Network Security Assignment 2

What is a Command and Control Attack?

Malicious network attacks have been on the rise in the last decade. One of the most damaging attacks, often executed over DNS, is accomplished through command and control, also called C2 or C&C. Command and control is defined as a technique used by threat actors to communicate with compromised devices over a network.

C2 usually involves one or more covert channels, but depending on the attack, specific mechanisms can vary greatly. Attackers use these communication channels to deliver instructions to the compromised device to download additional malware, create botnets or exfiltrate data.

According to the MITRE ATT&CK framework, there are over 16 different command-and-control tactics used by adversaries, including numerous subtechniques:

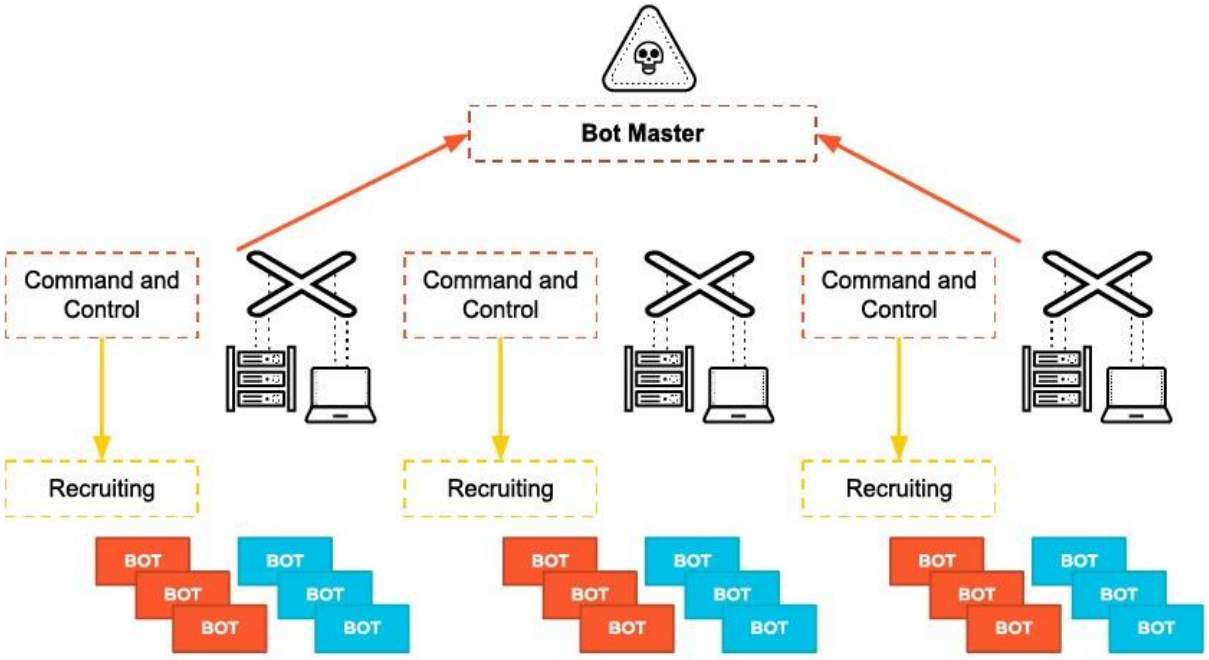
1. Application Layer Protocol
2. Communication Through Removable Media
3. Data Encoding
4. Data Obfuscation
5. Dynamic Resolution
6. Encrypted Channel
7. Fallback Channels
8. Ingress Tool Transfer
9. Multi-Stage Channels
10. Non-Application Layer Protocol
11. Non-Standard Port
12. Protocol Tunneling
13. Proxy
14. Remote Access Software
15. Traffic Signaling
16. Web Service

How a Command and Control Attack Works

The attacker starts by establishing a foothold to infect the target machine, which may sit behind a Next-Generation Firewall. This can be done in a variety of ways:

- Via a phishing email that:
  - Tricks the user into following a link to a malicious website or
  - opening an attachment that executes malicious code.

- Through security holes in browser plugins.
- Via other infected software.



Once communication is established, the infected machine sends a signal to the attacker's server looking for its next instruction. The compromised host will carry out the commands from the attacker's C2 server and may install additional software. Many attackers try to blend C2 traffic with other types of legitimate traffic like HTTP/HTTPS or DNS. The goal is to avoid being detected.

The attacker now has complete control of the victim's computer and can execute any code. The malicious code will typically spread to more computers, creating a botnet – a network of infected devices. In this way, an attacker can obtain full control of a company network.

Command and control is one of the last stages of the kill chain (coined by Lockheed Martin). It occurs right before threat actors complete their objectives. This means that the attacker has already bypassed other security tools that may have been in place. Thus, it is critical for security professionals to quickly discover and prevent C2.

Types of Command and Control Techniques

There are three different models C2C attacks use. These models dictate how the infected machine will communicate with the command and control server. Each were designed to evade discovery as effectively as possible.

1. Centralized architecture

This is likely the most common model, much like a client-server transaction architecture. When a new computer is infected by a bot, it will join the botnet by initiating a connection to the C&C server. Once joined to the channel, the bot waits on the C&C server for commands from the botmaster. Attackers often use prevalent hosting services for C2c servers.

This model can be easy to detect and block, as the commands originate from one source. Therefore, the IP can be quickly detected and blocked. However, some cybercriminals have adapted their approach by employing load balances, redirectors, and proxies in their setup. In this case, detection is more challenging.

2. Peer to peer (P2P) architecture

This model is decentralized. Rather than relying on a central server, botnet members transfer commands between nodes. This makes the P2P model much more difficult to detect. Even if detected, it's usually only possible to take down one node at a time.

The peer-to-peer model is used frequently in tandem with the centralized model for a hybrid configuration. The P2P architecture works as a fallback when the main server is compromised or taken down.

3. Random architecture

The random architecture model is by far the hardest to detect. This is by design. The objective is to prevent security personnel from tracing and shutting down the C&C server or identifying the botnet's chain of command. This model functions by transmitting communications to the infected host (or botnet) from disparate sources:

- IRC chat rooms
- CDNs
- Social media comments
- Email

Cybercriminals improve their odds of success by selecting trusted, commonly used sources.

Devices Targeted by C&C

Command and control attacks can target nearly any computing device, including but not limited to.

- Smart phones
- Tablets
- Desktops
- Laptops
- IoT devices

IoT devices have the potential to be at increased risk of C&C for various reasons:

- They are hard to control as a result of limited user interfaces.
- IoT devices are usually inherently insecure.
- Smart objects rarely get patched, if ever.
- Internet of Things devices share large amounts of data via the Internet.

What Hackers Can Accomplish Through Command and Control

1. Malware delivery: With control of a compromised machine within a victim's network, adversaries can trigger the download of additional malware.
2. Data theft: Sensitive data, such as financial documents, can be copied or transferred to an attacker's server.
3. Shutdown: An attacker can shut down one or several machines, or even bring down a company's network.
4. Reboot: Infected computers may suddenly and repeatedly shutdown and reboot, which can disrupt normal business operations.
5. Defense evasion: Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. Depending on the victim's network, attackers establish command and control with varying levels of stealth to circumvent security tools.
6. Distributed denial of service: DDoS attacks overwhelm servers or networks by flooding them with internet traffic. Once a botnet is established, an attacker can instruct each bot to send a request to the targeted IP address. This creates a jam of requests for the targeted server.