BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

JULHO 2022 | nº 2/2022

DESTAQUES

Cibercrime-como-serviço

O campo de atuação do cibercrime não se reduz a ações diretas sobre potenciais vítimas por parte de cibercriminosos que desenvolvam instrumentos técnicos maliciosos, mas é também constituído por um mercado de produtos e serviços que estes mesmos cibercriminosos vendem a outros cibercriminosos com menos competências técnicas ou que não investem em desenvolvimento. A esta atividade chama-se "cibercrime-como-serviço".

Problema

O cibercrime-como-serviço provoca várias dificuldades ao combate ao cibercrime e à investigação criminal: facilita a entrada na cibercriminalidade de atores que não têm competências técnicas (e.g., *script kiddies*), democratizando o cibercrime; dificulta a captura de toda a cadeia de cibercriminalidade, na medida em que o vendedor/prestador do serviço deixa menos pegada; e propicia uma maior massificação do número de incidentes de cibersegurança.

Resposta

Uma das formas de responder a esta realidade é através da promoção de um combate ao cibercrime que não incida apenas sobre o cibercriminoso que é diretamente responsável pela ação ilegal, mas também atuando, de forma estratégica, sobre as plataformas e fóruns *online* que servem de mercado para este tipo de produtos e serviços. A capacidade para desmantelar estes mercados é chave para a produção de efeitos mais abrangentes.

PANORÂMICA

Os tipos de produtos e serviços mais relevantes comercializados nos mercados típicos do cibercrime-como-serviço, de acordo com relatórios da ENISA e da Europol, são:

- *Access-as-a-Service*: serviço de intrusão prestado em geral por organizações, com frequência a Estados, mas também a empresas e indivíduos, com o fim de aceder a sistemas alheios e recolher informação sensível;
- *DDoS-For-Hire-Services*: ações contratadas de negação de serviço distribuída, dirigidas a alvos específicos, muitas vezes usando infraestrutura IoT e realizando um pedido de resgate;
- *Disinformation-as-a-Service*: campanhas de desinformação para manipular a opinião pública disponibilizadas sobretudo a governos, partidos políticos e empresas de relações públicas;
- *Phishing-as-a-Service*: ataques de *phishing* vendidos por um operador que desenvolve uma campanha completa, podendo incluir, por exemplo, uma página falsa para realização de credenciação, alojamento de *website* e análise e redistribuição de credenciais;
- *Ransomware-as-a-Service*: venda de serviços de *ransomware*, frequentemente através de uma plataforma que fornece os instrumentos para a realização da cifragem e para a receção do resgate, ficando o provedor da plataforma com uma parte do valor extorquido. O comprador do serviço fica responsável pela interação com a vítima.

Cibercrimes-como-serviço mais notabilizados (ENISA e Europol)	Taxonomia do CERT.PT/RNCSIRT
Access-as-a-Service	Intrusão
DDoS-For-Hire-Services	Disponibilidade
Disinformation-as-a-Service	N/A
Phishing-as-a-Service	Fraude
Ransomware-as-a-Service	Segurança da Informação

ENISA, Europol e CERT.PT

PERSPETIVA

1 Verifica-se uma importância crescente do cibercrime-como-serviço e de agentes de ameaça, os *Hackers-for-Hire*, que alimentam uma segunda esfera, eventualmente menos especializada, de outros agentes de ameaça que atuam no ciberespaço. Segundo a ENISA, os *Hackers-for-Hire* tornaram-se um dos principais agentes de ameaça em 2021 e tendem a especializar-se em *Access-as-a-Service* e em práticas da família da espionagem.

2 Algumas das organizações que prestam serviços de *Access-as-a-Service* exploram as ambiguidades legais nestas matérias nos seus países de origem e as que resultam da falta de delimitação territorial do ciberespaço. Desta forma, atuam como negócios legítimos e protegidos como tal. É particularmente difícil prever as ações destes agentes de ameaça na medida em que os seus objetivos dependem dos serviços contratados e das necessidades dos seus clientes (ENISA).

3 O restante cibercrime-como-serviço disponibiliza os seus préstimos em mercados do submundo da criminalidade *online* ou em *websites* e fóruns construídos propositadamente para a apresentação das suas ofertas. Assim que um interessado nestes serviços encontra aquilo que procura, geralmente a restante interação é realizada através de plataformas de mensagens como o Telegram, o Discord, o Skype, o Jabber ou o IRC (Akyazi *et. al.* 2021).

4 Os serviços prestados no domínio do cibercrime-como-serviço podem responder a diferentes necessidades ao longo da cadeia de valor da cibercriminalidade, nomeadamente no âmbito das atividades primárias (e.g., descoberta de vulnerabilidades, desenvolvimento e entrega de exploração de alvo, ou ataque), mas também das atividades secundárias (e.g., formação e recrutamento, comercialização, reputação ou lavagem de dinheiro) (Huang *et. al.* 2017).

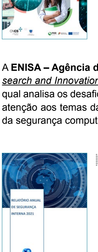
5 A título de exemplo, no caso do *Access-as-a-Service*, o desenvolvimento de soluções que exploram vulnerabilidades no sentido de realizar intrusões em sistemas de potenciais vítimas correspondem a atividades primárias. Uma vez que este tipo de serviço é prestado frequentemente por empresas, é acompanhado por atividades secundárias como a comercialização dos serviços junto de potenciais clientes usando métodos tradicionais de venda.

6 Uma componente "empresarial" das organizações ligadas ao cibercrime verifica-se também em entidades cujo caráter ilegal é mais evidente. Alguns grupos cibercriminosos que atuam em mercados alternativos e de visibilidade restrita na Internet são organizados como se de autênticas empresas se tratassem, apresentando uma divisão do trabalho típica de um negócio moderno (e.g., desenvolvimento, gestão, atendimento ao "cliente", "vendas", etc.).

PUBLICAÇÕES E NOTÍCIAS

A **ENISA – Agência da União Europeia para a Cibersegurança** divulgou, no dia 13 de abril, o relatório *Coordinated Vulnerability Disclosure Policies in the EU*, em que apresenta uma panorâmica sobre as políticas de divulgação coordenada de vulnerabilidades nos países da União Europeia (UE). Este estudo mostra que os países da UE estão em etapas distintas nesta matéria, mas que alguns se encontram bastante avançados na implementação deste tipo de políticas.

O **CNCS** publicou, no dia 18 de abril, o *Referencial de Competências em Cibersegurança*. Ao longo dos últimos meses, divulgou ainda dois documentos para consulta pública: no dia 13 de maio, o *Projeto de Guia para Gestão de Riscos*, que esteve disponível para contributos até dia 14 de junho; e no dia 9 de junho, a nova versão do *Esquema de Certificação para o Quadro Nacional de Referência para a Cibersegurança*, que esteve disponível para contributos até dia 8 de julho.



O **Observatório de Cibersegurança do CNCS** publicou vários documentos recentemente: no dia 28 de abril, o *Estudo Sobre o Ensino Pós-Secundário e o Ensino Superior de Cibersegurança em Portugal*; no dia 23 junho, o *Relatório Cibersegurança em Portugal, tema Riscos e Conflitos 2022*; e, no dia 5 de julho, o *Relatório Cibersegurança em Portugal, tema Economia 2022.*

A **ENISA – Agência da União Europeia para a Cibersegurança** publicou, no dia 12 de maio, o documento *Research and Innovation Brief - Annual Report on Cybersecurity Research and Innovation Needs and Priorities*, no qual analisa os desafios colocados à cibersegurança nos domínios da investigação e da inovação, com particular atenção aos temas da hiperconectividade, dos sistemas inteligentes, da cibersegurança nas ciências da vida e da segurança computacional.

O **Sistema de Segurança Interna (SSI)** publicou, no dia 25 de maio, o *Relatório Anual de Segurança Interna 2021*. Relativamente à "criminalidade informática", este documento mostra que, segundo a Polícia Judiciária, durante 2021 foram constituídos 743 arguidos, verificaram-se 88 detenções e 11 indivíduos foram colocados em prisão preventiva.

A **Equipa da Europa**, no dia 17 de junho, venceu o primeiro *International Cybersecurity Challenge*. Em segundo lugar posicionou-se a Equipa da Ásia e em terceiro a Equipa dos EUA. A Equipa da Europa venceu sobretudo nos desafios do tipo *Jeopardy* e a Equipa da Ásia nos do âmbito *Attack & Defence*. O evento decorreu em Atenas, Grécia. Na Equipa da Europa participaram os portugueses Nuno Sabino como capitão e Pedro Adão como treinador.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança