Prof. Esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp

- **Consultor de Tecnologia - [aXR6] Cyber Security e NtecSoftware**
- **Professor no Senac (contratado)**
- **Professor na Wyden Facimp (contratado)**
  - **Pós-graduação:** Segurança em redes de computadores - Wyden Facimp
- **Professor na Wyden Facimp (Efetivado)**
  - **Graduação:** Análise e desenvolvimento de sistemas - Wyden Facimp

Redes sociais:

- **Linkedin:** https://www.linkedin.com/in/thalles-canela/
- **YouTube:** https://www.youtube.com/aXR6CyberSecurity
- **Facebook:** https://www.facebook.com/axr6PenTest
- **Instagram:** https://www.instagram.com/thalles_canela
- **Github:** https://github.com/ThallesCanela
- **Github:** https://github.com/aXR6
- **Twitter:** https://twitter.com/Axr6S

Payload: a carga pesada do cibercrime

Já diria a sabedoria popular que o importante é saber o que importa

Mas afinal, qual o significado de payload?

- No geral, o termo payload (ou "carga útil") é utilizado simplesmente para distinguir informações essenciais de informações que não têm muito valor final.

Calma! É simples:

- Suponha que um caminhão pipa, que carrega 20 toneladas de água, vai em direção a um prédio com o intuito de ajudar a apagar um mega incêndio.
- No total, a sua carga é maior do que as 20 toneladas, por conta do peso da própria carcaça do veículo, do seu tanque, do combustível, do motorista, dos passageiros, etc.
- Porém, a informação que importa é **o quanto de água o caminhão está transportando.** Este é o seu payload — sua carga útil, a parte que interessa o destinatário; o resto, enquanto informação vital, é a sobrecarga de protocolo.

Nos campos da telecomunicação e computação:

- O termo tem sido referido como a parte de um pacote de dados transmitido que contém o ‘conteúdo real e principal’ de uma mensagem enviada, diferenciando aquilo que é útil daquilo que é inútil.

E no universo da cibersegurança:

- Payload é comumente empregado para se referir à carga (parte) de um arquivo malicioso que o distingue de arquivos legítimos.
- É constantemente associado à capacidade do código maligno de causar danos.

Os malwares, por exemplo:

- São identificados por uma ferramenta antimalware através da detecção dos seus payloads.
- Estes programas maliciosos são especialmente programados para se passarem por inofensivos, mas no fim, só causam mal ao sistema do usuário que os executou.

“É uma cilada, Bino!”

- Nesse "disfarce", os softwares podem até apresentar atributos de um programa autêntico, benigno; porém, no final, o que importa é que eles são malignos. E são os seus payloads que informam sua malícia.
- Assim, o payload é a ação danosa que uma ameaça executa, além do seu comportamento normal, fingido. E esse código faz muito mais do que apenas diferenciar um programa legítimo de um ilegítimo.
-

Payload x Overhead

- Alguns iniciantes confundem **overhead** com uma espécie de sobrecarga inconveniente na rede. Tipo algum dado que está trafegando sem necessidade.
- Se formos traduzir essas palavras em inglês, "payload" quer dizer "carga útil" e "overhead" quer dizer "sobrecarga".

Quando estamos falando de redes computacionais: "overhead"

- Essa palavra determina todos aqueles metadados contidos nos pacotes e que são extremante importantes, pois são codificações usadas para que os ativos de rede funcionem da forma desejada.
- "metadados" são nada mais que dados de controle, usados por determinados programas, protocolos ou hardwares.

Definindo:

- Então, retornando às nossas redes de computadores, esses metadados são chamados de "overhead" e a carga útil que vc quer veicular, os dados propriamente ditos, são chamados de "payload".