Types of Malware

Common Types

- Dropper/Downloader
- Keylogger/Info-Stealer
- (Spam) Bot
- Banker
- Worm
- Ransomware
- Miner
- Backdoor

Dropper/Downloader

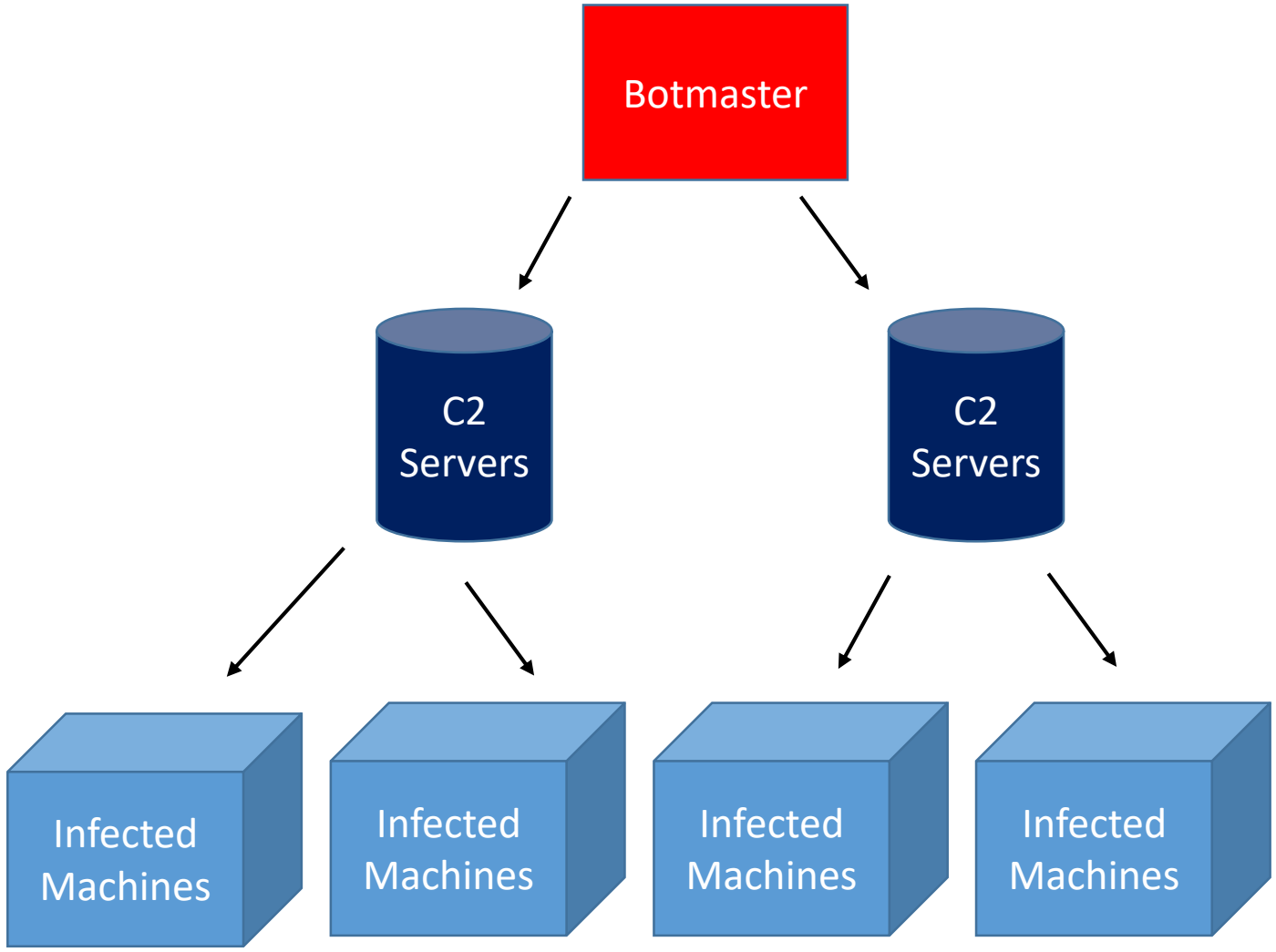
- Droppers:
  - Uses embedded scripts to extracts embedded executable from itself and executes it
  - Typically spreads through malspam using Office Word or Excel documents
- Downloaders:
  - Same as droppers, except second stage is downloaded remotely from a C2 (Command and Control) Server

Info-Stealers & Keyloggers

- Logs keystrokes
- Data exfiltration by emailing logs, ftp
- Data may be stored locally
- Communication may be encrypted
- Maybe able to steal browser or application password, eg Chrome, Firefox, IMVU, Outlook, FileZilla
- API used in Keyloggers: GetAsyncKeyState(), SetWindowsHookEx(), GetForegroundWindow()
- Features used in Stealers: SQLite3 for Chrome, Firefox DLL, CryptUnprotectData()

(Spam) Bot

- An infected machine becomes part of a botnet
- The botnet is controlled by the botmaster(s)
- May be used in mining cryptocurrencies, or in DDoS attacks, or sending malicious spam
- Eg: Mirai, Satori, Cutwail, ZeroAccess

