



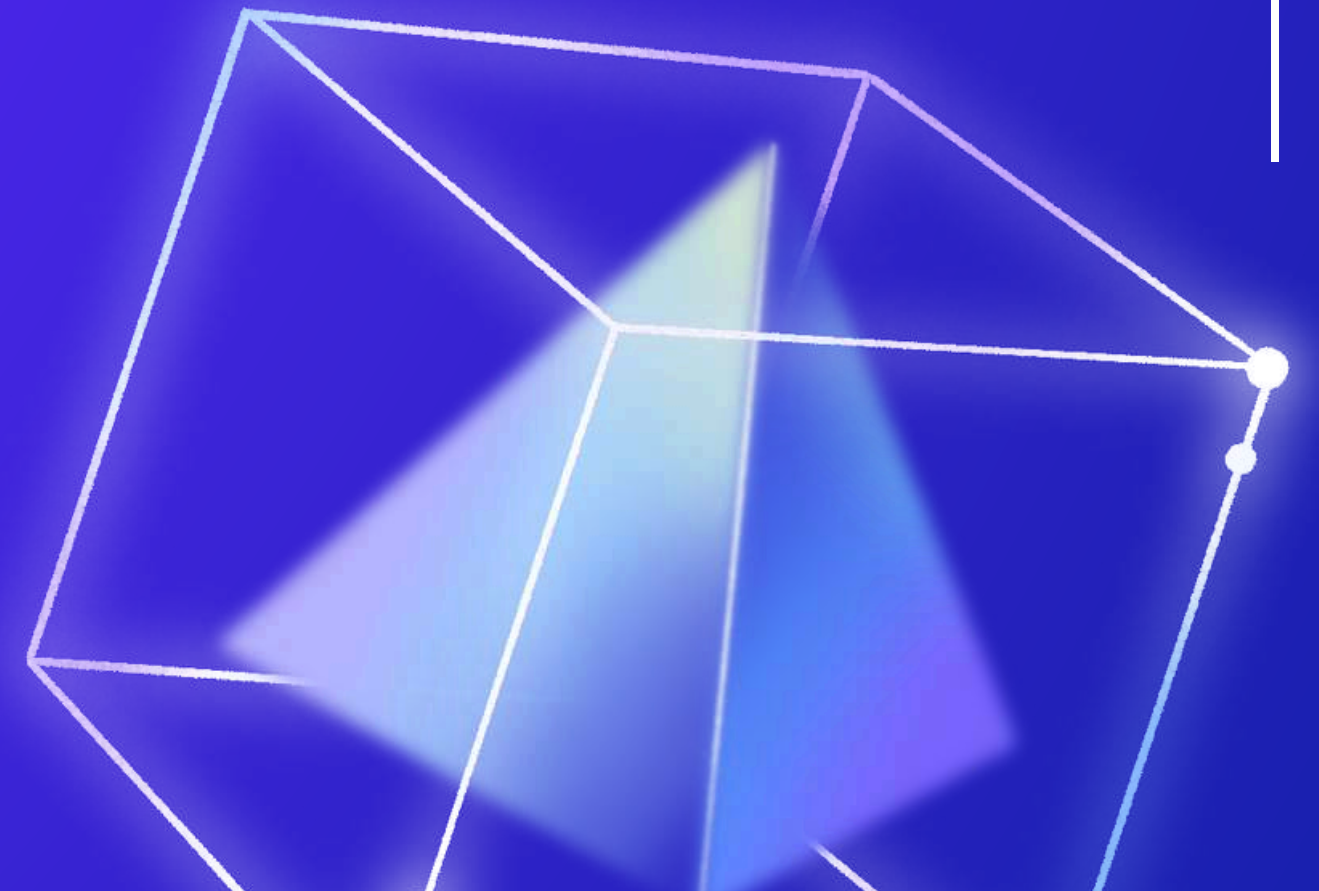
KEYLOGGER PROJECT

By Prakash vardanapu



TABLE OF CONTENTS

• Introduction	01
• Types of keylogger	02
• Project Scope	03
• Methodology	04
• How to protect devices	05
• Conclusion	06



INTRODUCTION

A KEYLOGGER OR KEYSTROKE LOGGER/KEYBOARD CAPTURING IS A FORM OF MALWARE OR HARDWARE THAT KEEPS TRACK OF AND RECORDS YOUR KEYSTROKES AS YOU TYPE. IT TAKES THE INFORMATION AND SENDS IT TO A HACKER USING A COMMAND-AND-CONTROL (C&C) SERVER. THE HACKER THEN ANALYZES THE KEYSTROKES TO LOCATE USERNAMES AND PASSWORDS AND USES THEM TO HACK INTO OTHERWISE SECURE SYSTEMS



TYPES OF KEYLOGGERS



Software Keylogger

Software keyloggers consist of applications that have to be installed on a computer to steal keystroke data. They are the most common method hackers use to access a user's keystrokes.

A software keylogger is put on a computer when the user downloads an infected application

Hardware keylogger

A hardware keylogger works much like its software counterpart. The biggest difference is hardware keyloggers have to be physically connected to the target computer to record the user's keystrokes. For this reason, it is important for an organization to carefully monitor who has access to the network and the devices connected to it.

HOW KEYLOGGERS ATTACK YOUR DEVICE?



Spear
phishing

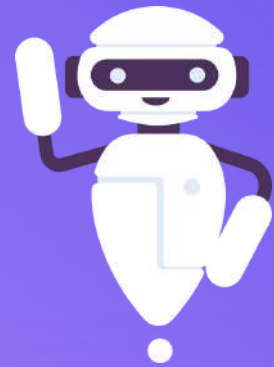


Drive-by
download



Trojan
horse

TYPES OF ATTACKS



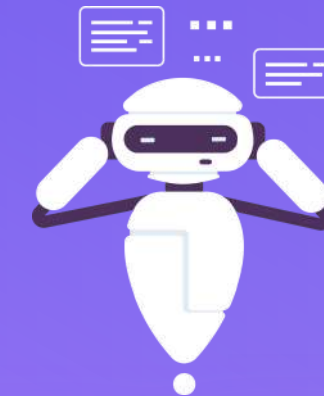
SPEAR PHISHING

Spear phishing is one of the most prominent methods of initiating a malware infection. In most cases, a phishing email or link is used to target a consumer. The link looks legitimate—it may even appear to come from a relative or a friend. However, after you open the email or click on a link, a keylogger is installed on your device. Spear-fishing attacks may also be used to launch a sextortion attack.



DRIVE-BY DOWNLOAD

Drive-by downloading refers to when a keylogger is installed on your computer without you knowing. This is often accomplished using a malicious website. When you visit the site, malware gets installed on your computer. It then works in the background, undetected, logging your keystrokes, then sending them to the attacker.



TROJAN HORSE

It is common for Trojan horses to have keyloggers bundled inside. A Trojan horse, similar to the one used in the Greek myth, appears to be benevolent. When the user opens it, malware containing a keylogger gets installed on their device. The malware, once installed, keeps track of the user's keystrokes and then reports them to a device accessed by the hacker.




HOW TO PROTECT MY DEVICES FROM KEYLOGGING?

The best way to protect your devices from keylogging is to use a high-quality antivirus or firewall. You can also take other precautions to make an infection less likely.

You may use a password manager to generate highly complex passwords—in addition to enabling you to see and manage your passwords. In many cases, these programs are able to auto-fill your passwords, which allows you to bypass using the keyboard altogether.

If you are not typing, a keylogger cannot record any strokes, and since password characters are usually replaced by asterisks, even a video surveillance system would not be able to figure out what was entered. In addition, use multi-factor authentication (MFA) when you have the option. A keylogger may deduce your password, but the second phase of the authentication process may deter them.



THANK YOU!



PROJECT LINK



<https://github.com/19PrAkAsHv/Keylogger-project.git>