



Malware Tracker Service

Remote Attack Trojans (RATs) and
Command & Control (C&C) Botnets

RATs and C&C Botnets

Command and Control (C&C) Botnets are networks of compromised computers or devices controlled by a centralized server, allowing attackers to remotely manage and coordinate various malicious activities. These activities often include launching Distributed Denial of Service (DDoS) attacks, spreading malware, stealing sensitive information, or carrying out other forms of cybercrime.

On the other hand, Remote Access Trojan (RATs) malware is a type of malicious software that provides unauthorized remote access to a victim's computer or system. Once deployed, a RAT allows attackers to manipulate the infected device, steal information, and execute various commands without the user's knowledge. Both C&C botnets and RATs are potent tools in the hands of cybercriminals, enabling them to compromise systems, exfiltrate data, and carry out a range of malicious activities.

Significant Threat

It has been recorded that approximately 80% of all malware in some countries is associated with Remote Access Trojans (RATs) and Command and Control (C&C) Botnets.

RATs and C&C botnets pose as one of the most significant threats, alongside Ransomware, especially as both are adept at evading traditional antivirus tools. These malicious entities often employ sophisticated techniques to circumvent detection mechanisms, allowing them to establish covert connections and carry out unauthorized activities on compromised systems. RATs, are designed to operate stealthily, granting remote control to an attacker without the victim's knowledge.

Despite the challenges posed by these evasive tactics, the field of malware hunting or tracking has emerged as a proactive defense strategy.

Malware Tracker

Malware trackers are specialized tools designed to detect the presence of RATs and C&C botnets within an environment. Instead of relying on

predefined signatures and antivirus solutions, these trackers simulate the behavior of infected clients and interact with the network as if compromised. By doing so, they can alert security teams to the existence of these threats, even when traditional antivirus tools may falter.

Cygienic Malware Tracker Service

Our Malware Tracker Service is included with our standard Cygienic Cloud Subscription. This service provides continuous scans of your registered assets to identify Remote Access Trojans (RATs) and Command and Control (C&C) botnets. You will be promptly alerted via phone calls, email, and WhatsApp if any malware is discovered.

Security Alert Note:

Malware tracking abstains from engaging in any attacks, and its requests are devoid of malicious content. The alert triggered by your security product is a result of the application of a signature intended exclusively for outgoing network traffic (egress) being inaccurately applied to incoming traffic (ingress).

For more information on Cygienic Malware Tracker Service, please contact **sales@cygienic.com**