

H02 TECHNOLOGY

My crime is that of  
curiosity

# O manual da CYBERSEGURANÇA: VOL. I

O que ninguém irá te contar

Patrick Resende

Em meados de 2013, fui hackeado. No começo não me importei muito, mas só depois percebi o que estava acontecendo.

Tudo começou com um .exe executado no meu computador por um adolescente de 17 anos, com bons conhecimentos para a época onde apenas tínhamos MSN e Orkut, redes sociais da época.

Esse Hacker utilizou de engenharia social, criou um chat para nossa comunicação de amigos e no backdoor do aplicativo existia um Keylogger que o daria acesso à todas as minhas informações em tempo real.

Desde a hora que eu deslogava, até a hora que eu acordava, os sites que eu visitava, minha senhas, minhas conversas mais íntimas. Ele se tornou eu!



Foi quando percebi o problema. Não querendo formatar o computador por não ter tempo de realizar os devidos backups, ele armazenava mais e mais informações sobre a minha pessoa e família.

Na época, não havia um negócio, não possuía arquivos importantes. Mas ainda assim, não é algo que alguém gostaria de passar.

Sempre gostei de tecnologia, e 7 após, dei início a minha jornada com a programação e cibersegurança. Aprimorando conhecimentos de criptografia, segurança ofensiva e defensiva, criação de scripts para monitoramento em tempo real, e então, os problemas diminuíram.

Mas desaparecer? Impossível.



Antes de tudo, deixa eu me apresentar:

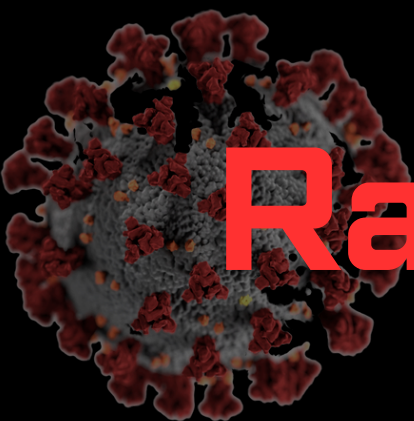
Me chamo Patrick Resende, sou fundador da Hoz Technology, uma empresa de ensino e consultoria na área de Tecnologia da Informação, formado como Analista de Sistemas com foco na área de Cybersecurity. Neste E-book trago algumas informações valiosas sobre proteção geral na internet

Desde já informo que esse não é um material para o público avançado, pois o meu objetivo aqui é informar e alertar os perigos na internet e como evitar infortúnios maiores com dicas simples.

Como é um e-book curto e ninguém gosta de perder tempo... Let's do it.



## Um dos Maiores Temores Empresariais:



# Ransomwares:

Ransomwares, popularmente conhecidos como "sequestradores de dados". São um tipo de vírus que sequestram informações dos usuários para fins de clonagem de cartão, acesso as plataformas, recompensa para tê-los de volta. E podem estar em qualquer tipo de arquivo que você baixa na internet.

A melhor resposta para prevenir um ataque desses é utilizar um bom antivírus e evitar baixar arquivos de fontes desconhecidas e não confiáveis.





## O que os Hackers procuram?

Basicamente falando? **BRECHAS!** Um black hat (como são chamados) basicamente procura uma falha no sistema, seja uma porta de servidor aberta, um funcionário que clicaria em arquivo malicioso, quebra de senhas usando força bruta ou engenharia social.

Para todos existem expertises de segurança virtual que irei elencar de maneira breve. Algumas técnicas de proteção necessitam o auxílio de softwares e domínios específicos para a proteção de sistemas.