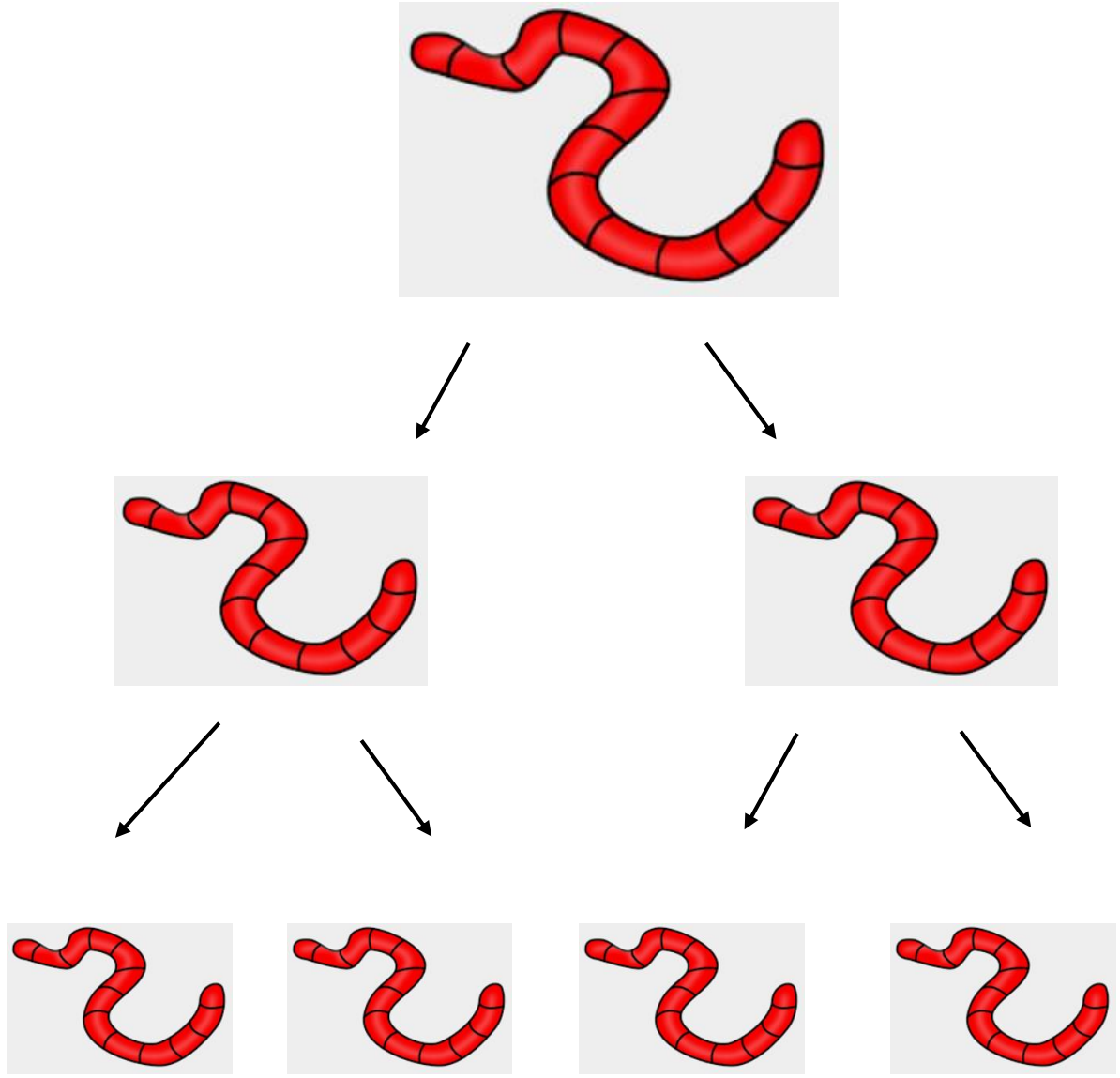


Banker

- Very common, alongside info-stealers
- Steals banking information
- Web Injection, API Hooking
- Eg: Zeus, Danabot, Ramnit
- API Hooking:
- Intercepts API and redirects to its fake API in order to steal information, eg hooking of HTTPSendRequest()

Worm

- Self-propagates across the network
- No interaction required
- Exploits vulnerabilities in operating systems (eg, EternalBlue)
- Contains malicious payload
- Eg, WannaCry (EternalBlue and DoublePulsar Exploit), contains ransomware payload



Ransomware

- Encrypts files and displays message to ask payment in order to release files
- Uses Bitcoin as payment
- Eg: WannaCry
- Gaining popularity because of crypto-currency
- Attacks becoming larger involving hundreds of thousands of machines becoming encrypted

Miners

- aka Crypto Miners
- Created from open source crypto-currency mining software
- Uses victim machines to mine for crypto-currency & sends them to attacker’s wallet
- Spreads through botnets or malspam

Backdoor (RAT = Remote Access Tool/Trojans)

- RAT = Remote Access Tool/Trojans
- Gives attacker hidden remote access to the system
- May include info-stealing and keylogging functionality
- Could be reverse TCP connection
- Sophisticated backdoors utilize modular framework, eg, Remcos

Thank you