Campanha de phishing “ZipLine” ameaça setor industrial

written by O Cidadão | 28 de Agosto, 2025

A **Check Point Software Technologies** divulgou, em **26 de agosto de 2025**, os resultados da investigação da sua equipa de **Check Point Research (CPR)** sobre a campanha **“ZipLine”**, classificada como uma das mais sofisticadas em termos de phishing e engenharia social dos últimos anos.

Diferente dos métodos tradicionais, os atacantes recorrem aos **formulários públicos de contacto** das empresas para originar o primeiro email. Este detalhe torna a comunicação mais credível e ajuda a evitar filtros automáticos. Seguem-se conversas profissionais mantidas durante **semanas**, nas quais chegam a solicitar a assinatura de **acordos de confidencialidade (NDAs)** antes de enviarem o ficheiro malicioso.

A etapa seguinte é a entrega de um **ficheiro ZIP** que contém documentos aparentemente legítimos, mas também um **ficheiro LNK malicioso**. Este aciona um **script PowerShell** executado apenas em memória, responsável pela instalação do **MixShell**, um implante que permite execução remota de comandos, exfiltração de ficheiros, criação de túneis de rede e manutenção de controlo furtivo.

O CPR identificou ainda uma variante recente em que os atacantes utilizam iscos associados a **avaliações de impacto de inteligência artificial**, explorando o atual contexto de transformação digital.

Segundo a investigação, os **principais alvos** são **empresas industriais e de cadeias de fornecimento críticas nos EUA**, com riscos de **roubo de propriedade intelectual, extorsão com ransomware, fraude financeira** e potenciais **disrupções na cadeia de abastecimento**.

Rui Duro, **Country Manager da Check Point Software em Portugal**, afirmou que "A ZipLine é um exemplo claro de inovação no phishing. Os atacantes abusam de canais legítimos, investem tempo em relações credíveis e usam iscos atuais como a inteligência artificial. É um alerta para as organizações reforçarem as defesas contra engenharia social sofisticada".

Entre as recomendações destacam-se: **monitorização de canais de entrada como formulários de contacto**, **sensibilização de colaboradores em áreas de procurement e supply chain**, **reforço da verificação de novos fornecedores**, **inspeção de anexos ZIP** e implementação de **MFA para prevenir compromissos de conta**.

A Check Point sublinha que a solução **Harmony Email & Collaboration** integra várias camadas de proteção com recurso a **IA e análise comportamental**, incluindo bloqueio de anexos maliciosos, proteção em tempo real de links de phishing e mecanismos de prevenção de fuga de dados.

OC/RPC