Overview of Havoc C2 vs Cobalt Strike

Report

May 9, 2025

Prepared by:Gurbanova Fatima
Prepared for: MilliSec.Org

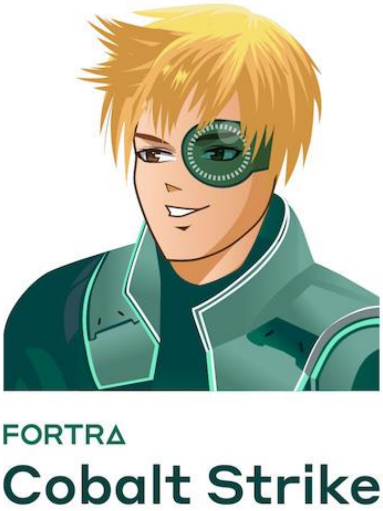


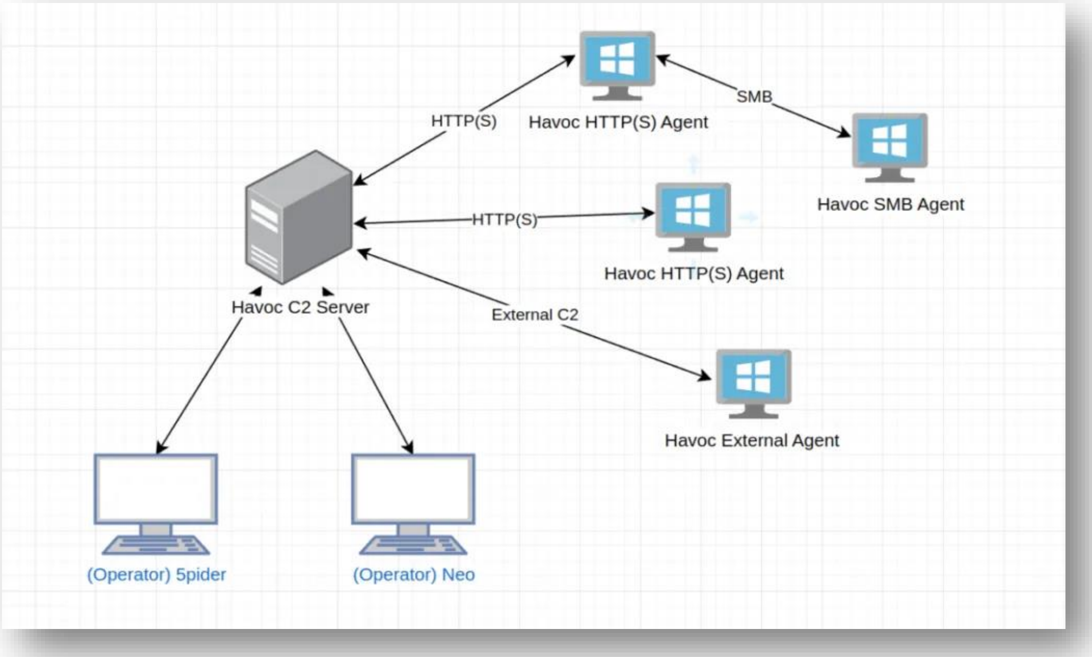
Table of Contents

Introduction

Command and Control (C2) frameworks are essential tools in both offensive security (red teaming) and adversary emulation. This report compares **Cobalt Strike**, a well-known and commercial tool, with **Havoc C2**, a newer and open-source alternative. Both platforms are used in security assessments, particularly for post-exploitation, lateral movement, and persistence.

Overview of Each Framework

Havoc C2:



Havoc C2 is a modern, open-source Command and Control (C2) framework designed for use in post-exploitation, red teaming, and adversary emulation. As a flexible and customizable alternative to commercial tools like Cobalt Strike, it provides cybersecurity professionals with a powerful platform for simulating real-world attacks and testing security defenses..

- **Modular Architecture**: Havoc C2 allows users to create and modify agents, as well as develop plugins, offering high levels of customization and adaptability for various red team operations.
- **Stealth Communication**: The framework supports encrypted communication channels over HTTP/HTTPS, making it difficult for security systems to detect and block C2 traffic.

□ **Customizable Payloads**: With the ability to build tailored payloads, Havoc C2 gives users flexibility to meet specific engagement needs, whether for penetration testing or adversary emulation.

□ **Advanced Evasion Techniques**: Havoc C2 is designed with a focus on evading modern detection systems, offering features that help bypass endpoint security solutions and remain undetected.

