersegurança na relação com terceiros.

O **Gabinete Cibercrime** da Procuradoria-Geral da República publicou, no dia 25 de janeiro, a nota informativa *Cibercrime: denúncias recebidas em 2021*, documento que analisa as denúncias de cibercrimes a este organismo em 2021. Durante o ano passado foram realizadas 1160 denúncias, mais do dobro do que em 2020, ano durante o qual se registaram 544. O *phishing* e as burlas *online* encabeçam as causas mais frequentes.



A **ENISA – Agência Europeia para a Cibersegurança**, juntamente com o **CERT.EU** (equipa de resposta a incidentes de cibersegurança das instituições da União Europeia), divulgou, no dia 14 de fevereiro, a publicação conjunta *Boosting your Organisation's Cyber Resilience*, através da qual divulga algumas recomendações essenciais dirigidas a organizações públicas e privadas, em resposta ao aumento do nível de ameaça ao ciberespaço comunitário.



Foi publicado, em **Diário da República**, o Regulamento n.º 183/2022, de 21 de fevereiro, com a instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidente, complementando o Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço.

O **CNCS** partilhou uma análise relativa ao Contexto Atual, através da qual se destaca um conjunto de ameaças no ciberespaço que marcam a atualidade, bem como as ações de mitigação que são consideradas fundamentais para uma melhor proteção e reação das organizações e das pessoas a eventuais incidentes no ciberespaço de interesse nacional. O CNCS recomenda a leitura atenta deste documento e a aplicação das recomendações.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança