Command and Control Servers: The Backbone of Cyber Operations and Ethical Hacking

Ari Torczon

aatorczon@cpp.edu

Abstract

The Command and Control server (C2) provides a backbone in cybersecurity for conducting malicious cyber attacks or the essential tool in ethical hacking. This essay looks into how C2 servers function, common use cases, and their importance with respect to both offensive and defensive strategy. The C2 server is utilized by malicious actors for persistence, data exfiltration, and the management of large scale operations such as botnets and APTs (advanced persistent threats). On the other hand, red teams and ethical hackers make use of C2 frameworks to simulate real world attacks, identify vulnerabilities, and improve organizational defenses. This essay, while showcasing a variety of detection techniques and mitigation strategies, underlines the importance of understanding C2 activity to actively take up the fight against cyber threats and highlights the role of ethical hacking in building robust security systems. This analysis underlines that investment in cybersecurity education and technology is a long way from being able to address the ever evolving threat landscape.

Command and Control Servers: The Backbone of Cyber Operations and Ethical Hacking

According to UcedaVélez (2015), “In the Middle Ages, attackers stormed the castle from different positions, bypassing the defensive walls, and breaking into the main entry castle doors. In the modern era, attackers strike from the different data interfaces that are available, breaking into the applications user and data interfaces, attacking the firewalls, and application access controls” (Foreword). This makes it clear that although the tactics of attackers have changed over centuries, the basic idea of breaching defenses is still relevant and consistent. In the modern world, one of the most advanced tools that a hacker uses is the C2 server. C2 servers act as a central hub when hackers coordinate attacks. This enables them to maintain control over compromised systems, steal sensitive data, and spread to other devices; however, C2 servers are not exclusively for bad guys. It is these very tools that have been used by ethical hackers and red teams in the same ways to simulate real-world attacks, expose vulnerabilities, and strengthen security defenses. This paper explores C2 servers in understanding their role in cyberattacks and their applications in red team operations, besides the methods for detection and mitigation. Additionally, the importance of understanding and countering the threat of C2, as will be discussed, is very crucial in protecting organizations and critical infrastructures.

Understanding C2 Servers

The C2 server mainly establishes and maintains communications with the attacker to their targeted systems, even in the presence of any security measures or monitoring. How it works is that it's a system which infects the victim’s devices with agents that are tasked to send malware or another form of malicious code that allows the hacker to take control of the device. It enables both the server and the agents to seamlessly execute commands for extracting sensitive data, installing additional malware, or moving laterally within a network.

Now, C2 servers are typically made up of a command server, which is the attacker's main system, through which the commands are issued to control the devices. This server can start and stop listeners, generate payloads, and handle agents. A listener handles the agents while being

able to host files. An agent is able to execute tasks, send results back to the listener, and persist on the compromised system. As for communication protocols, C2 servers often use standard protocols such as HTTP, HTTPS, DNS, or even custom protocols to communicate with agents. These protocols are chosen to blend in with regular network traffic and avoid detection using different methods like encryption in order to avoid detection. As this is going on, infected systems periodically check in with the C2 server using agents and listeners to receive commands or report the current status. Additionally, in case a server has been detected and is thus blocked, many C2 infrastructures have backup servers that allow them to remain operational. This includes DGA's (domain generation algorithms) which dynamically produces many domain names to point to their C2 servers in order to continue communication (Menon).

Hacking with C2 Servers

Now, hackers utilize C2 servers to achieve a range of different objectives throughout the duration of an attack. For example, hackers want to achieve persistence, long term access to compromised systems, even in cases where the victim attempts to remove the malware or disrupt the connection, either by shutting down systems or other methods. Hackers typically also want to exfiltrate data like passwords, financial records, or intellectual property, back to the hacker. Hacker's also want to move laterally, gaining access to other systems within the network for privilege escalation or just expanding the attack scope in general. Coordinating large scale operations is the management of, say, a botnet where control is exercised over thousands or millions of infected devices. To maximize the effectiveness of C2 servers, hackers employ various tools and strategies like different C2 frameworks, which are prebuilt platforms like Cobalt Strike, Metasploit, and Empire, where an attacker already has ready infrastructures to manage C2 operations. These frameworks have built in payload delivery, encryption, and other automated tasks. To stay hidden, attackers will encrypt C2 communications in attempts to avoid detection and monitoring. They might also use techniques like steganography to mask data within regular images or other non-malicious files. In terms of the protocols and channels hackers use, they typically use legit communication protocols like HTTP, HTTPS, DNS, and other protocols to hide malicious traffic within normal network traffic, which makes the defender's job of distinguishing malicious traffic from normal network traffic quite hard. Advanced attackers even use social media or cloud services for C2 channels.

