C&C Malware

Prevent data breaches from C&C malware – botnets, ransomware, RATs

There are many types of malware that, once installed, communicate with a Command & Control (C&C) server. This C&C server, typically hosted in the cloud, provides attackers with a way to centrally control and update malware. This makes these types of threats highly versatile and persistent.

This chatter between malware and controller includes things like keep-alive traffic to tell the C&C server that the malware is still live and running. Or it could be to the malware transferring screenshots, or keylogger captures of passwords etc. Examples of C&C malware include botnets, ransomware or RATs (Remote Access Trojans). More than half of all malware victims are SMBs.

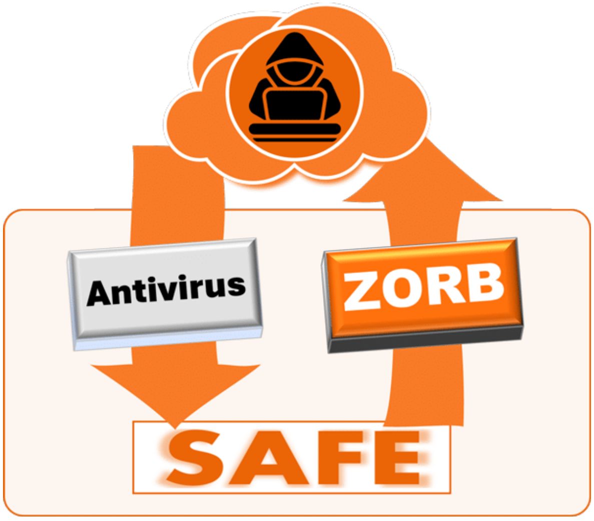
Some ransomware will contact their C&C server after installation, in order to obtain their encryption key. If this communication can be intercepted, it is often possible to prevent the ransomware from encrypting a device. In 2023, a business fell victim to a ransomware attack every 14 seconds.

RATs are a type of malware that gives attackers remote control of an infected system via a backdoor. RATs are usually delivered by email or malicious links. RATs such as NanoCore (healthcare, manufacturing, financial services) and Poison Ivy (defence, government, healthcare, financial services) have been used in targeted attacks and cyber espionage cam-

START TODAY
10 FREE licences
www.zorbsecurity.com/trial

The use of crypto-jacking malware to covertly mine cryptocurrency on infected systems has surged. Many variants use C&C servers to receive instructions and updates from attackers. Almost every part of the world experienced triple or quadruple-digit jumps in crypto-jacking incidents in 2023.

Advanced Persistent Threats (APTs), sophisticated threat groups often backed by nation-states, frequently use C&C infrastructure to maintain access to compromised networks for extended periods of time for cyber espionage or other malicious purposes.



ZORB

Prevention

Defending against C&C malware is still a significant challenge for cybersecurity professionals. One reason is that as much as 50% of these malware are zero-day, which means an applicable antivirus signature has yet to be released.

Blocking the communication between the malware and C&C is key to stopping the threat. Even if malware installs, blocking outbound comms 1) prevents the malware from registering with its C&C and 2) prevents exfiltration of stolen data. Some solutions, such as Cisco Umbrella, rely on DNS filtering to block malware comms at the DNS level.

ZORB takes a much simpler approach. Any communication from “untrusted” applications are blocked before the data flow can be established.

NOTE: ZORB are specialists in blocking outbound traffic. ZORB software is **NOT** a replacement for your device’s regular antivirus. ZORB does not monitor incoming data, so won’t detect malware being downloaded. Nor do we stop it from installing. We can, however, stop malware from sending data back to its C&C if it does install.

Example - Preventing ransomware

Safelist

Application	Trusted Destinations	Trusted Ports
Onedrive	Microsoft	
Excel	Microsoft, 192.168.1.62	
Outlook	Microsoft	
Word	Microsoft, 192.168.1.62	

A user clicked an email link that downloaded ransomware onto their device. The ransomware was able to bypass the device antivirus and installed on their machine as a file called ransomware.exe.

The company’s safelist contains all trusted business applications. ZORB applies a “BLOCK” to all outgoing traffic, unless it has come from a safelisted application. “Ransomware.exe” is NOT in the safelist, so ZORB blocks all outbound communications from “ransomware.exe” to its C&C server.

The ransomware has been programmed to evade endpoint protection. It realises that its traffic is blocked. So it renames itself to “Word.exe” (a safelisted application)

The ransomware comms data is now originating from a so-called “trusted” application (fake Word.exe). Tools such as Microsoft Defender for Endpoint will allow this “trusted” traffic to be transmitted. ZORB can take security a level deeper by associating trusted destinations to trusted applications. In the company’s safelist, Word is permitted to talk only with the internal server or Microsoft’s cloud. ZORB sees that the “trusted” application’s data is bound to a server hosted in Russia. This is not a trusted destination, so the outbound data is blocked.

Finally, the ransomware tries to communicate with a compromised Microsoft IP via SSH.

ZORB sees that traffic is coming from a trusted application (fake Word.exe) and wants to go to a trusted IP address associated with the source application (fake Microsoft IP address). However, ZORB blocks covert channels, such as SSH, FTP, TOR, RDP, etc, unless specifically permitted in the safelist. Again, the ransomware’s attempt at outbound communication with its C&C is blocked.