Infostealers: o ataque silencioso impercetível

digitalinside.pt/infostealers-o-ataque-silencioso-imperceptivel

Bruno Castro

Os infostealers consistem numa categoria de malware desenhados para se infiltrarem em sistemas informáticos e extrair dados sensíveis, como credenciais de acesso, cookies, informações financeiras e outros dados pessoais. Esta tipologia de malware opera de forma furtiva, muitas vezes passando até despercebida pelos utilizadores e até por algumas soluções de segurança. Depois de os dados serem roubados, são frequentemente vendidos de forma ilícita, por exemplo, na dark web, ou utilizados para facilitar outras atividades criminosas, como fraudes financeiras e roubo de identidade. Este tipo de malware propaga-se, tipicamente, através de ligações de phishing, websites comprometidos e também anexos maliciosos em emails, tendo como alvo tanto dispositivos pessoais como empresariais.

Entre 2023 e 2024, a Kaspersky estimou que aproximadamente 2,3 milhões de cartões bancários foram comprometidos e divulgados na dark web devido à atuação de infostealers. Essa conclusão baseia-se na análise de ficheiros de registo de diversos malwares de roubo de dados que operaram durante esse período. Embora globalmente a percentagem de cartões comprometidos seja inferior a 1%, é alarmante notar que 95% desses dados bancários parecem ser ainda tecnicamente válidos.

Mas… como é que os infostealers conseguem ser tão bem-sucedidos? A realidade é que por detrás desta tipologia de cibercrime existe todo um modelo de negócio altamente maduro com uma clara divisão de trabalhos já bastante enraizada no submundo digital. Alguns são encarregues de desenvolver os infostealers e ainda as respetivas ferramentas de gestão dos mesmos – cada vez mais no modelo de Malware as a Service (MaaS). Outros tratam de libertar o malware nos dispositivos das vítimas, utilizando phishing e outras técnicas. Outros lidam especificamente com o que fazer com os dados roubados. Estas três “categorias” de cibercriminosos operam geralmente de forma independente, no entanto, mantêm relações comerciais entre si.

O malware Infostealer, embora não seja uma ameaça nova, demonstrou um aumento preocupante de sofisticação e eficácia como é patente no relatório “Cybersecurity Forecast 2025” da Google, que sublinha que esses malwares têm um papel cada vez mais relevante no roubo de credenciais, especialmente, em ambientes que não adotam determinadas medidas de cibersegurança – e medidas tão simples como é a autenticação de dois fatores. A ausência desta camada de segurança adicional deixa as organizações suscetíveis a violações de dados de vários graus de gravidade. Além disso, a sofisticação do malware infostealer tem aumentado nos últimos anos, com os avanços nas técnicas e nos recursos para contornar a deteção e a resposta de endpoint (EDR), tornando cada vez mais desafiante o panorama das ciberameaças.

Ainda de acordo com este relatório, em 2024, os cibercriminosos aproveitaram as credenciais roubadas, obtidas através de campanhas generalizadas de roubo de informação, para se infiltrarem num número significativo de organizações importantes, resultando em várias intrusões de grande impacto. A alarmante acessibilidade de credenciais destas ferramentas, mesmo para agentes de ameaças pouco qualificados, amplifica o seu potencial de impacto generalizado. Deste modo, a previsão é de que a utilização de credenciais roubadas persista em 2025, com os infostealers a continuarem a servir como vetor primário para obtenção das mesmas.

Adicionalmente, novas variantes de infostealers, como o “Banshee Stealer”, emergirão com a capacidade de afetar tanto dispositivos Windows quanto Apple, ampliando o alcance e o impacto dessas ameaças.

A proliferação de infostealers tem alimentado um mercado negro cada vez mais lucrativo, onde dados roubados são vendidos não apenas em fóruns da dark web, mas também em plataformas descentralizadas e redes sociais, como o Telegram. Essa dinâmica facilita a disseminação de informações confidenciais e aumenta os riscos associados ao cibercrime. Não se esqueça que, a prevenção começa nas pequenas coisas e mais vale ter uma autenticação dois fatores na mão, do que ver os seus dados confidenciais a voar.