We can look at real world examples of C2 servers playing a core role in several prominent cyber attacks, demonstrating their capabilities and effects. One case study in particular is Emotet, which was one of the most notorious malware campaigns that depended on C2 servers for conducting its operations, distributing payloads, and exfiltrating sensitive information from its victims. Its modular C2 infrastructure made it adaptable and persistent across a wide range of environments. There are also APT campaign groups like APT29 (Cozy Bear), which have been seen online using C2 servers to communicate stealthily with the compromised systems for several years. These operations incorporate various techniques such as advanced encryption and obfuscation of traffic. We can also look at examples of botnets like the famous Mirai botnet, which uses a C2 server to drive a DDoS attack against a website, a server, or even critical

infrastructure. As demonstrated, these hackers proved to be challenging for defenders and cybersecurity professionals. For example, the stealth of hackers is seen in their encryption and use of legitimate protocols to make C2 communications evade traditional detection methods, such as signature-based IDS (intrusion detection systems), more on advanced detection systems later. Hackers are also extremely agile, as expressed before, they often set up redundant C2 infrastructure, such as fallback servers and dynamic DGAs, to enable continued operations in case a C2 server is taken down.

Ethical Hacking

These techniques used by hackers are adopted by ethical hackers, people who test critical infrastructure to prevent future attacks. Red teams employ such an approach via a C2 server so as to closely emulate the action and tactics utilized in a proper cyber attack. C2 systems facilitate more organization of a red team in terms of task implementation while also enabling the better and smooth execution of attack scenarios from the attackers (Haynes). Red teams use C2 infrastructures much like a military command hierarchy for communication, task delegation, and oversight of operations. This mirrors the military's Cyber Command and Control system, or C3, which combines strategic planning with dynamic task allocation. In fact, the NMSG (NATO Modeling and Simulation Group) envisioned this a while ago where they said the following, “The year is 2025, and somewhere in the vicinity of the North Atlantic a need has arisen for a military force to perform a peacekeeping mission. NATO has agreed to deploy a Multinational Brigade for this mission, and three of its member nations have agreed to provide forces. The designated military organizations promptly connect their command and control (C2) and simulation systems over a secure network and begin training together for their new, common mission” (Pullen and Clark). It is currently almost 2025 and this is what NATO envisioned as far as C2 servers involvement in military operations. C2 servers also allow red teams to mimic various tactics, techniques, and procedures from APT and ransomware groups; this makes such testing far more valid, using attack vectors common in the wild. The approach of using C2 servers in red teaming keeps the team effort in order by putting everything on a single platform for tracking, resource allocation, and communication on a single platform. Going back to Haynes, she indicates that red teams require tools such as Armitage and Faraday, which were designed for collaboration and thus enable task management. Armitage makes it possible for team members to share insights, track the progress of the operation, and avoid redundancies in work. Additionally, C2 systems aggregate information about identified vulnerabilities and ongoing efforts, creating a comprehensive operational overview. In her study, Haynes evaluated the performance of a Cyber C3 prototype in a Capture the Flag setting. The experiment revealed that red teams that used C3 systems had a higher level of organization with fewer duplications. The experimental team did not win against the control group but indicated that the C3 system improved efficiency and group harmony. Haynes' participants reported more visibility of their teammates' actions and were hence able to collaborate more effectively. Nevertheless, along with the advantages, the C2 systems also have their setbacks, including dependence on adherence by the user and requiring extra features to be more effective, like automated notifications and

file-sharing capabilities. In this regard, with these improvements included, C2 tools are likely to perform better in red team operations as suggested in Haynes' research.

Conclusion

The C2 server is a required tool of the bad guy for control and expansion, but indeed serves the red team in modeling a threat to find new vulnerabilities, enhancing an organization's strategic defense. This again underlines C2 infrastructure as an essential concept, not only within the field of detection and mitigation but also in the future in improvement of defensive measures within controlled, ethical use of it. Such cybersecurity education and training are of utter importance if the gap is to be filled between attackers and defenders. Therefore, this comprises an advanced set of tool developments, refining ethical hacking, and effective training of blue teams that would respond appropriately towards the C2 activities. A necessary aspect in a wide range of cybersecurity strategies, such advanced education provides the future generation with enough knowledge and preparedness for evolved threats that endanger not only organizations but individual digital spaces. We have to fight fire with fire, or in this case, to beat the hacker you must become the hacker (ethically).

References

A. Menon, "Thwarting C2 Communication of DGA-Based Malware using Process-level DNS Traffic Tracking," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-5, doi: 10.1109/ISDFS.2019.8757555.

Tony UcedaVelez, Marco M. Morana. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. 2015, John Wiley and Sons, Inc.

Haynes, Kaitlin Britt, "A Command and Control Approach to Red Teaming" (2014). Theses and Dissertations. 45. https://scholarsjunction.msstate.edu/td/45

Dr. J. Pullen and Nicholas K. Clark. Frontiers of C2: A Distributed Development Environment for a C2SIM System of Systems. November 2017, 22nd ICCRTS https://netlab.gmu.edu/pubs/ICCRTS2017_paper86_final-C2SIM.pdf