□ **Open-Source and Community-Driven**: As an open-source framework, Havoc C2 is freely available and benefits from continuous contributions from a growing community of cybersecurity experts, making it a constantly evolving tool.

Cobalt Strike

Cobalt Strike is a professional **tool for cybersecurity testing**. It is used by **red teams** to act like hackers in a safe way. The goal is to help companies find weaknesses in their systems before real attackers do.

Cobalt Strike is a **commercial tool**, so people need to buy a license to use it. It is popular among cybersecurity experts. But sadly, some **hackers** also use it in real attacks. That’s why many security programs can recognize it easily today.

Beacon (The Agent on the Target Computer)

- **Beacon** is a small program that runs on the target system.
- It connects to the attacker's server and waits for instructions.
- It can collect data, run commands, and stay hidden for a long time.

Command and Control (C2) Communication

- Beacon talks to the Cobalt Strike **team server** over the internet.
- It uses common protocols like **HTTP, HTTPS, DNS, and SMB**, which helps it hide in normal traffic.
- All communication is **encrypted** to avoid detection.

Post-Exploitation Tools

After gaining access to a computer, Cobalt Strike can:

- **Steal passwords**
- **Move to other systems** on the network
- **Hide tools and processes**
- **Create backdoors** for future access

Aggressor Script (Custom Automation)

- Users can write scripts to automate tasks using **Aggressor Script**.
- It helps to:
  - Save time
  - Control many Beacons at once
  - Create custom behaviors during an operation

Team Collaboration

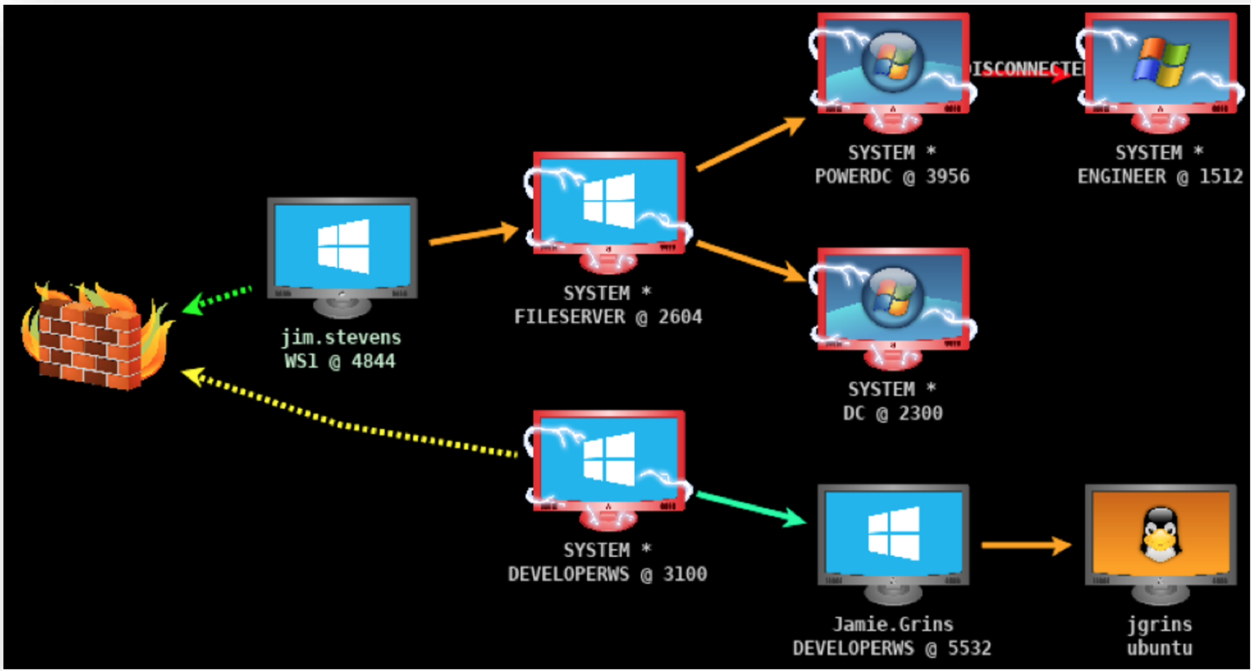
- Many red team members can work together at the same time.
- Everyone sees the same actions in real time through the shared interface.

Evasion Techniques (Avoiding Detection)

- Cobalt Strike uses several tricks to stay hidden:
  - **In-memory execution** (runs without saving files on disk)
  - **Sleep mask** (hides Beacon while it's inactive)
  - **Process injection** (runs inside trusted system apps)

Professional Tool with License

- Cobalt Strike is a **paid software** (not free).
- It is trusted by **cybersecurity professionals**, but also used by **real attackers**.
- Because of this, many antivirus programs know its default behaviors.



Side-by-Side Comparison of Havoc C2 vs Cobalt

- **Tool Type**
  Havoc C2 is **free** and open-source. It can be used without paying for a license.
  Cobalt Strike is a **paid** tool. You need to buy a license to use it.
- **Main Agent**
  Havoc uses **Demon**, a small and fast program that is hard to detect.
  Cobalt Strike uses **Beacon**, a more powerful agent with many features.
- **Control Server**
  Both tools use a **server** to control infected systems.
  Havoc's server is built using **Go** language.
  Cobalt Strike's server is built with **Java**.
- **User Interface**
  Havoc has a **modern and simple interface** that works on different

operating systems.
Cobalt Strike has an interface for **Windows** only.

- **Payload Types**
  Havoc can create **.exe**, **.dll**, and **shellcode**.
  Cobalt Strike can create **.exe**, **.dll**, **Powershell scripts**, and **macro documents**.
- **Communication Methods**
  Havoc uses **HTTP**, **HTTPS**, and **SMB** to talk to the server.
  Cobalt Strike uses the same methods, but it can also use **DNS** and **named pipes** to avoid detection.
- **Evasion Techniques**
  Havoc uses **smart tricks** like hiding the sleep time and making system calls look normal.
  Cobalt Strike uses techniques like **in-memory execution** and **process injection** to stay hidden.
- **Scripting and Customization**
  Havoc allows you to use **Python scripts** and add plugins to extend its features.
  Cobalt Strike uses a **scripting language called Aggressor Script** to automate tasks and customize actions.
- **Team Collaboration**
  Both tools allow multiple team members to work together during an operation.
  Cobalt Strike has a more **professional team setup**, but Havoc also supports collaboration.
- **Detection by Security Tools**
  Havoc is newer and **less recognized** by antivirus programs, making it harder to detect.
  Cobalt Strike is **more well-known** and is often detected by security tools.
- **Community and Support**
  Havoc has a growing **open-source community** that supports it through GitHub and Discord.
  Cobalt Strike offers **official support** for users who buy the tool, with regular updates.
- **Used by Hackers?**
  Yes, both tools are used by real **hackers** and **cybercriminals** in attacks.
- **Best for**
  Havoc C2 is great if you want a **free, customizable** tool that is **harder to detect**.
  Cobalt Strike is ideal for professional red teams and organizations that need a **full-featured** and **stable** tool for security testing.

Applications in Cybersecurity

Applications of Havoc C2 in Cybersecurity

- **Red Team Operations**:
  Havoc C2 is used by **red teams** to simulate **real-world cyberattacks** and test the defenses of an organization. It is effective for testing how well a company's security systems can detect and respond to hidden threats.
- **Penetration Testing**:
  Penetration testers (ethical hackers) use Havoc C2 to find and exploit weaknesses in a network. It is a good tool for performing **stealthy attacks** and checking the strength of security defenses.
- **Exploitation and Post-Exploitation**:
  After successfully compromising a system, Havoc C2 helps in **post-exploitation** tasks like **privilege escalation** and moving laterally inside the network. This helps security teams understand what an attacker could do after gaining access.
- **Learning and Research**:
  Because it is open-source, Havoc C2 is also used by **students**, **researchers**, and **cybersecurity enthusiasts** to learn more about ethical hacking and explore new attack techniques.

Applications of Cobalt Strike in Cybersecurity

- **Red Team Operations**:
  Cobalt Strike is a well-known tool for **red team operations**. It allows **ethical hackers** to simulate advanced cyberattacks and test how well an organization's security responds to real-world threats. It is commonly used in **professional red team operations**.
- **Advanced Threat Simulation**:
  Cobalt Strike is perfect for simulating **Advanced Persistent Threats (APTs)**, which are long-term, targeted cyberattacks. This makes it an ideal tool for testing how security systems handle sophisticated attacks over time.
- **Training and Awareness**:
  Cobalt Strike is often used in **training programs** for cybersecurity professionals. It helps them practice detecting and responding to advanced cyberattacks. Additionally, it is used in **Capture the Flag (CTF)** competitions to improve skills and test real-world security tactics.
- **Exploiting Vulnerabilities**:
  Security experts use Cobalt Strike to exploit **vulnerabilities** in a system. It

can simulate attacks like **phishing** and **social engineering** to identify weaknesses in an organization's defenses.

