

# Malicious Code Analysis

Fangtian Zhong  
CSCI 591

Gianforte School of Computing  
Norm Asbjornson College of Engineering  
E-mail: [fangtian.zhong@montana.edu](mailto:fangtian.zhong@montana.edu)





# Overview

---

**01**

**Spyware**

**02**

**Adware**

**03**

**Polymorphism and  
Metamorphism**



*Part One*

01

2025-9-14

# Spyware

An isometric illustration of a digital workspace. It features several stylized figures: a man in a suit pointing at a large screen displaying a grid of data, a man in a light blue shirt walking, and a woman in a dark dress talking to a man in a white shirt. The background is filled with various digital elements like floating screens, a calendar, a document, and a padlock icon, all in a light blue and white color scheme.



# What is Spyware?

---

- 🏆 Application that sends information from your computer to the creator of the spyware
- 🏆 Sometimes consists of an apparent core functionality and a hidden functionality of information gathering (Trojan)
- 🏆 Can be used by websites for marketing information, to determine their stance with regard to competitors and market trends
- 🏆 Can also be used to log keystrokes and send those to whomever



# What is Spyware ?

---

- 🏆 Software installed on a computer without the user's knowledge which gathers information about that user for later retrieval by whomever controls the spyware.
- 🏆 Spyware can be broken down into two different categories:
  - surveillance spyware
  - advertising spyware.



# What is Spyware ?

---



## Surveillance spyware:

- Includes key loggers, screen capture devices, and Trojans. They would be used by corporations, private detectives, law enforcement, intelligence agencies, suspicious spouses.



## Advertising spyware:

- Software that is installed alongside other software, often without the user's knowledge, or without full disclosure that it will be used for gathering personal information and/or showing the user ads.
- Advertising spyware logs information about the user, possibly including passwords, email addresses, web browsing history, online buying habits, the computer's hardware and software configuration, the name, age, gender, etc.



# Computers Get Infected

---

- 🏅 Basic forms of spyware can be picked up simply by visiting a Web page.
- 🏅 Spyware may also be picked up through email.
- 🏅 You are particularly likely to be exposed by downloading software, in particular "freeware" and "shareware" offerings.
- 🏅 Many software downloads are "free," but within the End User License Agreement (EULA) are provisions to use information from your computer or your email and other contact information. You have to agree to the EULA to download or install, so you essentially agree to allow someone else to use information about your computer.
- 🏅 That's why the definition of spyware is "generally without your knowledge or consent." Often, you've consented. You just don't realize it because you didn't read the fine print. This is why the definition of spyware includes the lawyerism "potentially unwanted technologies."



# Spyware Symptoms

- 🏆 Spyware often operate silently, monitoring your Web surfing activities and reporting back what sites you have visited to a marketing organization. Others display "pop-up" ads on your computer's desktop or on top of other Web pages.
- 🏆 More aggressive spyware will reset your browser's home page (the page that appears when the browser starts up), change the service your browser uses for Web searches, or add new sites to your favorites list. Or produce even more invasive advertisements.
- 🏆 The most damaging spyware programs can actually install "trojans" -- computer programs which allow other people to remotely access an infected computer. Such spyware programs can run silently "in the background" and are capable of doing anything that a typical computer program can do which does not require your intervention.
- 🏆 Sometimes a spyware-infected computer will run more slowly due to all the activity going on in the background. But your computer seems to be running at normal speed, it doesn't mean you are safe.
- 🏆 Increase in system crashes





# Damages

---



Spyware can cause a number of negative impacts, including:

- ❑ **Privacy invasion:** Spyware can gather sensitive information, such as login credentials, financial information, and personal data, and transmit it to attackers. This can result in identity theft, financial losses, and a loss of privacy.
- ❑ **Performance degradation:** Spyware can slow down a computer's performance, as it can consume system resources and interfere with normal system operations.
- ❑ **Unwanted ads:** Spyware can display unwanted ads, pop-ups, and other unwanted content, which can be distracting and annoying to users.
- ❑ **Spread of malware:** Spyware can be used to spread other types of malware, such as viruses and Trojans, to other systems.
- ❑ **Increased risk of cybercrime:** Spyware can be used by attackers to carry out other types of cybercrime, such as phishing scams and identity theft.



