MALWARE

“MALICIOUS SOFTWARE”

INTRODUCTION TO MALWARE

Malware, short for "**malicious software**," is a broad term used to describe any software specifically designed to **harm**, **exploit**, or **compromise** computer systems, networks, or user devices.

Used for various **illegal** or **unethical** purposes, such as **stealing** sensitive information, **damaging** data, or **gaining unauthorized** access to computer systems.

TYPES AND CATEGORIES OF MALWARE

Viruses: Self-replicating programs that attach themselves to legitimate files or programs. Spread from one computer to another and can cause various types of damage, including data loss and system instability. ***Requires a user interaction and usually affect on one machine.***

Worms: Standalone programs that can replicate themselves and spread to other computers over a network or the internet. Exploit vulnerabilities to infect systems and can cause network congestion and data loss. ***Does not require user interaction and can spread across networks***.

Trojans (Trojan Horses): Disguised as legitimate software or files but contain hidden malicious code. Used to create backdoors for remote attackers, steal data, or perform other harmful actions.

Ransomware: Encrypts a user's files and ***demands a ransom*** in exchange for the decryption key.

Spyware: Designed to ***secretly gather information about a user's activities***, including keystrokes, web browsing habits, and login credentials. This information is often sent to a remote attacker.

Adware: ***Displays unwanted advertisements*** on a user's device. While not always malicious, it can be considered malware if it disrupts the user's experience and privacy.

Rootkits: Malicious programs that ***gain unauthorized access to the root-level*** of an operating system, allowing attackers to hide their presence and control the system.

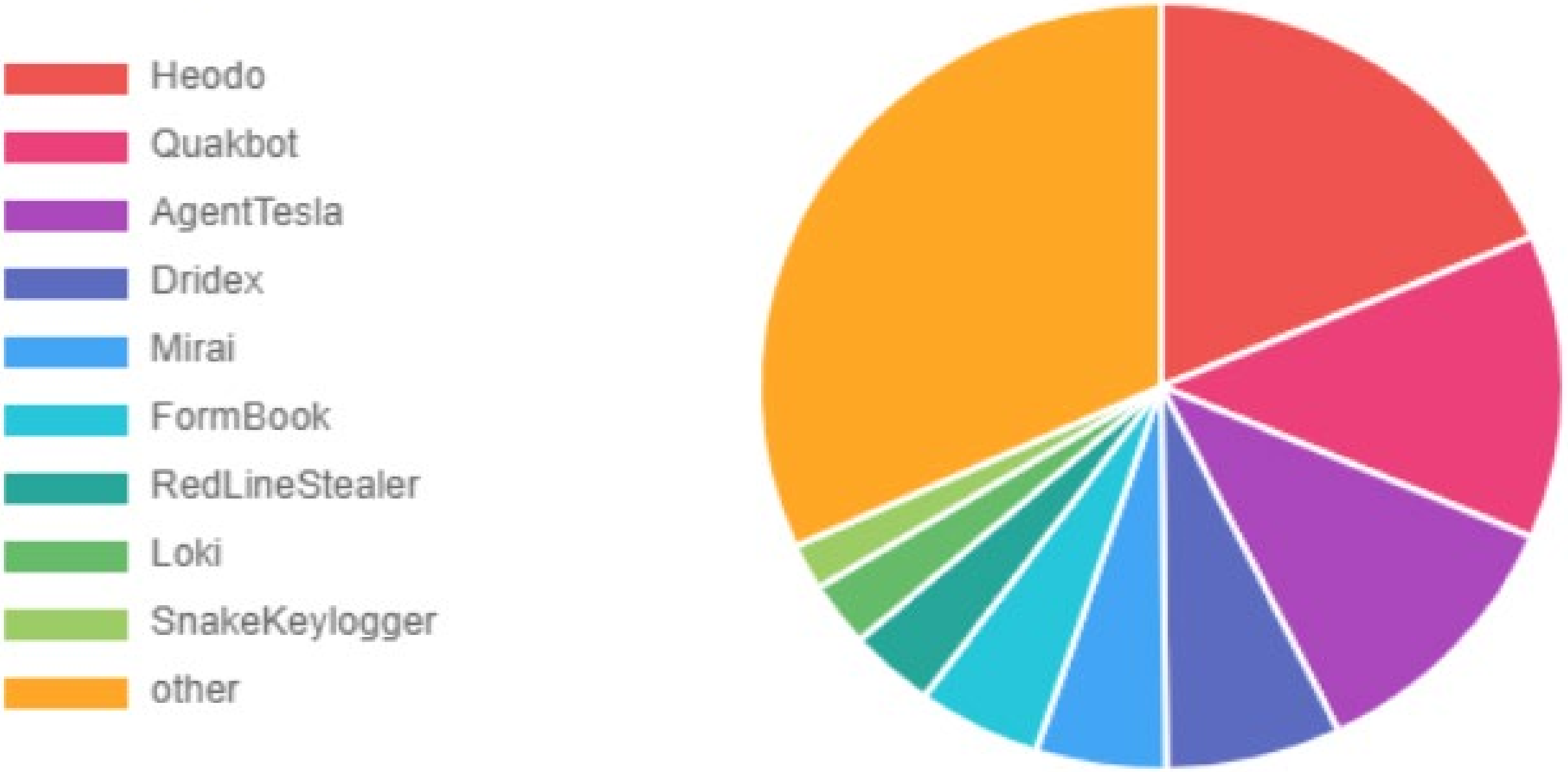
Botnets: ***Networks of compromised devices*** (often called "bots" or "zombies") controlled by a central server. They can be used for various malicious purposes, such as launching distributed denial-of-service (***DDoS***) attacks.