- **Evasion and Persistence**:
  Cobalt Strike is known for its **evasion techniques**, allowing it to avoid detection by **antivirus** and **endpoint security tools**. It can run in **memory**, avoiding writing files to disk, and uses **process injection** to stay hidden.

Application Area	**Havoc C2**	**Cobalt Strike**
Red Team Operations	Great for stealthy operations with low detection.	Widely used in professional red teaming.
Penetration Testing	Ideal for stealthy exploitation and lateral movement.	Great for full-scale penetration testing.
Exploitation and Post-Exploitation	Supports post-exploitation and persistence tasks.	Excellent for advanced post-exploitation and persistence.
Advanced Threat Simulation	Still developing, but effective for simpler attacks.	Perfect for simulating **APT** attacks and complex threats.
Evasion Techniques	Uses advanced tricks to avoid detection.	Strong evasion techniques but easier to detect.
Training and Research	Good for learning and experimenting with C2 techniques.	Used widely in professional training and CTF competitions.

Risks of Detection in Security Systems

Detection Risks with Havoc C2

- **New Tool**:
  Since **Havoc C2** is a newer tool, it is **less known** by security systems compared to more established tools like Cobalt Strike. This means that at

first, there might be a **lower chance of detection**. However, as more people use it, security systems will start to recognize it.

- **Customizable Payloads**:
  Havoc C2 allows users to **customize** how the tool behaves. This means attackers can change how it communicates with the target system, making it **harder to detect**. However, if not configured properly, it could still show signs that security systems can spot.

- **Obfuscation and Encryption**:
  Havoc C2 uses **encryption** and **obfuscation** to hide its activity. This means it can make the malicious code harder to see by security software. However, if the encryption is weak or not done well, it may still be detected.

- **Fileless Execution**:
  Havoc C2 avoids writing files to the disk, which helps it avoid detection by **file-based security tools**. However, some systems monitor activities in **memory**, which could still lead to detection.

Detection Risks with Cobalt Strike

- **Well-Known Tool**:
  Cobalt Strike is a **well-known tool** in cybersecurity. It is often used in **professional security testing**. Because of this, **security systems are more likely to recognize** Cobalt Strike's attack methods. This means the risk of detection is **higher** compared to Havoc C2.
- **Signature Detection**:
  Security systems, like antivirus software and EDR, use **signatures** to detect tools like **Cobalt Strike**. Since Cobalt Strike has been around for a while, there are **known signatures** that security systems can look for, making it easier to detect.
- **Beaconing and Command Traffic**:
  Cobalt Strike uses a tool called **Beacon** to communicate with the attacker's server. This creates regular network traffic, which can be spotted by security systems like **IDS** or **IPS** (Intrusion Prevention Systems). If not hidden properly, this **beaconing** can be detected.
- **Advanced Evasion Techniques**:
  Cobalt Strike does have **evasion features** that try to avoid detection, such as running in **memory** (so it does not leave files on the disk). However, **modern security systems** have become very good at spotting these techniques, so detection is still possible if the tool is not used carefully.
- **Higher Detection Risk in Large Networks**:
  Because Cobalt Strike is so widely used, many **organizations** look for it specifically. In large or well-monitored environments, **security teams** may

already be aware of Cobalt Strike's attack patterns and know how to recognize it quickly.

Aspect	Havoc C2	Cobalt Strike
Tool Popularity	New and less known, so **lower detection risk** at first.	**Higher detection risk** due to being well-known.
Payload Customization	Highly customizable, **more difficult to detect**.	Less customizable, but still detectable with the right tools.
Obfuscation/Encryption	Hides its code with encryption, but could be detected if not done well.	Uses evasion techniques, but may still be detected.
Fileless Execution	Avoids detection by not writing files, but can still be caught by **memory monitoring**.	Runs in **memory** too, but still detectable by advanced tools.
Traffic Patterns	Can hide traffic to avoid detection.	**Beaconing traffic** can be easily spotted.
Detection by Security Systems	Lower risk at first, but may increase over time.	**Higher risk** because it is widely recognized.

Conclusion

Havoc C2 is a newer tool, focused on stealth and customization, making it ideal for low-profile attacks and harder to detect initially. However, as it becomes more widely used, detection risks may increase.

Cobalt Strike is a well-established, professional tool with advanced features like beaconing and post-exploitation. While highly trusted, its widespread use means it is more likely to be detected by security systems.

In short, Havoc C2 is better for flexibility and stealth, while Cobalt Strike is better for professional red teaming but comes with higher detection risks. The right choice depends on your needs and environment.