Command and Control (C2): **Key Facts**

QinetiQ
People Who Know How

Modern advanced attack software often communicates and receives instructions from remote machines on the Internet – this communication path is called a Command and Control (C2) channel. **Given the prevalence and complexity of current malware then the assumption should be that your organisation is likely to have already been compromised**. You need a way to detect the infection and its C2 channels and then to remove it. The goal of any business is to defend against infections; but its goal should also be to detect the inevitable attacks as early as possible, respond quickly, limit the damage and recover promptly.

The following are the key facts about C2 channels and are taken from the report "Command and Control: Understanding, denying, detecting".

Core Facts

- C2 channels use many methods to communicate:
  - Hidden in normal traffic: HTTP, HTTPS, email, chat
  - Hidden in supporting traffic: DNS, ICMP, peer-to-peer
  - Hidden in content: images, documents and anything else that passes the security boundary
- Attacks are not just against servers
  - Client desktops are also targeted
- Do not assume that the C2 channel will be TCP to a central master server
  - Peer-to-peer protocols mesh many computers for control networks
  - UDP-based protocols such as DNS can be as useful as TCP protocols
- Bring Your Own Device (BYOD) and Take a Business Laptop Home (TBLH) puts equipment in less managed and less secured environments
  - C2 channels have more potential ways to communicate with their servers when outside the corporate boundary
- Advanced C2 channels use techniques to bypass firewall/ web blacklist & whitelist restrictions:
  - Social media sites (such as Facebook & Twitter) can host command servers
  - Shopping sites and their reviews (such as Amazon) have been used to host data extracted from compromised networks
  - Encoding and encryption can hide messages in almost any traffic type
- New technologies create new ways for C2 channels to be created
- But equally new technologies and innovative analysis methods also provide new opportunities for detecting C2 channels

Defending and Disrupting

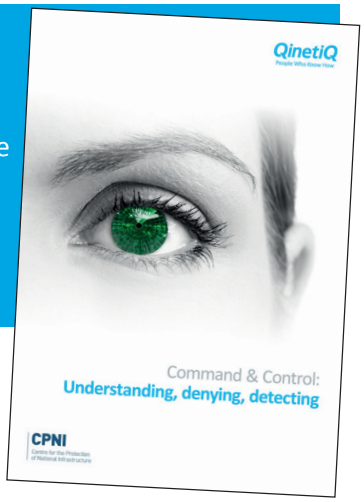
- C2 channels will find and exploit any holes in perimeter firewalls:
  - Filter both inbound (ingress) and outbound (egress) traffic to limit opportunities for C2 channels
  - Only open the minimal amount of firewall ports that are necessary to meet the business's requirements
- Use proxy servers to intercept and inspect all outbound traffic for malware and C2 channels
  - Web proxies to inspect and filter HTTP traffic
  - 'SSL breakers' in sensitive environments to inspect secure traffic
  - FTP and SSH proxies to inspect less common traffic
  - External connectivity should only be allowed via the proxy
- Separate internal DNS from external DNS, so that:
  - Internal DNS only resolves intranet addresses, proxy servers resolve public addresses
  - Malicious software is unable to resolve its command and control server
  - DNS cannot be used as a C2 channel from internal machines

CPNI
Centre for the Protection of National Infrastructure

Detecting

- IDS (Intrusion Detection Systems) alone are not the answer – advanced C2 will be designed to bypass them
  - However, careful sensor placement can detect the presence of some C2 channels
- IDS sensors must be configured to spot protocol anomalies
  - e.g. TCP port 80 is HTTP by convention – IRC chat over port 80 is anomalous
- Network flow ("Netflow") data can be used to profile an organisation's network surface, to spot traffic anomalies in busy networks
- The best patterns and most useful autopsies are made by analysing large data sets over extended periods
  - Log everything from all machines and devices
  - If possible, collect full packet network traffic at boundaries
  - Maintain logs for an extended period of time (months or more)
  - Examine the data for anomalies by comparing supposedly "similar" machines
- Watch trends over time to observe changes in patterns of communication
  - Good visualisations can be very helpful in spotting anomalous patterns

For more information about the threat of C2 channels and defences that can be put in place against them, please see the full report: "Command and Control: Understanding, denying, detecting" (QinetiQ.com/cpni-idata).



QinetiQ. Cyber security you can trust.

Customer Contact Team
QinetiQ
Cody Technology Park
Ively Road, Farnborough
Hampshire GU14 0LX
United Kingdom
Tel +44 (0)843 658 4668
cyberteam@QinetiQ.com
www.QinetiQ.com/cyber

QinetiQ would like to acknowledge the help and support of CPNI in producing this Command and Control document, sponsoring the underlying research and assisting in the production of the accompanying material.

QinetiQ
People Who Know How