C2 Frameworks: Essential Cybersecurity Guide

redfoxsec.com/blog/introduction-to-c2-frameworks

Shashi Kant Prasad July 27, 2023

Introduction to C2 Frameworks

- July 27, 2023
- Red Team
- Shashi Kant Prasad

Command and Control (C2) frameworks have emerged as a sophisticated and consequential dimension in the ever-evolving cybersecurity landscape. These frameworks are commonly employed by threat actors, particularly those involved in Advanced Persistent Threats (APTs), to orchestrate and manage cyber-attacks on targeted organizations or individuals. This blog delves into the intricacies of such frameworks, explaining their significance, functionality, and various types to equip you with the knowledge needed to bolster your organization's cybersecurity measures.

What is a C2 Framework, and Why is it Important?

C2 frameworks, or command and control frameworks, are tools that allow red teams and threat actors to communicate with and control compromised systems. They are used to send commands to the system, receive data from the system, and manage the system's

operations.

C2s provide:

- A stealthy communication channel between an infected host and the attacker's server.
- Enabling the propagation of malicious activities.
- Exploitation of vulnerabilities.
- Data exfiltration.

Importance

C2 frameworks are important for red teams because they allow them to conduct simulated attacks and assess the security of their networks. They can also be used to gather intelligence on the target network and its defenses.

For threat actors, C2 frameworks are essential for carrying out malicious activities. They allow them to maintain control of their compromised systems and avoid detection by security solutions.

There are a variety of C2 frameworks available, both commercial and open source. Some of the most popular C2 frameworks include:

- **Cobalt Strike**
- **Empire**
- **Light C2**
- **Machete**
- **Sliver**

The best C2 framework for you will depend on your specific needs and requirements. However, all of the frameworks listed above are effective and reliable.

Features of the Best C2 Framework for Red Teaming

Given below are some of the features of the **best C2 framework for red teaming**:

Intuitive user interface: Since the C2 framework has user-friendly interface, it simplifies the management of every aspect of your red team operations. From effortlessly configuring targets and triggers to real-time monitoring and response to threats, the C2 Framework streamlines the entire process, making it convenient and efficient.

1. **Advanced automation capabilities:**The C2 Framework offers full automation, making it highly suitable for scaling up your red team operations without compromising on performance or accuracy. Whether you need to execute multiple targeted attacks on numerous targets simultaneously or simulate extensive cyberattacks, the C2 Framework effortlessly manages all these tasks with seamless efficiency.

2. **Robust security features:** The primary objective of the C2 Framework is to provide robust data protection and operational security through advanced encryption and authentication features. It comprises a precise permissions system, which guarantees that confidential information and critical functionalities are accessible only to authorized users.
3. **Extensive third-party integrations:**The C2 Framework offers seamless integration with several industry-leading tools as well as resources. In addition to this, it includes IDS/IPS systems, SIEMs, vulnerability scanners, threat intelligence platforms, and more.

Benefits

Here are some of the benefits:

- **Ease of use:**C2 frameworks make it easy to communicate with and control compromised systems. They provide a user-friendly interface that allows you to send commands, receive data, and manage the system's operations.
- **Robustness:**C2 frameworks are designed to be robust and reliable. They can withstand attacks from security solutions and keep your agents communicating even under duress.
- **Evasion:**C2 frameworks can be used to evade detection by security solutions. They can use a variety of methods, such as encrypted communications, obfuscating traffic, and changing C2 domains.
- **Flexibility:**C2 frameworks are flexible and can be customized to meet your specific needs. You can choose the features that you need and the way that you want to use the framework.

If you are looking for a way to communicate with and control compromised systems, then a C2 framework is a good option. They are easy to use, robust, and can be used to evade detection.

C2 Framework

A C2 framework typically works in the following way:

1. The attacker compromises a system and installs a C2 agent on the system.
2. The C2 agent periodically connects to the C2 server to check for commands.
3. When the C2 agent receives a command, it executes the command on the compromised system.
4. The C2 agent then returns the results of the command to the C2 server.

The C2 server can be a standalone server or a cloud-based server. The C2 server is typically protected by encryption and authentication mechanisms to prevent unauthorized access.

This frameworks can be used for a variety of purposes, including:

- **Attacking systems:**C2 frameworks can be used to attack systems by sending commands to the compromised systems.
- **Gathering intelligence:**C2 frameworks can be used to gather intelligence about the target network by sending commands to the compromised systems to collect data.
- **Maintaining control:**C2 frameworks can be used to maintain control of compromised systems by sending commands to the systems to keep them running and to prevent them from being cleaned up.

C2 frameworks are a valuable tool for both red teams and threat actors. They allow red teams to conduct simulated attacks and assess the security of their networks. They also allow threat actors to maintain control of their compromised systems and avoid detection by security solutions.

Open-Source C2 Frameworks

Numerous open-source C2 frameworks are available that provide robust and customizable solutions for orchestrating cyber-attacks. Some of the most popular include:

- **Sliver:**A multi-platform, open-source C2 framework that enables automated adversary emulation and post-exploitation activities.
- **AsyncRAT:**A Remote Access Trojan (RAT) designed to control and monitor computers over an encrypted secure connection remotely.
- **Sillenttrinity:**A post-exploitation C2 framework that leverages.NET DLR to perform malicious activities.
- **Koadic:**A post-exploitation rootkit that provides various penetration testing options to the attacker.
- **Covenant:**A .NET command and control framework that emphasizes the attack surface of.NET, offering a collaborative platform for red teamers.
- **Metasploit:** It is a widely used tool found in the Kali Linux distribution, designed for identifying network and server vulnerabilities. Being an open-source platform, it allows operators to customize it for various operating systems like Android, iOS, macOS, Linux, Windows, Solaris, and more. One of its key components, Meterpreter, offers a range of capabilities, including both staged and non-staged payloads that simplify port forwarding across different networks.

Each framework provides a unique set of tools and capabilities, allowing attackers to tailor their approach based on their specific objectives and the target’s system configuration.

Commercial C2 Frameworks

In addition to open-source solutions, several commercial C2 frameworks are available that offer advanced features and capabilities. These include:

- **Cobalt Strike:**A commercial, full-featured C2 framework that offers a wide range of tools for reconnaissance, attack planning, and post-exploitation activities.
- **Brute Ratel:**A Red Team & Adversary Simulation Software that provides a range of sophisticated, stealthy attack capabilities.

- **INNUENDO:**A post-compromise implant architecture that simulates complex data exfiltration attacks.
- **Scythe/ Purple Team Exercise Framework:**A comprehensive evaluation tool for information security that facilitates cooperative attack, detection, and response exercises.

Commercial C2 frameworks often provide more robust and reliable solutions than their open-source counterparts, making them a favored choice among advanced threat actors.

Detection and Mitigation

Detecting and mitigating C2 attacks requires a multi-faceted approach that combines proactive measures with reactive strategies. Some key steps include:

- **Implement Robust Security Measures:**Adopting robust security practices such as network segmentation, rate-limit restrictions, and traffic monitoring can significantly reduce the risk of a C2 attack.
- **Continuously Update and Scan Systems:**Regularly updating and scanning your systems with trusted antivirus software can help identify and eliminate potential threats before they can establish a C2 channel.
- **Educate Users:**Providing security awareness training to all employees can help them recognize potential threats and understand the risks associated with C2 attacks.
- **Implement Access Control:**Limiting user rights and implementing two-factor authentication can provide additional protection against C2 attacks.
- **Monitor Network Traffic:**Ongoing network traffic monitoring can help identify unusual patterns or anomalies that could indicate a C2 attack.

Case Studies

In recent years, C2 attacks have been responsible for some of the most high-profile and damaging cyber-attacks. Some notable examples are as follows:

- **US Missile Systems:**Chinese hackers allegedly hacked the plans for several modern US missile systems, marking a significant breach in national security.
- **The New York Times:**In a four-month-long attack, Chinese hackers reportedly gained access to the passwords of all 53 Times employees and stole documents related to ongoing investigations.
- **Twitter:**In 2013, a sophisticated C2 attack compromised over 250,000 user accounts on Twitter, gaining access to usernames, email addresses, and more.

To learn more about C2 Framework, checkout our comprehensive guide on how to set up the Covenant C2 Framework!

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. If you are looking to improve your organization's security posture, **contact us** today to discuss your security testing needs. Our team of security professionals can help you **identify vulnerabilities and weaknesses in your systems, and provide recommendations to remediate them.**

“Join us on our journey of growth and development by signing up for our comprehensive **courses**.“

PreviousAbusing ACL Misconfigurations
NextGPO Abuse

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack
September 05, 2025
This Is the Hacker’s Swiss Army Knife. Have You Heard About It?