



CIBERSEGURANÇA E CIBERDEFESA

Nº 01/2024, de 23 de outubro de 2024.

1. DESCRIÇÃO

- a. As tecnologias de informação e de comunicações e os militares e trabalhadores civis que as utilizam são elementos essenciais para assegurar a manutenção da atividade do Exército.
- b. Este boletim informativo tem por finalidade apresentar o que é um *Infostealer*, quais são os seus meios de propagação, qual a tipologia de informação em risco e quais as medidas de mitigação.
- c. O ciberespaço é palco de ameaças, de diferentes origens e motivações. No entanto, é possível aumentar a nossa capacidade de cibersegurança, para melhor proteger a confidencialidade, integridade e disponibilidade da nossa Informação.
- d. A utilização de equipamentos pessoais para aceder aos Sistemas de Informação (SI) e à infraestrutura de rede do Exército acarreta riscos que poderão ser reduzidos a um nível aceitável com a aplicação de algumas regras de boas práticas, de carácter simples.

2. SUMÁRIO

a. O que é um Infostealer?

Um *Infostealer* é um tipo de *malware*, normalmente um vírus *Trojan*, que tem a capacidade de se disfarçar, passando despercebido ao utilizador comum, que irá permitir ao atacante ganhar acesso a informação sensível e pessoal. Genericamente, este tipo de *malware* pode recolher informação através da escrita do teclado, *screenshots*, atividade da rede e do *browser*.

b. Métodos de propagação de um *Infostealer*

Um *Infostealer* pode ser transmitido de diversas formas sendo normalmente requerida a interação por parte da vítima e do utilizador, das quais se destacam as seguintes:

- E-mails falsos (e-mails de *phishing* com anexos/links maliciosos);
- Jogos não licenciados;
- Softwares/programas grátis;
- *Links* maliciosos nas plataformas das redes sociais;
- Anúncios falsos.

c. Tipo de informação

Muitas vezes a informação do Utilizador está guardada no *browser* facilitando assim a ação dos *infostealers* para realizar uma variedade de ações que lhes irá permitir recolher informações sensíveis, como por exemplo:

- Extração de Credenciais de Login – Utilizador e password;
- Histórico de navegação (Websites, cookies, informação de preenchimento automático, etc.);
- Informação financeiras - cartão de crédito;
- Acesso às sessões ativas no browser;
- Informações pessoais (Nome, endereço, número de telefone, documentos de identidade, etc.).

3. RECOMENDAÇÕES

Por forma a impedir que os *Infostealers* não tenham sucesso na exploração de vulnerabilidades existentes nos nossos computadores que lhes permita comprometerem os nossos sistemas e serviços, devem ser adotadas as seguintes medidas de mitigação, **quer nos terminais de trabalho, quer nos computadores e dispositivos pessoais:**

- **Nunca guardar/memorizar as credenciais institucionais (do Exército e particulares) nos navegadores (*browser*), em qualquer dispositivo, quer de trabalho quer nos pessoais** (telemóvel, computador, tablet);
- Não utilizar a password da conta institucional (do Exército) em outras aplicações/serviços da internet;

- Não carregar em *links* de *emails* de fonte não fidedigna;
- Instalar nos terminais de trabalho da Rede de Dados do Exército apenas os softwares existentes no “Centro de Software” ou os que forem previamente autorizados;
- Instalar nos computadores e dispositivos pessoais softwares de fontes fidedignas e não instalar softwares ilegais (“pirateados”);
- Não carregar em quaisquer anúncios das páginas da Internet;
- Manter todo o software atualizado, uma vez que essas atualizações servem muitas vezes para corrigir vulnerabilidades;
- Utilização de um antivírus por forma a detetar e bloquear ameaças indesejadas;
- Estar atento e reportar através do *helpdesk* quaisquer comportamentos anómalos dos computadores;
- Estar atento aos potenciais ataques de *phishing* (ver boletins informativos 05/2019 e 06/2019).

4. DISTRIBUIÇÃO

Todos os utilizadores da Rede de Dados do Exército.

Esta informação é apenas para uso oficial e não deve ser publicada ou divulgada fora do Exército Português.