BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

DEZEMBRO 2021 | nº 5/2021

DESTAQUES

Palavra-passe

A palavra-passe é um dos instrumentos de segurança mais críticos para a cibersegurança, na medida em que é a última barreira de segurança para aceder a plataformas nas quais são guardados dados pessoais e/ou sensíveis. Contudo, é também uma das funcionalidades de segurança mais frágeis, visto o seu nível de segurança depender muito da forma como é utilizada, ficando muito suscetível às dinâmicas do fator humano e às tendências do cibercrime.

Fragilidade

Desde a sua primeira utilização na informática nos anos 1960 que a palavra-passe é tida como frágil. Existem pelo menos 4 modos de a descobrir: por mecanismos que, por tentativa-erro, ensaiam as combinações possíveis de caracteres até descobrirem a correta - a chamada *força-bruta*; por palpite, sobretudo se tiver termos associados ao utilizador; por visualização discreta maliciosa; ou por furto de bases de dados, chegando a ser vendida na *dark web*.

Solução?

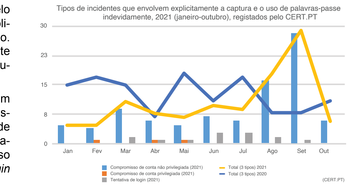
Para contornar estas vulnerabilidade de segurança, foram desenvolvidos vários esforços. Alguns acarretam soluções complementares, como é o caso da utilização do múltiplo fator de autenticação; outros, vão no sentido de sensibilizar e educar as pessoas para os cuidados que devem ter na escolha e uso das palavras-passe. Alguns serviços procuram dispensar o uso deste instrumento através de autenticações com dados biométricos, por exemplo.

VISUALIZAÇÃO

Na taxonomia de incidentes registados pelo CERT.PT, vários tipos de incidentes podem implicar o furto de palavras-passe e o seu uso indevido. Por exemplo, o *phishing* procura frequentemente capturar palavras-passe através de um *login* fraudulento.

Mas existem 3 tipos de incidentes que implicam necessariamente o uso indevido de palavras-passe por um agente malicioso: o compromisso de conta não privilegiada (acesso a conta de utilizador); o compromisso de conta privilegiada (acesso a conta de administrador); e a tentativa de *login* (apenas tentativa e não acesso a conta).

Tipos de incidentes que envolvem explicitamente a captura e o uso de palavras-passe indevidamente, 2021 (janeiro-outubro), registados pelo CERT.PT



(CERT.PT)

Entre estes 3, o tipo de incidente mais frequente é o compromisso de conta não privilegiada, que, até outubro de 2021, foi registado 92 vezes pelo CERT.PT. Os meses de agosto e setembro foram particularmente significativos, com 16 e 28 incidentes deste tipo registados, respetivamente.

Ainda neste período, aqueles 3 tipos de incidentes somavam em conjunto 108 registos (8% do total de incidentes); até outubro de 2020, registavam-se 127 (11% do total de incidentes); no final de 2020, o valor foi de 143 (10% do total de incidentes). O compromisso de conta não privilegiada foi o 4º tipo de incidente mais registado em 2020 pelo CERT.PT.

PERSPETIVA

1 Os dados disponibilizados pelo Relatório sobre a vertente comportamental da cibersegurança, do Observatório de Cibersegurança, mostram que os indivíduos em Portugal manifestam ter menos cuidados com o uso de palavras-passe do que a média da União Europeia (UE). Por exemplo, em 2019, apenas 15% dos indivíduos admitiam ter passado a utilizar palavras-passe mais complexas fruto de preocupações com a Internet, quando a média da UE foi de 26% (Eurobarómetro, 2020).

2 Os cuidados com a palavra-passe exigidos resultam das suas vulnerabilidades. Por exemplo, deve ser complexa (com caracteres diversificados) e longa devido aos mecanismos que a decifram com mais facilidade caso seja simples e curta; não deve ser constituída por termos relacionados com a pessoa para que não seja descoberta por palpite; não deve ser repetida em vários serviços porque o compromisso de uma conta pode conduzir ao compromisso de outras contas.

3 As violações de dados comprometem frequentemente listas de utilizadores onde se encontram palavras-passe que depois podem ficar disponíveis em ficheiros na *dark web*. Existem plataformas através das quais é possível perceber se uma determinada conta foi comprometida em alguma destas violações de dados. É por isso que, sempre que existe alguma desconfiança relativamente a esta possibilidade, se deve alterar a palavra-passe da conta em questão.

4 O múltiplo fator de autenticação permite fazer depender o acesso a uma conta de mais fatores além da palavra-passe, normalmente algo que sabemos (e.g., um PIN), que possuímos (e.g., um dispositivo) ou que somos (dados biométricos, e.g., impressões digitais). Para contornar a dificuldade natural em memorizar diferentes palavras-passe complexas para diversos serviços, utilizam-se os gestores de palavras-passe, de preferência desconectados da rede.

5 Os dispositivos do âmbito da Internet das Coisas e a rede Wi-Fi apresentam vulnerabilidades ligadas a palavras-passe fracas e por defeito que podem ter consequências graves. Por isso, existem alguns esforços (ver Reino Unido) que vão no sentido de obrigar os fornecedores de dispositivos ligados à Internet *e routers* a definirem palavras-passe únicas para os aparelhos, sem possibilidade de repor uma palavra-passe genérica por defeito.

6 Segundo algumas perspetivas, no futuro a palavra-passe poderá deixar de ser usada. Todavia, essa possibilidade encontra alguns desafios: o hábito enraizado nos indivíduos, que pode dificultar a adoção de novas soluções; a necessidade de ter tecnologia atualizada e disponível para o efeito; e os problemas que as alternativas também colocam (e.g., o PIN atribui demasiada importância ao dispositivo e os dados biométricos são particularmente sensíveis).

PUBLICAÇÕES E NOTÍCIAS

A **ENISA – Agência da União Europeia para a Cibersegurança** publicou, no dia 27 de outubro, mais um *ENISA Threat Landscape 2021*, através do qual faz uma análise anual das principais ameaças à cibersegurança. As ameaças mais importantes identificadas, atualmente, são o *ransomware*, o *malware*, o *cryptojacking*, ameaças ao uso de *email*, violação de dados, ataques à disponibilidade de serviços, desinformação, ameaças não maliciosas e ataques à cadeia de fornecimento.

A **Comissão Europeia** lançou, no dia 12 de novembro, o *Índice de Digitalidade da Economia e da Sociedade (IDES) de 2021*, um índice que avalia a situação dos países da UE quanto à maturidade digital em termos de capital humano, conectividade, integração das tecnologias digitais e serviços públicos digitais. Portugal ocupa o 16º lugar em 27 países (subida de 3 lugares em relação a 2020), destacando-se pela positiva nos serviços públicos digitais.

O **CNCS** aprovou, no dia 17 de novembro, o Projeto de Regulamento para Instrução Técnica Relativa ao Decreto-Lei n.º 65/2021, com respeito à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes, para dar cumprimento ao estabelecido no Decreto-Lei mencionado. O projeto foi submetido a consulta pública, que está disponível até dia 30 de dezembro de 2021.

A **ENISA** disponibilizou, no dia 29 de novembro, o Relatório *Raising Awareness of Cybersecurity*, um documento dedicado à análise das ações de sensibilização para a cibersegurança realizadas nos vários países da UE. Portugal, nesta matéria, particularmente o CNCS, surge como procurando desenvolver ações que sublinhem as boas práticas em lugar do estímulo ao medo, o uso de instrumentos de sensibilização diversificados e uma abordagem *whole-of-society*.

O **CNCS** publicou, no dia 29 de novembro, um conjunto de vídeos com recomendações para que as organizações elevem o seu nível de cibersegurança, de forma acessível, apelativa e simples. Este conjunto de vídeos, organizado em 23 módulos, surge como complemento do *Roteiro para as Capacidades Mínimas de Cibersegurança* e está associado ao *Quadro Nacional de Referência para a Cibersegurança*.

O **Observatório de Cibersegurança** do CNCS publicou, no dia 10 de dezembro, o *Relatório Cibersegurança em Portugal, tema Políticas Públicas*, o primeiro que diz respeito à linha de observação Políticas Públicas da cibersegurança. Este documento apresenta um panorama sobre as Estratégias e Programas Públicos nacionais relacionados com a cibersegurança e analisa os indicadores disponíveis sobre as perceções dos cidadãos sobre esta matéria.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança