Bots and Botnets

Bots and *botnets* are notoriously difficult for organizations to detect and defend against using traditional anti-malware solutions.

Key Terms

Bots (or *zombies*) are individual endpoints that are infected with advanced malware that enables an attacker to take control of the compromised endpoint.

A *botnet* is a network of bots (often tens of thousands or more) working together under the control of attackers using numerous servers.

In a botnet, advanced malware works together toward a common objective, with each bot growing the power and destructiveness of the overall botnet. The botnet can evolve to pursue new goals or adapt as different security countermeasures are deployed. Communication between the individual bots and the larger botnet through C2 servers provides resiliency in the botnet (see Figure 1-4).

Given their flexibility and ability to evade defenses, botnets present a significant threat to organizations. The ultimate impact of a botnet is largely left up to the attacker, from sending spam one day to stealing credit card data the next – and far beyond, because many cyberattacks go undetected for months or even years.

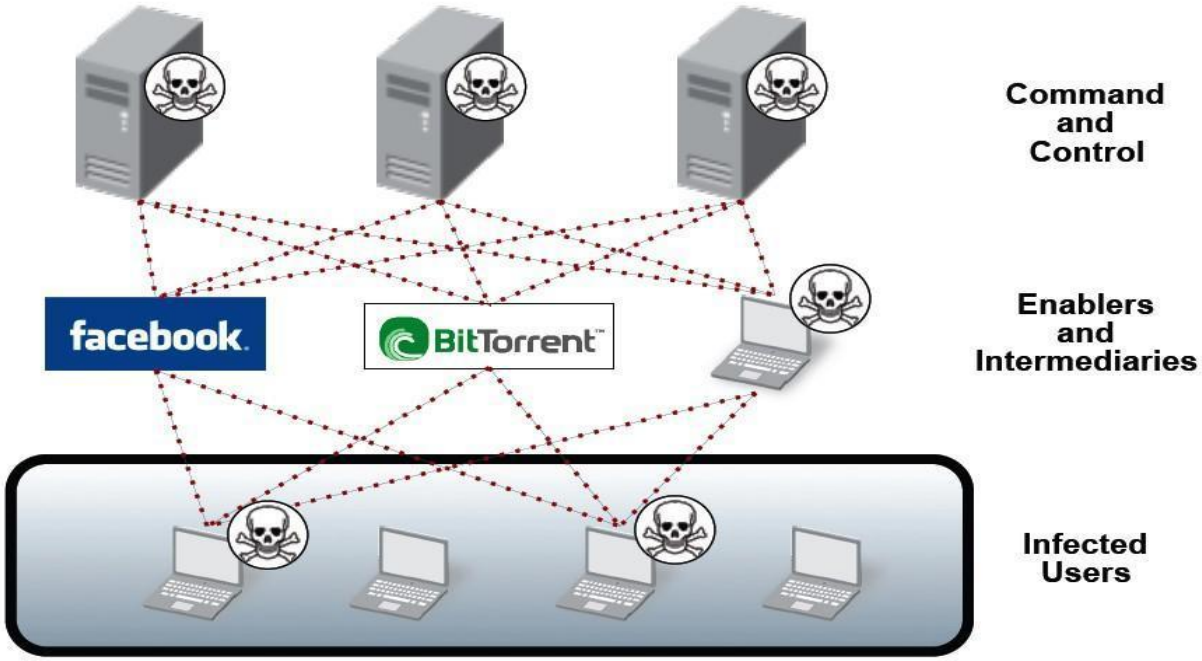

Figure 1-4 *The distributed C2 infrastructure of a botnet*

Botnets themselves are dubious sources of income for cybercriminals. Botnets are created by cybercriminals to harvest computing resources (bots). Control of botnets (through C2 servers) can then be sold or rented out to other cybercriminals.

The key to "taking down" or "decapitating" a botnet is to separate the bots (infected endpoints) from their brains (C2 servers). If the bots cannot get to their servers, they cannot get new instructions, upload stolen data, or do anything that makes botnets so unique and dangerous.

Although this approach may seem straightforward, extensive resources are typically required to map the distributed C2 infrastructure of a botnet, and this approach almost always requires an enormous amount of investigation, expertise, and coordination between numerous industry, security, and law enforcement organizations worldwide.

Disabling of C2 servers often requires both physically seizing the servers and taking ownership of the domain and/or IP address range associated with the servers. Very close coordination between technical teams, legal teams, and law enforcement is essential to disabling the C2 infrastructure of a botnet. Many botnets have C2 servers all over the world and will specifically function in countries that have little or no law enforcement for internet crimes.

Further complicating takedown efforts is the fact that a botnet almost never relies on a single C2 server but rather uses multiple C2 servers for redundancy purposes. Each server also is typically insulated by a variety of intermediaries to cloak the true location of the server. These intermediaries include P2P networks, blogs, and social networking sites, and even communications that proxy through other infected bots. These evasion techniques make simply finding C2 servers a considerable challenge.

Most botnets are also designed to withstand the loss of a C2 server, meaning that the *entire* botnet C2 infrastructure must be disabled almost simultaneously. If any C2 server is accessible or any of the fallback options survive, the bots will be able to get updates and rapidly populate a completely new set of C2 servers, and the botnet will quickly recover. Thus, even a single C2 server remaining functional for even a small amount of time can give an attacker the window needed to update the bots and recover the entire botnet.

