BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

ABRIL 2024 | n.º 1/2024

DESTAQUES

Infostealers

Os *infostealers*, ou *stealers*, são um tipo de código malicioso (*malware*) desenvolvido para sub-repticiamente recolher dados sensíveis de um sistema. Os *infostealers* recolhem dados extremamente delicados tais como palavras-passe, *cookies*, detalhes bancários, carteiras de criptomoedas, *emails* e outros documentos. Este código malicioso representa um desafio elevado, pois permite contornar algumas das boas práticas clássicas na proteção de dados.

Ameaça

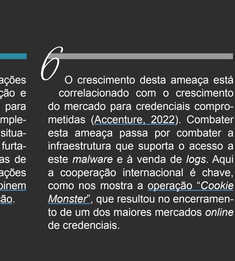
Embora os *infostealers* tenham ganho notoriedade já em 2007 com o Zeus/Zbot (FBI, 2010), o seu nível de ameaça tem aumentado ao longo dos anos devido ao desenvolvimento de múltiplas variantes com capacidades cada vez mais sofisticadas. Estas novas variantes destacam-se por serem não só capazes de recolher dados sensíveis de forma massiva (DOJ, 2022), como também por terem sido cruciais para perpetrar ciberataques de larga escala (Uber, 2022).

Ecossistema

Por detrás desta crescente ameaça encontramos um "ecossistema" comercial composto por fóruns *online* que operam como mercados. Aqui encontramos atores a venderem o acesso a *infostealers* (*Malware-as-a-service*) e atores a venderem *logs* com dados recolhidos por *infostealers* (Accenture, 2022). A aquisição de credenciais neste ecossistema é instrumental para a execução de outros ciberataques, como o *ransomware* (CSRB, 2023).

PANORÂMICA

- Com base em dados da matriz MITRE ATT&CK Enterprise relativa a 30 variantes por esta monitorizadas, apontam-se algumas técnicas utilizadas por este *malware*. A técnica de acesso inicial mais frequentemente utilizada é o *spearphishing* com anexo, estando presente em 43% das variantes. Segue-se o *spearphishing* com *link*, representando 30% das técnicas utilizadas. Identificam-se, ainda, variantes que recorrem a técnicas de *replication through removable media*, e.g. distribuição do *malware* através de dispositivos USB, e *drive-by compromise*, e.g. distribuição durante visita a *website* comprometido.



Técnicas mais frequentemente utilizadas por infostealers no âmbito das táticas.
Fonte: MITRE ATT&CK Enterprise Matrix. TTP: Técnicas , Táticas e Procedimentos

- Nesta visualização, destacamos as técnicas mais frequentes no âmbito das táticas de recolha e acesso a credenciais. Em particular, técnicas de captura de *input*, como o *keylogging*, presentes em 60% das variantes, bem como outras técnicas de captura de conteúdo, como captura de ecrã, 36% das variantes, ou captura de áudio e de vídeo, 10% das variantes.
- Com a presença em 46% das variantes, destaca-se, ainda, neste contexto a recolha direta de credenciais de várias fontes, desde credenciais presentes em *browsers*, gestores de palavras-passe ou ficheiros, assim como de informação associada a outros métodos de autenticação, nomeadamente *cookies*.

PERSPETIVA

1

Em setembro de 2022, membros do grupo Lapsus$ comprometeram os sistemas da Uber. Uma análise ao incidente revelou que a intrusão terá sido possível devido à aquisição na *dark web* de credenciais de um colaborador subcontratado, tendo estas sido alegadamente recolhidas a partir do seu computador pessoal após este ser infetado por *malware* (Uber, 2022).

2

Este episódio mostra como os *infostealers* são uma ameaça a dois níveis: por um lado, existe a ameaça para os indivíduos cujo dispositivo informático pode ser infetado por *infostealers* e, por outro, existe a ameaça para as organizações cujos colaboradores podem ter as suas credenciais profissionais furtadas e postas à venda em mercados de *logs*. Cada foco de ameaça está associado a diferentes riscos e às respetivas medidas de mitigação.

3

A fronteira entre o risco individual e o risco para as organizações tornou-se mais ténue com a pandemia. Em particular, o trabalho remoto levou a que alguns trabalhadores utilizassem o computador pessoal para tarefas profissionais (Pranggono e Arabo, 2020), pondo assim em risco as suas credenciais profissionais em caso de o seu computador pessoal ser infetado por *infostealers*.

4

Ao nível do indivíduo, as estratégias de mitigação não divergem das boas práticas de cibersegurança recomendadas pelo CNCS. Destacam-se em particular as relativas ao *phishing*, *smishing* e *vishing*, já que, como se demonstra acima, estão particularmente associadas a esta ameaça. Igualmente cruciais são as boas práticas relativas à navegação na Internet e à utilização de dispositivos profissionais, nomeadamente em teletrabalho.

5

Já a proteção das organizações passa, por um lado, pela formação e sensibilização dos colaboradores para estas ameaças e, por outro, por implementar processos para lidar com situações em que as credenciais são furtadas. Aqui destacam-se as políticas de autenticação, devendo as organizações dar primazia a soluções que combinem dois ou mais fatores de autenticação.

6

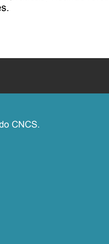
O crescimento desta ameaça está correlacionado com o crescimento do mercado para credenciais comprometidas (Accenture, 2022). Combater esta ameaça passa por combater a infraestrutura que suporta o acesso a este *malware* e à venda de *logs*. Aqui a cooperação internacional é chave, como nos mostra a operação "*Cookie Monster*", que resultou no encerramento de um dos maiores mercados *online* de credenciais.

PUBLICAÇÕES E NOTÍCIAS

Decorreram nos dias 6 e 8 de fevereiro, em Viseu, as comemorações para assinalar o Dia da Internet Mais Segura. A 21.ª edição do Dia da Internet Mais Segura (SID Summit 2024) foi organizada pelo Consórcio do **Centro Internet Segura**, sob a coordenação do CNCS e contou com o apoio do Instituto Politécnico de Viseu. A Inteligência Artificial deu o mote às comemorações, que tiveram como evento em destaque o fórum "*Zoom na IA: Explorar Dimensões Invisíveis*".

O **Centro Nacional de Cibersegurança**, no dia 9 de fevereiro, realizou, nas suas instalações, um Exercício de Cibersegurança dedicado às Eleições com o objetivo de testar os diferentes mecanismos de articulação entre as várias entidades envolvidas. Para este exercício foi definido como cenário a ocorrência de uma série de incidentes associados a campanhas de desinformação.

O **Observatório de Cibersegurança do CNCS**, no dia 28 de dezembro de 2023, publicou o *Relatório Cibersegurança em Portugal – tema Sociedade 2023*. Este documento, que vai na sua quinta edição, analisa o estado da componente humana da cibersegurança, nomeadamente as atitudes, os comportamentos e a sensibilização e educação nesta matéria. Este relatório foi também tema de debate num Cibertema promovido pelo CNCS a 21 de fevereiro.



A **NIST**, no dia 26 de fevereiro, lançou a versão 2.0 do *Cybersecurity Framework* (CSF), marcando a primeira grande atualização do Quadro de Referência para a Cibersegurança do regulador Norte-Americano desde a sua criação há 10 anos. Esta atualização teve como foco a governança da cibersegurança e a gestão de riscos nas cadeias de fornecimento.

A ENISA – Agência da União Europeia para a Cibersegurança, a 28 de fevereiro, publicou o estudo *Best Practices for Cyber Crisis Management*, que visa auxiliar no planeamento e preparação da gestão de cenários de crise. Desenvolvido pela Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe), este estudo mapeia uma série de cenários de crise e melhores práticas, visando reforçar a capacitação e cooperação operacional no contexto da gestão de cibercrises.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança