Command and Control (C2) Channels

How is C2 established?

**Initial Infection**
Malware can come from many sources, including phishing attacks, infected USB sticks and downloads from malicious or compromised websites.

**C2 Channel Creation**
The malware reports back to the attacker with a beacon message. It is now ready to be controlled.

**Commanding and Controlling**
Once compromised, the malware establishes communication for C2 messages and results.

**Remember: C2 is remote**
Attacks can be run remotely from anywhere at any time. There is low risk and high reward for the attacker when they use C2.

How is C2 used?

Commands can have diverse effects, including:

- Explore networks and find vulnerable or important machines
- Infect other machines
- Take part in coordinated attacks
- Start programs and record user activity
- Copy data and valuable Intellectual Property (IP)
- Send captured data and IP out of the network

Commands are transferred to infected machines. Those commands are acted on and results are returned to the attacker. The attacker processes those results, transfers more commands, and waits for the next cycle in the loop.

QinetiQ would like to acknowledge the help and support of CPNI in producing this Command and Control document and the accompanying material.
© QinetiQ Ltd 2014

For more information please see the ‘Command and Control: Understanding, denying, detecting’ report at QinetiQ.com/cpni-data
Detecting and Disrupting C2 channels

The problem

C2 is quiet
Compared to normal user traffic, command and control messages are very small

C2 uses “normal” channels
Web, email, chat, DNS – all are commonly used Internet protocols, but they may not be expected on all organisations’ networks

C2 disguises itself
C2 can use tricks to evade some defences and detection – like sending chat messages across ports normally used for HTTP

The solution

Separate your networks and filter their traffic
Block unnecessary communication protocols
Log as much as possible and look for anomalies
Keep the logs for months or more
Correlate your data with other data sets

Correlate your data with other data sets.
Example correlation data sources:

Threat intelligence
What are antivirus companies, CISP and other organisations reporting?

Public holidays
Is there activity on an office close day?

For more information please see the ‘Command and Control: Understanding, denying, detecting’ report at QinetiQ.com/cpni-idata

QinetiQ would like to acknowledge the help and support of CPNI in producing this Command and Control document and the accompanying material.
© QinetiQ Ltd 2014