According to a 2019 botnet threat report, Spamhaus Malware Labs identified and issued Spamhaus Block List (SBL) listings for 17,602 botnet C2 servers on 1,210 different networks.[1] Botnet C2 servers are used to control infected endpoints (bots) and to exfiltrate personal and/or valuable data from bots. Botnets can be easily scaled up to send massive volumes of spam, spread ransomware, launch *distributed denial-of-service* (DDoS) attacks, commit click-fraud campaigns, and/or mine cryptocurrency (such as Bitcoin).

[1] "Spamhaus Botnet Threat Report 2019." Spamhaus Malware Labs. January 2020. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019.

Key Terms

Distributed denial-of-service (DDOS) is a type of cyberattack in which extremely high volumes of network traffic such as packets, data, or transactions are sent to the target victim's network to make their network and systems (such as an e-commerce website or other web application) unavailable or unusable.

Spamming botnets

The largest botnets are often dedicated to sending spam. The premise is straightforward: The attacker attempts to infect as many endpoints as possible, and the endpoints can then be used to send out spam email messages without the end users' knowledge. The relative impact of this type of bot on an organization may seem low initially, but an infected endpoint sending spam could consume additional bandwidth and ultimately reduce the productivity of the users and even the network itself. Perhaps more consequential is the fact that the organization's email domain and IP addresses could also easily become listed by various real-time blackhole lists (RBLs), causing legitimate emails to be labeled as spam and blocked by other organizations, and damaging the reputation of the organization.

The Rustock botnet is an example of a spamming botnet. It could send up to 25,000 spam email messages per hour from an individual bot and, at its peak, sent an average of 192 spam emails per minute per bot. Rustock is estimated to have infected more than 2.4 million computers worldwide. In March 2011, the U.S. Federal Bureau of Investigation (FBI), working with Microsoft and others, was able to take down the Rustock botnet, which had operated for more than five years and at the time was responsible for sending up to 60 percent of the world's spam.

Distributed denial-of-service botnets

A DDoS attack is a type of cyberattack in which extremely high volumes of network traffic such as packets, data, or transactions are sent to the target victim's network to make their network and systems (such as an e-commerce website or other web application) unavailable or unusable. A DDoS botnet uses bots as part of a DDoS attack, overwhelming a target server or network with traffic from a large number of bots. In such attacks, the bots themselves are not the target of the attack. Instead, the bots are used to flood some other remote target with traffic. The attacker leverages the massive scale of the botnet to generate traffic that overwhelms the network and server resources of the target.

Unlike other types of cyberattacks, a DDoS attack does not typically employ a prolonged, stealthy approach. Instead, a DDoS attack more often takes the form of a highly visible brute-force attack that is intended to rapidly cause damage to the victim's network and systems infrastructure and to their business and reputation.

DDoS attacks often target specific organizations for personal or political reasons, or to extort a ransom payment in exchange for stopping the DDoS attack. DDoS attacks are often used by hacktivists to promote or protest a particular political agenda or social cause. DDoS attacks may also be used for criminal extortion purposes to extract a hefty ransom payment in exchange for ending the attack.

DDoS botnets represent a dual risk for organizations: The organization itself can be the target of a DDoS attack. And even if the organization isn't the ultimate target, any infected endpoints participating in the attack will consume valuable network resources and facilitate a criminal act, albeit unwittingly.

A DDoS attack can also be used as part of a targeted strategy for a later attack. While the victim organization is busy defending against the DDoS attack and restoring the network and systems, the attacker can deliver an exploit to the victim network (for example, by causing a buffer overflow in a SQL database) that will enable a malware infection and establish a foothold in the network. The attacker can then return later to expand the (stealthy) attack and extract stolen data.

Examples of recent DDoS attacks include attacks against *World of Warcraft Classic* and Wikipedia in September 2019.[2]

Financial botnets

Financial botnets, such as ZeuS and SpyEye, are responsible for the direct theft of funds from all types of enterprises. These types of botnets are typically not as large as spamming or DDoS botnets, which grow as large as possible for a single attacker. Instead, financial botnets are often sold as kits that allow attackers to license the code and build their own botnets.

The impact of a financial breach can be enormous, including the breach of sensitive consumer and financial information, leading to significant financial, legal, and brand damage. As reported by Tech Republic:

"A Mirai botnet variant was used in attacks against at least one financial sector company in January 2018 – possibly the first time an IoT botnet has been observed in use in a DDoS attack since the Mirai botnet took down multiple websites in 2017, according to a Thursday report from Recorded Future."[3]

[2] Oleg Kuprev, Ekaterina Badovskaya, and Alexander Gutnikov. "DDoS attacks in Q3 2019." Kaspersky. November 11, 2019. https://securelist.com/ddos-report-q3-2019/94958/.

[3] Rayome, Alison DeNisco. "Mirai variant botnet launches IoT DDoS attacks on financial sector." Tech Republic. April 5, 2018. https://www.techrepublic.com/article/mirai-variant-botnet-launches-iot-ddos-attacks-on-financial-sector/.