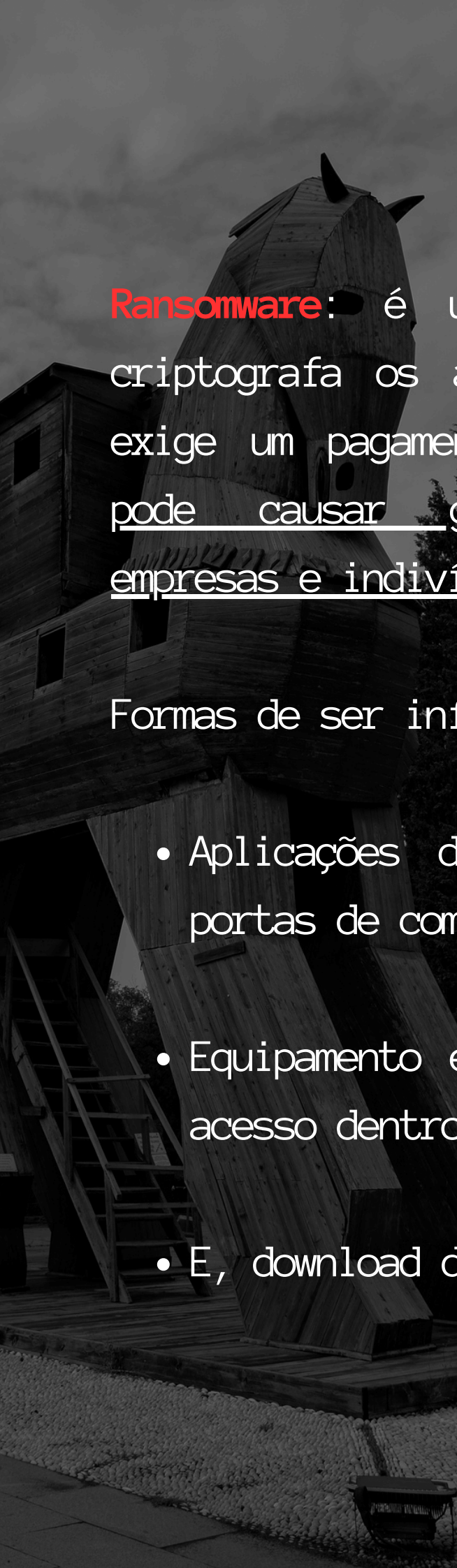
## 4 - Alguns tipos perigosos de vírus

- **Cavalo de Tróia (Trojan Horse):** é um tipo de malware que se disfarça como algo bom, mas que pode roubar dados, senhas e credenciais bancárias dos usuários. Ele também pode se espalhar via e-mails e redes sociais.

Formas de ser infectado:

- Download de programas pirateados.





**Ransomware:** é um tipo de malware que criptografa os arquivos do computador e exige um pagamento para liberá-los. Ele pode causar grandes prejuízos para empresas e indivíduos.

Formas de ser infectado:

- Aplicações desatualizadas que deixam portas de comunicação aberta.
- Equipamento exposto com facilidade de acesso dentro da empresa.
- E, download de aplicações duvidosas.





- **RaaS (Ransomware as a Service)**: é um modelo de negócio em que hackers vendem ou alugam ransomware para outros criminosos, facilitando a disseminação desse tipo de malware. O cliente paga uma taxa ou uma porcentagem do resgate obtido.
- **Atualizações falsas do Windows (Ransomware oculto)**: são e-mails que instruem os usuários a instalar atualizações urgentes do Windows, mas que na verdade contêm um ransomware que sequestra os dados do computador<sup>1</sup>.

Mas, não menos importante...



# Engenharia Social:

A **Engenharia social** é o puro suco da persuassão e gathering de informações. É o ato de entrar na casa, empresa ou computador da vítima e descobrir informações importantes e confidenciais.

Ela acontece há séculos, foi e é pioneira de grandes guerras, como a Máquina de Turing na 2ª Guerra Mundial, na qual era capaz de decifrar mensagens que eram transmitidas pelos Alemães.

Alan Turing ficaria orgulhoso e temeroso de onde chegamos, na qual muitas mensagens são encriptadas e descriptadas por segundo, por vezes aparentando estarmos em uma guerra cibernética infinita.



# Como se proteger de forma simples de ataques:

- 1 – Evite realizar downloads de aplicativos de fontes desconhecidas, sem avaliação e de sites estranhos.
- 2 – Tenha atenção aos sites que não tenham proteção HTTPS.
- 3 – Aprenda a instalar uma VPN (Virtual Private Network) ou configure um proxy.
- 3 – Atualização constante dos sistemas operacionais (as maiores falhas são em sistemas obsoletos).
- 4 – Criptografe arquivos importantes, anote em um caderno e guarde em um local seguro.
- 5 – Conheça as vulnerabilidades dos seus equipamentos e esteja por dentro de novas tendências de ataques.



## **O Mercado da Segurança da Informação**

Infelizmente, no Brasil, este setor ainda possui pouco valor, mas com muitos danos materiais e financeiros.

Sendo que notícia relatadas em diversos jornais relevantes do país alegam que o Brasil é um dos países mais visados para essas operações, por conta das leis que são brandas e a falta de informação de pessoas e empresas em ter um profissional qualificado para as demandas.

Um banco não deixa a porta de entrada sem segurança, certo?

Contanto, o mercado de trabalho para outros países chega a ser bem promissor, com salários girando em





torno de US\$ 101.926, aproximadamente R\$585.279, anualmente.

No dia 28/03/25, o Instituto de Pesquisas Energéticas e Nucleares IPEN/CNEN, em São Paulo, sofreu um ataque cibernético, comprometendo dados e tendo que acionar equipes para mitigar o problema, pois apenas se evita um ataque previamente ou durante, tentar algo após é como uma guerra: sem equipamentos, muros quebrados, danos irreparáveis. E os espólios? Ao vencedor.



De acordo com a VULTUS Cybersecurity Ecosystem, Até 2026, apenas 10% das grandes empresas terão maturidade em cybersecurity.

Entretanto, esse não é apenas um problema que assola grandes empresas, pode afetar o desde grandes negócios, à segurança do seu patrimônio.

Uma informação isolada é capaz de buscar e realizar uma engenharia social com um phishing bem sucedido e colocar qualquer um em risco.



Curtiu o conteúdo?

Se inscreva nas nossas redes para ter acesso a todas as informações atuais da área cyber. Em breve nosso site estará no ar!

instagram: @hoz.tech

Precisa de assessoria para a sua empresa ou residencial? entre em contato conosco no e-mail:

hoztech@proton.me

"A defesa aprimorada se torna o seu maior ataque"

