DuQu the precursor to the next Stuxnet

Charalampos Mavroforakis

Why talk about it ?

- Connection with Stuxnet (Feb 2010)
- Exploit used to get DuQu rolling
- P2P infection strategy

Goals of InfoStealer

- List of running processes
- Key presses
- File exploration, including removable drives
- Network information
- Open window names

Level-by-level

Internet

- True-type font exploit
- Kernel shellcode

Kernel

- Executes a driver to inject code in `services.exe` and runs the installer

Installer

- Decrypts the main DLL and the load point driver and creates a service. Also, writes a configuration file to the disk

Services

- Invokes the load point driver, which injects the main DLL to a process.

Level-by-level

DLL

- Reads the configuration file and injects the payload loader to the appropriate process

Loader

- Loads the payload into the memory and executes it

Payload

- Enables command-and-control (C&C) functionality

Info Stealer

- …

Configuration file

Lifetime value

DNS Addresses

List of injected processes

Table 3

Processes checked by Duqu

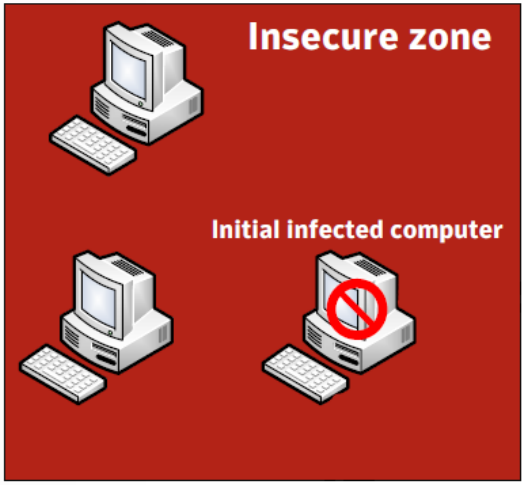
Product	Injection Target
Kaspersky Antivirus (versions 1-7)	lsass.exe
Kaspersky Antivirus (versions 8-11)	Kaspersky process
McAfee	winlogon.exe
AntiVir	lsass.exe
Bitdefender	lsass.exe
Etrust v5 and v6	does not perform injection
Etrust (other versions)	lsass.exe
Symantec	lsass.exe
ESET NOD32	lsass.exe
Trend	Trend process
Rising	Rising process

C&C communication protocol

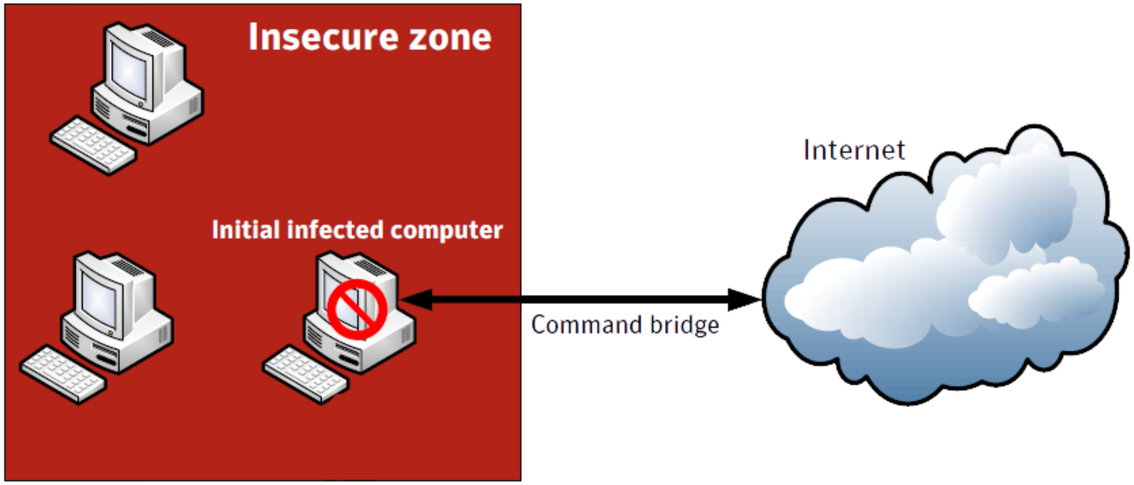
HTTP & friends	SMB
• outbound requests to server • results returned inside JPG files	• stands for *Server Message Block* • is a client server, for sharing files, printers, etc • serves P2P cases

Peer-to-Peer C&C

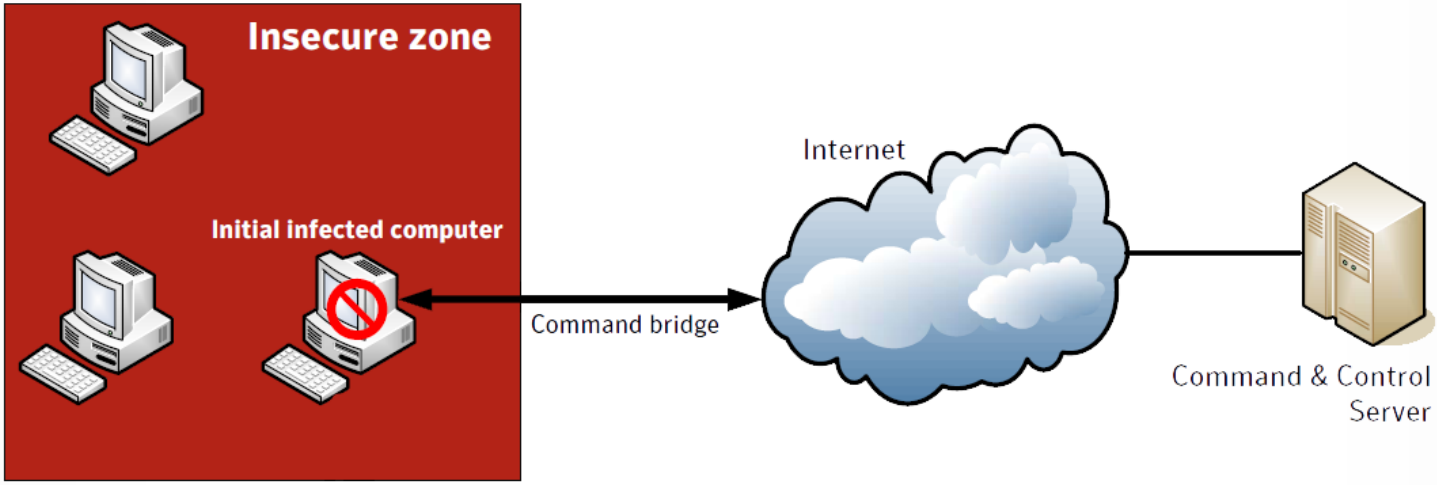
Peer-to-Peer C&C



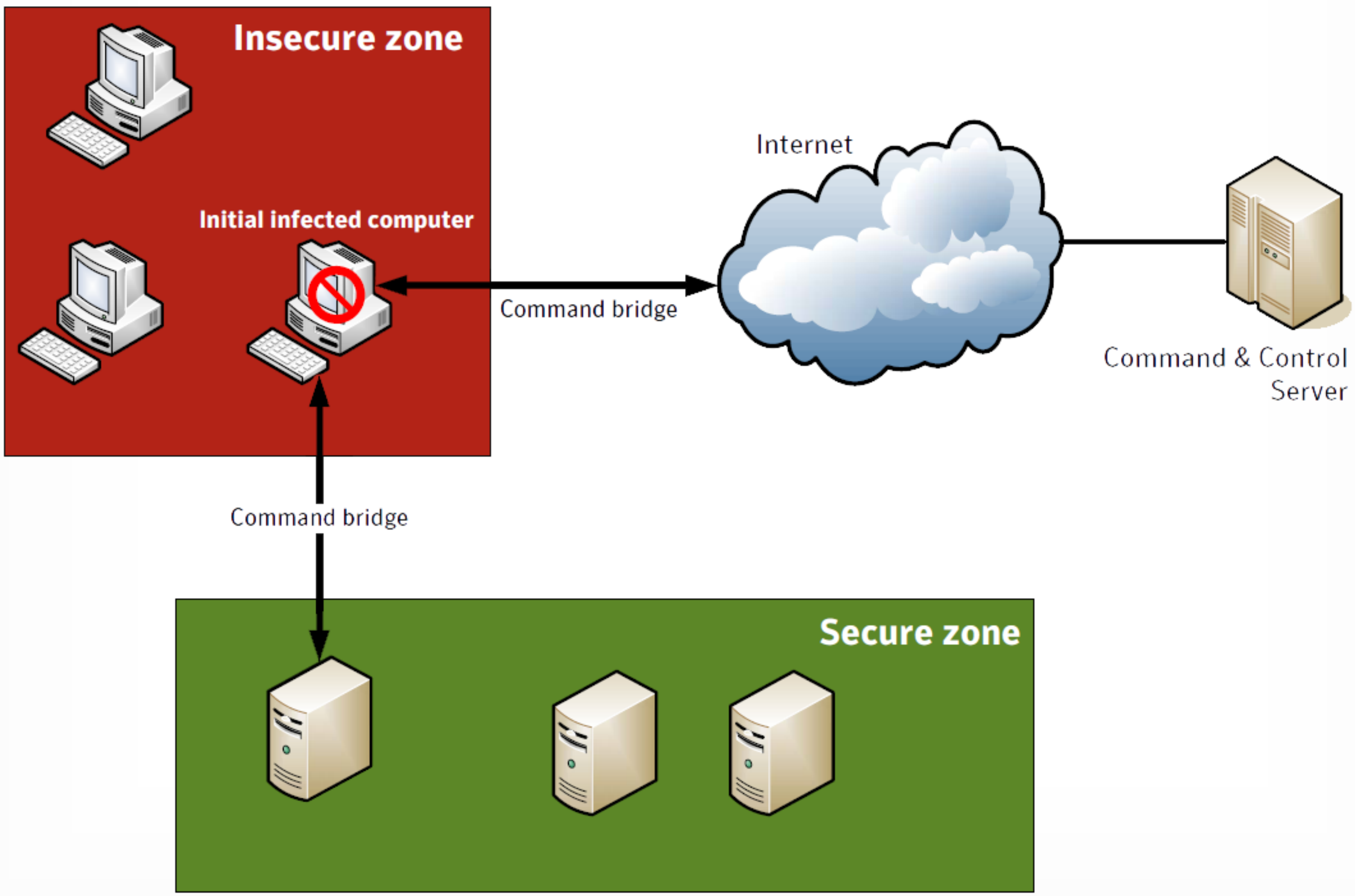
Peer-to-Peer C&C



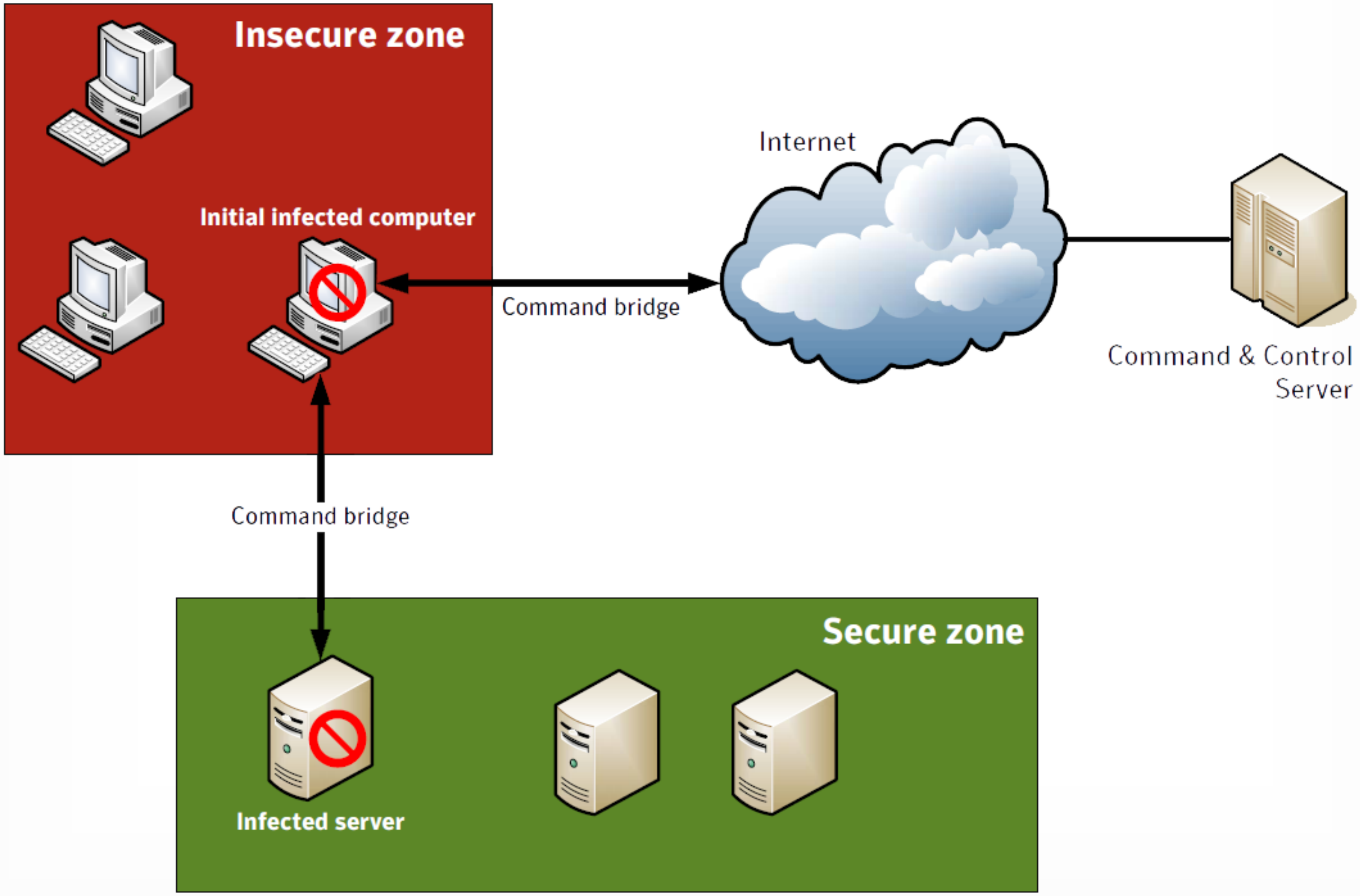
Peer-to-Peer C&C



Peer-to-Peer C&C



Peer-to-Peer C&C



C&C functionality

Download executables

Run

Upload results

Hubble image

Steganography: Hiding messages, so that no one suspects their existence

References

- W32.Duqu – The precursor to the next Stuxnet (Symantec, Nov 2011)
- Duqu: A Stuxnet-like malware found in the wild (CrySys, Oct 2011)
- Duqu – Threat Research and Analysis (McAfee Labs)