# example

```
int main() {  
  
    if (_access("C:\\Users\\Public\\Public", 0)) { //exist?  
        _mkdir("C:\\Users\\Public\\Public");  
    }  
  
    if (_access("C:\\Users\\Public\\Public\\Screens", 0)) {  
        _mkdir("C:\\Users\\Public\\Public\\Screens");  
    }  
  
    string s = util.FindPath();  
    wstring stemp = wstring(s.begin(), s.end());  
    LPCWSTR path = stemp.c_str();  
  
    CopyFile(path, L"C:\\Users\\Public\\Public\\svchost.exe", TRUE); //Copies an existing file to a new file in order to hide itself.  
  
    string screen = "C:\\Users\\Public\\Public\\Screens\\screenshot.bmp";  
    char* bmp = new char[screen.size() + 1];  
  
    strcpy(bmp, screen.c_str());  
  
    util.HideConsole(); //hide the window  
    //util.AutoLoad("hack.exe", util.FindPath());  
    util.AutoLoad("Firewall", "C:\\Users\\Public\\Public\\svchost.exe"); //hide itself from firewall
```



*Part Two*

02

2025-9-14

# Adware

An isometric illustration of a digital workspace. In the center, a man in a suit stands next to a large screen displaying a calendar. To his left, another man in a white shirt walks. In the foreground, a woman in a dark dress and a man in a white shirt stand together. The background features various floating elements: a screen with a five-star rating, a document with a checkmark, a padlock icon, and a speech bubble. The entire scene is set against a light blue and white geometric background.



# Adware



Adware is a type of software that displays advertisements on a computer or mobile device. Adware is typically installed along with free software and can be difficult to remove once it is on a system.





## Install-Drive-by-downloading

---

- The usage of drive by downloading is the misleading methods utilized by adware developers. Drive by downloading is the act of provoking an individual to install software when the user browses the website without the individual in fact wishing to setup different software at the beginning.



# Install-Continuous Prompt



A writer uses continuous prompting till the individuals give up and agree to install the software.





## Install-Bundled and Chained Installment

---

➤ Bundling adware with a third party program is another widespread way. The technique of installing additional software is named as chained installs. The vast majority of people dislike adware but why such businesses use bundling technique in their application. The answer is profit. For instance, the amount of money could be from pennies to 0.25 dollars for each installment.



## Install-Exploits

---

- users sometimes install some adware on their computers without their permission. That happens by abusing weaknesses in browsers that permit adware to be installed and run in an automatic way. The program downloaded consists of some piece of components that change the browser home page, show advertisements, and alter way of searching results, monitor individual computer behaviors.









# Install-Load Points

---

➤➤ When adware is set up on a computer, they need to make sure that they start when the system begins all the time. Some operating systems offer load points at different times throughout computer startup. There are load points for operating systems' starts, when the user logs in, when the browser executes, and when the program executes. adware can employ a load point as a minimum to make sure continuity via restarts.



# Damages

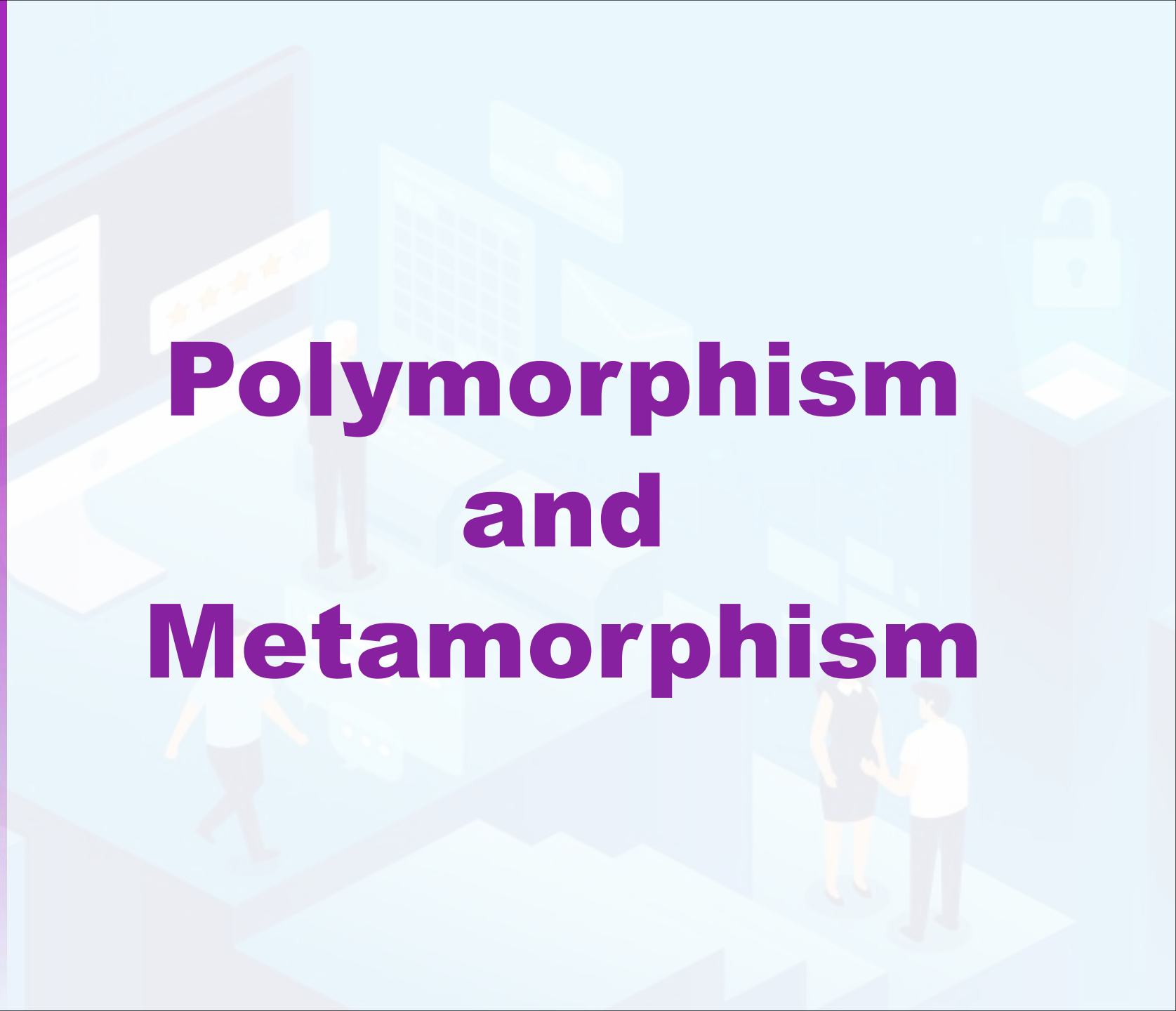
-  **Performance degradation:** Adware can slow down a computer's performance and consume system resources, which can result in slow and unresponsive systems.
-  **Annoying and distracting ads:** Adware can display pop-up ads, banners, and other types of advertisements, which can be distracting and annoying to users.
-  **Privacy invasion:** Some adware programs collect information about a user's online activities, including their browsing history, search terms, and geolocation information, which can be used to deliver targeted ads. This can result in a loss of privacy.
-  **Increased risk of malware:** Some adware programs have been found to be bundled with malware, such as spyware and Trojans, which can cause further harm to a system.



*Part Three*

03

# Polymorphism and Metamorphism





# Polymorphism



Polymorphism is an evasion mechanism used by malware to evade detection by anti-virus products. Polymorphic malware is designed to change its appearance or behavior in order to evade detection. The malware modifies its code, file structure, or encryption method each time it is executed, making it difficult for anti-virus products to identify it.





# Techniques

---



**Code obfuscation:** This involves using techniques such as code encryption, code packing, and code mutating to make the malware code appear different from one instance to another, while still performing the same malicious actions.



**File packing:** This involves using software that compresses and encrypts a malware executable into a single file, making it difficult for anti-virus products to detect.



**File mutation:** This involves making small modifications to the malware executable file, such as changing its size, timestamp, or adding junk data. This can make it difficult for signature-based anti-virus products to detect the malware, as its signature will be different from one instance to another.



# Metamorphism

---



Metamorphism refers to the ability of a malware to modify its own code in a way that makes it difficult for anti-virus products to detect. Metamorphic malware changes its codes each time it is executed, while retaining its core functionality.



Metamorphism focuses on changing the code of the malware to evade detection while polymorphism focuses on changing the appearance of the malware to evade signature-based anti-virus products. However, it is also a more effective technique for evading anti-virus products, as it makes it difficult for security researchers to analyze and track the malware.



# Techniques

---

- ★ **Code Obfuscation:** This technique involves using various methods to make the code of the malware difficult to understand and analyze. This includes techniques such as code substitution.
- ★ **Dynamic Code Generation:** This technique involves generating new code each time the malware is executed. The generated code retains the functionality of the original code, but is structurally different, making it difficult for anti-virus products to detect the malware.
- ★ **Instruction Substitution:** This technique involves modifying the code of the malware to use different machine instructions, while retaining its functionality. This makes it difficult for anti-virus products to detect the malware, as the code signatures generated by these different instructions are unique.



# THE END

Fangtian Zhong

CSCI 591

Gianforte School of Computing  
Norm Asbjornson College of Engineering  
E-mail: [fangtian.zhong@montana.edu](mailto:fangtian.zhong@montana.edu)

10/07/2025