Keyloggers: Keyloggers ***record a user's keystrokes***, which can include sensitive information like passwords and credit card numbers. The recorded data is then sent to the attacker.

MALWARE FAMILY

Malware family is a **term that refers to a collection of malware that is produced from the same code base**. Malware families share **common traits** such as the **codebase** or the development group that authored the original strain

Top Malware Families



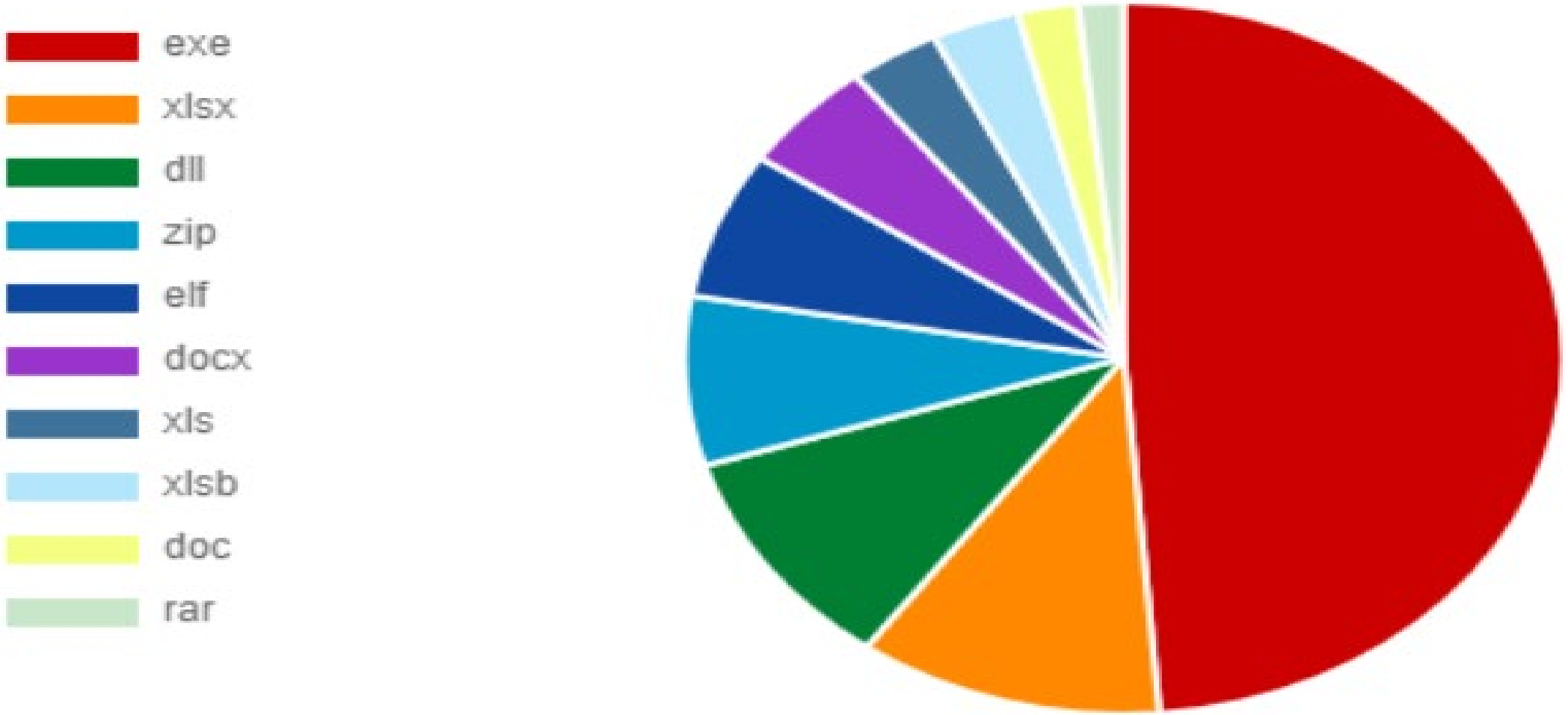
MALWARE DATABASE

https://malpedia.caad.fkie.fraunhofer.de/families

File Types

Top File Types

Most seen `file types` associated with malware samples on MalwareBazaar.



COMMON FILE TYPES

Office

Word
.doc
.docx
.docm
.dot
.dotx
.dotm
.xml

Excel
.xls .xml
.xlsx
.xlsm
.xlt
.xltx
.xltm
.xlb
.xlsb
.iqy
.slk

Power point
.ppt .ppsx
.pptx
.pptm
.pot
.potx
.potm
.ppa
.ppam
.pps
.ppsm

Access
.accdb
.adn
.accdr
.accdt
.accda
.mdw
.accde
.ade
.mdb
.mda

Visio
.vsd .vss
.vst .vsw
.vdx
.vtx
.vsdx
.vsdm
.vssx
.vssm
.vstx
.vstm

Others
.mpp
.pub
.puz
.hwp
.hwt

Windows

Executable
.exe .js
.scr .jse
.lnk .cmd
.bat .wsc
.vbs .ws
.vbe .sct
.wsf .ps1
.jar
.class

System
.dll
.sys
.ocx
.msi
.msp

Adobe

.pdf

Text/Video

.rtf
.swf

Internet

.url
.htm
.html
.hta
.chm
.mhtml
.mht

Email

.eml
.msg

Compressed

.zip
.7z
.tar
.cab
.rar
.iso
.vdf
.wim

MacOS

Executable
Mach-O
.app

Script
.sh .tclsh
.bash .tcsh
.zsh
.command
.py
.applescript
.osascript
.scpt
.csh
.ksh

Others
.java
.class
.pkg
.dmg

SUSPICIOUS FILE TYPES

.sh	→	bash script
.py	→	python script
.exe	→	windows executable
.vbs	→	visual basic script
.js	→	JavaScript
.bat	→	batch file
.ps1	→	PowerShell

MALWARE LIFECYCLE

Infection: Initial entry point for the malware into a target system

Propagation: Spreading the malware to as many vulnerable targets as possible

Execution: Starts to carry out its malicious actions, which can vary widely depending on its purpose

Concealment: Tries to hide its presence and activities on the infected system

Payload: Involves activities like data exfiltration, data encryption (in the case of ransomware), initiating further attacks (e.g., launching DDoS attacks), or establishing persistent access for future exploitation.

TYPES OF ATTACK

- **DoS** ➔ A Denial-of-Service (DoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming it with a flood of illegitimate traffic or resource requests.

- **DDoS** ➔ In a DDoS attack, a large number of compromised computers, often referred to as "botnets," are coordinated to send traffic to the target, making it difficult or impossible for legitimate users to access the targeted resource.

- **MiTM** ➔ A (Man-in-the-Middle) attack is a type of cyberattack where an attacker intercepts communication between two parties without their knowledge.

- **Buffer Overflow** ➔ A buffer overflow attack is a type of security vulnerability that occurs when a program or process attempts to store more data in a buffer (temporary data storage area) than it was intended to hold.

- **Bruteforce Attack** ➔ A Brute Force Attack is a type of cyberattack methodology used by hackers to gain access to a system or data by trying all possible combinations of passwords or encryption keys until the correct one is found.

- **Dictionary Attack** ➔ A Dictionary Attack is a type of brute-force attack method used to gain unauthorized access to a system or data by systematically entering every word in a predefined list, often called a "dictionary," until the correct password is found.

DEMO

- Go to https://hexed.it/

- Click on “open file” then select a file from your computer

- NOTE: All **.exe** files will start with **MZ** in a Hex Editor (**4D5A**)

MALWARE BEHAVIOR AND GOALS

Malware objectives:

Data Theft

Financial Gain

System Disruption

Spying and Surveillance, etc.

Malware impact on infected systems:

Data Loss or Compromise

Financial Loss

System Downtime

Reputation Damage

Legal Consequences, etc.

SIGNS OF MALWARE INFECTION

Unrecognized Processes: Use the Task Manager (**Ctrl+Shift+Esc**) or **Activity Monitor** (on macOS) to check running processes. If you notice unfamiliar or suspicious processes, they may be related to malware.

High System Resource Usage: Some malware strains consume excessive CPU or memory resources, causing your computer to become unresponsive or slow.

Sluggish Performance

Unwanted Pop-Ups

Unwanted redirects

Ransom Notes

MALWARE ANALYSIS TECHNIQUES

Static Analysis: Security experts begin with static analysis, which involves examining the malware's code without executing it. This includes inspecting the binary, file structure, and embedded resources. Key static analysis techniques include:

File signature analysis: Identifying known malware signatures

Code disassembly: Converting machine code into human-readable assembly code

String analysis: Identifying suspicious or hardcoded strings, URLs, and encryption keys

Resource analysis: Inspecting embedded files, configurations, or other resources

MALWARE ANALYSIS TECHNIQUES

Dynamic Analysis: Dynamic analysis involves executing malware within a controlled environment, such as a sandbox, to observe its behavior. This includes:

Behavior Monitoring: Recording system calls, network activity, and file modifications.

API Call Monitoring: Tracking API calls made by the malware during execution.

Memory Analysis: Examining the malware's interaction with memory, including injection techniques.

MALWARE ANALYSIS TOOLS

Cuckoo Sandbox Provides a balance between automated and manual malware analysis tools, complete with multiple sandbox environments

IDA Pro A highly technical tool designed with forensic and cybersecurity pros in mind.

CrowdStrike Falcon Insight This EDR analyzes malware on two levels and also identifies intruder activity.

Hybrid Analysis Simple web-based tool, ideal for researchers looking to perform malware searches

Limon Developed to detect Linux-based malware

VirusTotal A massive repository of malware signatures available online for both end-users and researchers alike

Wireshark Provides deep packet inspection to uncover malware communicating across a network

PeStudio Designed to streamline the analysis process for malware researchers

Fiddler Identifies malicious activity by monitoring HTTP/S traffic via proxy

Process Monitor Uncovers the relationship between executables and procedures to help identify malware and its behavior

MALWARE PREVENTION

Use Antivirus Software

Keep Software Updated

Use a Firewall

Implement Network Segmentation

User Education and Training

Continuous Monitoring